Online-Durchsuchung (Bundestrojaner)

Seminar IuG Überwachungs-Special

Christian Korscheck
Rechnernetze und Internet
Wilhelm-Schickard-Institut für Informatik
Universität Tübingen
Email: korschec@informatik.uni-tuebingen.de

***Kurzfassung*— Diese Ausarbeitung soll einen Überblick über das Thema Online-Durchsuchung verschaffen und die verschiedenen Positionen in der damit verbundenen Diskussion beleuchten. Es werden die Ziele und Möglichkeiten der Online-Durchsuchung, aber auch die Bedenken und Gefahren betrachtet. Ein Überblick über die rechtlichen Grundlagen und die Entwicklung in den letzten zwei Jahren unterstreicht die Dringlichkeit der Auseinandersetzung mit dem Thema Online-Durchsuchung. Abschließend wird auf eine mögliche technische Realisierung eingegangen.**

***Schlüsselwörter*— Online-Durchsuchung, Überwachung, Bundestrojaner, Gefahrenabwehr, Umgehen von Verschlüsselung**

I. Einleitung

Als Online-Durchsuchung bezeichnet man den Zugriff auf informationstechnische Systeme durch den Staat. Zu diesen Systemen gehören in erster Linie PCs und Laptops, aber auch PDAs, Smartphones und Handys. Diese Durchsuchung soll heimlich, das heißt ohne das Wissen des Überwachten ablaufen, indem über das Internet immer wieder auf das System zugegriffen wird.

Online-Durchsuchung ist in Deutschland parallel zur Diskussion um die Vorratsdatenspeicherung ein hochaktuelles und vieldiskutiertes Thema. Der Mangel an Informationen von offizieller Seite führt zu vielen kontroversen Standpunkten. In den Reihen der Politiker herrscht keine Einigkeit über den Funktionsumfang und den Nutzen der Online-Durchsuchung. Während einige Politiker in der Online-Durchsuchung ein Mittel zur Strafverfolgung sehen, möchten sie andere Politiker zur Gefahrenabwehr einsetzen. Eine dritte Gruppe von Politikern sieht in der Online-Durchsuchung eine Vereinigung aller Möglichkeiten und eine vierte Gruppe äußert sich allgemein sehr skeptisch.

Im Folgenden werden die einzelnen Standpunkte näher beleuchtet. Auf etwaige Forderungen zur privaten Nutzung der Online-Durchsuchung durch die Industrie im Kampf gegen Softwarepiraterie oder dem illegalen Herunterladen von Musik wird in dieser Ausarbeitung nicht weiter eingegangen, ebenso wenig wie auf die technischen Details von Überwachungssoftware, die sich im Ausland bereits im Einsatz befindet.

II. Ziele

Zu den Zielen gehören Gefahrenabwehr, nachrichtendienstliche Informationsbeschaffung und Strafverfolgung. Das größte Hindernis bei Ermittlungen, sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung, stellt die Verschlüsselung von Festplatteninhalten, aber auch von Daten, die über das Internet verschickt werden (E-Mails, VoIP, ...) dar [1]. Herkömmliche E-Mail-Überwachung durch bloßes "Mitlesen" der Datenpakete wird dadurch nutzlos. Die Daten müssen vor der Verschlüsselung aufgezeichnet werden. Dies kann erreicht werden, wenn auf dem System eine Hintertür (auch genannt: Backdoor, Trojanisches Pferd, Trojaner) für die Behörden eingerichtet wird. Diese Hintertür wird von offizieller Seite "Remote Forensic Software" (Fernforensische Software) genannt [2].

Auch wenn Gefahrenabwehr und Strafverfolgung durch die Verschlüsselung vor dem gleichen Hindernis stehen, unterscheiden sich die beiden Bereiche sowohl in ihren rechtlichen Grundlagen, die weiter unten diskutiert werden, als auch in den im Folgenden erläuterten Punkten.

A. Gefahrenabwehr und nachrichtendienstliche Informationsbeschaffung

Neben dem Abfangen von Daten vor der Verschlüsselung oder der Durchsuchung von Festplatteninhalten, die temporär entschlüsselt vorliegen, könnten auch kürzlich besuchte Websites, zugehörige Passwörter, Kontakte in Adressbüchern etc. gespeichert werden. Eine umfassende Informationssammlung über das System kann dabei helfen den Trojaner immer wieder neu an das System anzupassen, sobald Änderungen am System vorgenommen werden. Dazu gehören Informationen über Betriebssystem, installierte Sicherheitsupdates, Sicherheitssoftware wie Firewalls oder Antivirenprogramme, verwendete Hardware und installierte und häufig verwendete Programme.

Nachrichtendienste, wie z. B. der Verfassungsschutz, haben zur Aufgabe Daten zu Sammeln und Auszuwerten. Die gewonnen Informationen können dann zur Gefahrenabwehr, beispielsweise zur Anschlagsverhinderung, eingesetzt werden. Somit ist es wichtig eine möglichst große Informationsdichte zu erzielen.

B. Strafverfolgung

In Deutschland widmet sich das Bundeskriminalamt (BKA) der Strafverfolgung. Strafverfolgung mit Hilfe von

Online-Durchsuchung könnte so aussehen, dass die Online-Rekrutierung und -Kommunikation von Terroristen überwacht wird. Die Bildung einer terroristischen Vereinigung fällt unter das Strafgesetz und damit in den Bereich der Strafverfolgung (StGB §129a).

Aber auch den Kampf gegen Kinderpornografie wollen einige Politiker mit Hilfe der Online-Durchsuchung vereinfachen [3]. Wie die Online-Durchsuchung dabei genau helfen kann, ist allerdings nicht ganz klar. Eine Möglichkeit wäre, Informationen zu Aufenthaltsorten von Tätern, Opfern oder Tatgegenständen zu finden, welche konkrete Beweise zum untersuchten Fall liefern.

III. Möglichkeiten

Die Online-Durchsuchung erweitert klassische Polizeiarbeit im 21. Jahrhundert. Wo bisher die Wohnung oder das Auto von Verdächtigen durchsucht und der Festnetzanschluss überwacht wurde in der Hoffnung, schriftliche Aufzeichnungen oder anderweitig belastendes Material zu finden, muss diese Arbeit heutzutage durch die Dezentralisierung von Daten und der Speicherung von Informationen im Internet neue Wege gehen. Die Online-Durchsuchung kann dazu beitragen, besonders empfindliche Informationen zu erhalten, wenn es den Behörden gelingt die Daten vor der Verschlüsselung zu kopieren.

Die gesammelten Daten erhöhen die Informationsdichte, was die Planung des weiteren Vorgehens effizienter macht. Wer steht mit wem in Verbindung? Welche Rollen spielen die beteiligten Personen? Wer muss überwacht werden? Wo könnte ein Anschlag stattfinden? Wie wird dabei vorgegangen? Es kann genauer bestimmt werden, worauf die Behörden besonders zu achten haben und wie viele Beamte welchem Fall mit terroristischem Hintergrund zugeteilt werden können. Die gesammelten Informationen können auch dazu dienen, Täterprofile zu verfeinern, beispielsweise, um die Anti-Terror-Datei mit erweiterten Daten zu versorgen. Die Online-Durchsuchung bildet damit eine hervorragende Ergänzung zur Anti-Terror-Datei.

IV. Bedenken und Gefahren

Die größten Bedenken rühren daher, dass sich die Online-Durchsuchung mit dem momentanen Verständnis eines Rechtsstaates nicht vereinbaren lässt. Nachhaltigkeit und Transparenz gelten als Kernidee staatlichen Handelns und stehen zu der geforderten heimlichen Durchsuchung im Widerspruch. Online-Durchsuchung bedeutet einen massiven Eingriff in die Privatsphäre. Artikel 10 und/oder Artikel 13 [4] des Grundgesetzes müssten geändert werden, um die Online-Durchsuchung zu ermöglichen.

Ein weiterer Punkt ist, dass sich Terroristen zu schützen wissen. Ausbildungslager machen sie vertraut im Umgang mit Verschlüsselung und Geheimhaltung und lehren sie, wie sie sich gegen die Installation eines Trojaners schützen können. Darüber hinaus könnte es technisch versierten Terroristen sogar gelingen das System auszunutzen, um gezielt Falschinformationen zu verbreiten, auf Kosten Unschuldiger. Sie könnten auch versuchen, die Kontrolle über bestimmte mit einem Trojaner versehenen Systeme zu übernehmen oder einen Angriffsversuch auf die zentralen Server zu starten mit dem Ziel, Informationen zu stehlen oder zu manipulieren. Die Überflutung des Systems mit Terabyte an Datenmüll könnte dazu führen, automatisierte Auswertungsroutinen lahmzulegen und menschliche Kapazitäten zu binden, die eigentlich an anderer Stelle benötigt werden.

Digitale Daten sind bei der aktuellen Rechtsprechung in ihrer Beweiskraft umstritten, da die Unveränderbarkeit der Daten vor Gericht eine große Rolle spielt [5]. Bei digitalen Daten lässt sich im Nachhinein nicht eindeutig sagen, wer die Daten erstellt und auf der Festplatte abgelegt hat und ob sie bereits in genau dieser Form vor dem Zugriff auf der Festplatte lagen. Somit eignet sich die Online-Durchsuchung zur Strafverfolgung bei aktueller Gesetzeslage nur bedingt.

Die Überwachungsbefugnisse könnten zugunsten privater Nachforschungen missbraucht werden, wie dies bereits beim Bundesnachrichtendienst vorgekommen ist. So wird einem Beamten vorgeworfen den E-Mail-Verkehr eines Deutschen ausgespäht zu haben, weil dieser ein Verhältnis mit seiner Frau hatte [6].

Des Weiteren bestehen Zweifel an der Verhältnismäßigkeit der Online-Durchsuchung. Es stellt sich die Frage, ob die Online-Durchsuchung nur bei technisch ungeschulten Verdächtigen funktioniert und ob bei ihnen auch herkömmliche Ermittlungsverfahren ausreichen würden. Der Staat gerät in einen Konflikt, weil das Bundesamt für Sicherheit in der Informationstechnik die Aufgabe hat, die IT-Sicherheit im Land und bei jeder Privatperson zu erhöhen und die Online-Durchsuchung zum Ziel hat, ein System zu überwachen, möglicherweise durch die Installation eines Trojaners über Sicherheitslücken.

Die Etablierung einer IT-Infrastruktur zur Online-Durchsuchung muss stets gewartet werden. Sicherheitslücken im System würden die gesamte IT-Infrastruktur in Deutschland schwächen, sobald sich Unbefugte Zugang verschafften. Sensible Daten, die fälschlicherweise durch den Trojaner gesammelt und zentral abgelegt wurden, könnten die Tore zu Serversystemen der Wirtschaft öffnen.

Die Einrichtung des “E-Governments” zur Reduzierung von Behördengängen war kosten- und zeitintensiv. Mit Hilfe des E-Governments ist es beispielsweise möglich Steuererklärungen online zu machen ohne zum Finanzamt gehen zu müssen oder einen Brief mit den Unterlagen abzuschicken. Die Steuererklärung wird elektronisch übermittelt. Vor dem Hintergrund der Online-Durchsuchung nimmt das Vertrauen der Bürger in staatliche elektronische Kommunikation ab, sodass das E-Government an Bedeutung verliert.

Ein Bewusstseinswandel in der Bevölkerung könnte das Stimmungsbild in Deutschland verschlechtern. Das Gefühl, überwacht zu werden, erzeugt Misstrauen. Ein überwachter verhält sich oft anders als ein nicht überwachter Bürger. Das Misstrauen seitens der Bevölkerung alarmiert die Behörden und führt wiederum zu Misstrauen. Die Begrifflichkeit “Stasi 2.0” hat sich insbesondere in der Bloggerszene zu einem Schlagwort entwickelt, das das Unbehagen der Szene ausdrückt.

Abb. 1. “Stasi 2.0”

V. Rechtliche Grundlagen

A. Bundesebene

Die erste Online-Durchsuchung erfolgte bereits 2005 durch Geheimdienste. Die entsprechende Dienstvorschrift hatte der derzeitige Bundesinnenminister Otto Schily (SPD) abgezeichnet [7].

Die Zulässigkeit der Online-Durchsuchung zwecks Strafverfolgung war im Bundesgerichtshof zunächst umstritten. Am 21. Februar 2006 ordnete ein Ermittlungsrichter die Durchsuchung des PCs/Laptops eines Beschuldigten an. Die Strafprozessordnung zur Haus- und Wohnungsdurchsuchung galt als Grundlage dieser Entscheidung [8]. Am 25. November 2006 wurde ein weiterer Antrag des Generalbundesanwalts zur Durchführung einer Online-Durchsuchung durch einen anderen Ermittlungsrichter abgelehnt [9]. Seine Entscheidung beruhte darauf, dass die Online-Durchsuchung die Anwesenheit von Zeugen (vgl. §105 Abs. 2 StPO) und des Inhabers (vgl. §106 Abs. 1 StPO) des zu durchsuchenden Objekts erfordert. Eine heimliche Durchsuchung sei demnach nicht rechtsgültig.

Der Bundesgerichtshof erließ im Februar 2007 ein Verbot der Online-Durchsuchung aufgrund fehlender gesetzlicher Grundlagen.

Die geheimdienstliche Nutzung der Online-Durchsuchung ist umstritten. Nach Ansicht des Bundesinnenministeriums ist die heimliche Durchsuchung von PCs für den Verfassungsschutz, den Militärischen Abschirmdienst und den Bundesnachrichtendienst erlaubt.

Zur Beantwortung der Zulässigkeitsfrage im Bereich der Nachrichtendienste kann die Entscheidung des Bundesgerichtshofs vom Februar 2007 nicht ohne weiteres herangezogen werden. Diese bezieht sich allein auf die Rechtsgrundlagen der Strafverfolgung. Im Bereich der Gefahrenabwehr durch Geheimdienste gelten spezielle Eingriffsvorschriften.

B. Länderebene

Auf Länderebene ist die Online-Durchsuchung den Nachrichtendiensten vorbehalten, sofern das Recht einzelner Bundesländer Staatsorganen verdeckte Online-Durchsuchung erlaubt. Eine besondere Rolle spielt dabei Nordrhein-Westfalen. Dem Verfassungsschutz ist dort seit dem 30. Dezember 2006 der Zugriff auf informationstechnische Systeme zur Informationsbeschaffung erlaubt (vgl. §5 Abs. 2 Nr. 11 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen) [10]. Gegen diese Vorschrift wurde eine Verfassungsbeschwerde eingereicht. Die Entscheidung des Gerichts wird im Januar 2008 erwartet.

VI. Ausland

A. Österreich

In Österreich erfolgt die Diskussion um Online-Durchsuchung etwa zeitgleich wie in Deutschland. Der Fokus liegt dort allerdings auf dem Bereich Strafverfolgung. Eine Online-Fahndung soll bei Verbrechen eingesetzt werden dürfen, die zu einer Strafe von über 10 Jahren Gefängnis führen können. Ein richterlicher Beschluss ist notwendig zur Durchführung der Durchsuchung.

Ein Gesetz soll bereits bis Sommer 2008 beschlossen werden. Die technische Umsetzung ist noch unklar, wird aber aller Voraussicht nach auf einen Trojaner hinauslaufen [11].

B. Schweiz

In der Schweiz wird die Überwachung von Internettelefonie fokussiert. Ein “Polizeitrojaner” soll verschlüsselte VoIP-Kommunikation erfassen können, denn die Überwachung von VoIP-Servern erfasst weder verschlüsselte Gespräche noch Gespräche, die über eine Direktverbindung zweier Systeme laufen.

C. USA

In den USA wird seit 2001 durch die Bundespolizei FBI die Spionage-Software Magic Lantern eingesetzt, um Daten über das Internet mitzuschneiden. Dabei handelt es sich um einen Trojaner, der in erster Linie als Keylogger fungiert.

Im Jahr 2007 wurde erstmals ein Programm namens CIPAV (Computer and Internet Protocol Address Verifier) bestätigt. Dabei handelt es sich um einen Trojaner, der Festplatteninhalte ausspäht, benutzte und installierte Programme, Informationen über das Betriebssystem und Benutzerinformationen aus der

Windows Registry sammelt. Somit soll ein möglichst umfassendes Bild erzeugt werden, über welche Programme mit welchen IP-Adressen kommuniziert wird. Der Einsatz von CIPAV ist allerdings nur mit einem richterlichen Beschluss möglich.

VII. Mögliche technische Umsetzung

Das Ziel ist es, Daten vor der Verschlüsselung abzufangen. Da die Verschlüsselung auf dem System des Benutzers erfolgt, muss die Software zwangsläufig eine Art Trojanisches Pferd oder Rootkit sein, um auf Benutzerinteraktion mit dem System effektiv reagieren zu können.

Das größte Hindernis stellt die Verteilung der Software dar. Dafür gibt es verschiedene Möglichkeiten, die im Folgenden erläutert werden sollen:

A. Man-In-The-Middle Angriff

Über einen Man-In-The-Middle Angriff wird der Trojaner an andere Datenpakete, die der zu Überwachende anfordert, angehängt. Will dieser beispielsweise eine Datei herunterladen, so wird der Trojaner an den Download angehängt und kann somit an einer Firewall vorbeigeschleust werden. Automatische Updates von Betriebssystemen, Antivirensoftware, Firewallsoftware und sonstigen Programmen könnten ebenfalls als Träger für den Trojaner bei einem Man-In-The-Middle Angriff dienen. Die TKÜV (Telekommunikations-Überwachungsverordnung) ist eine Überwachungsschnittstelle, die jeder Internet Service Provider bereitstellen muss und beim Einschleusen des Trojaners behilflich sein kann.

Der Trojaner kann aber stets von Virenscannern erkannt werden oder auch manuell vom Überwachten, indem die Prüfziffer des abgeschlossenen Downloads mit der offiziellen Prüfziffer abgestimmt wird.

B. Kooperationen

Alternativ zum Man-In-The-Middle Angriff könnte auch die Kooperation mit Softwareherstellern zur Verteilung des Trojaners von Nutzen sein, insbesondere Hersteller von Betriebssystemen oder weit verbreiteten Antiviren-Programmen könnten eine Schnittstelle bereitstellen, die den Trojaner herunterlädt und auf dem System installiert.

Hier stellt sich das Problem, dass selbst die Kooperation mit einem Betriebssystemhersteller nicht zwangsläufig zum Erfolg führt, wenn der zu Überwachende ein angepasstes Betriebssystem verwendet, beispielsweise eine eigene Linux-Distribution.

C. E-Mail-Anhang

Die Versendung des Trojaners per E-Mail als Anhang ist eine weitere Möglichkeit zu dessen Verteilung. Eine möglichst personalisierte E-Mail soll den zu Überwachenden dazu bringen den Anhang zu öffnen, um den Trojaner unbemerkt zu installieren. Zu einer Zeit von Massenspammails erfordert diese Methode allerdings sehr gute Social Engineering Skills zusammen mit Hintergrundinformationen über das “Alltagsleben” des zu Überwachenden.

E-Mail-Anhänge werden allerdings ebenfalls von Virenscannern gescannt.

D. Manuelle Installation

Es bietet sich in manchen Fällen auch die manuelle Installation des Trojaners an, indem die Behörden in der Wohnung des zu Überwachenden die Software auf den Rechner spielen.

Das Hauptproblem hierbei besteht darin, dass ein Einbruch in die Wohnung des zu Überwachenden viel leichter bemerkt werden kann als ein Zugriff über das Internet. Die Beamten hätten außerdem mit passwortgeschützten Systemen und verschlüsselten Festplatten zu kämpfen.

E. Sicherheitslücken

Das Ausnutzen von Sicherheitslücken (Buffer-Overflows etc.) in verwendeter Software oder dem Betriebssystem des zu Überwachenden kann dabei helfen den Trojaner zu installieren. Dies käme einem “klassischen Hackerangriff” am nächsten.

Diese Methode ist zeitaufwändig und erfordert exzellentes technisches Know-how und führt dennoch nicht immer zum Erfolg.

Die technischen Möglichkeiten zur Verbreitung sind vielfältig und obwohl es möglich ist, jeden einzelnen Fall auf eine bestimmte Weise zu verhindern, könnte die Summe der Möglichkeiten dazu führen, dass ein effizienter Schutz vor der Installation kaum möglich ist. Oftmals ist es die Kombination verschiedener Methoden, die letztendlich zum Erfolg führt. Da sich die betroffenen Personen niemals vollständig sicher sein können, welche Methoden gerade auf sie angewandt werden, muss sie sich gegen sämtliche nur erdenklichen Methoden zu schützen wissen.

VIII. Effizienz

Obwohl das Thema Online-Durchsuchung, inbesondere die technische Umsetzung, zum gegenwärtigen Zeitpunkt eher spekulativer Natur ist, soll an dieser Stelle eine kurze Kosten-Nutzen Analyse aufgestellt werden.

A. Kosten

Zu den Kosten zählen zunächst die Änderungen an bestehenden Gesetzen. Davon ist das Grundgesetz betroffen, aber auch eine Vielzahl von weiteren Bundes- und Ländergesetzen. Der Trojaner selbst erfordert zwar nur eine einmalige Umsetzung und somit eine einmalige Investition, jedoch muss die Software an Sicherheitsupdates und Änderungen des Betriebssystems bzw. des Zielsystems angepasst werden. Im schlechtesten Fall stellt jeder Trojaner eine Art Individuallösung für das entsprechende Zielsystem dar. Damit verbunden ist auch die Wartung der Sicherheit der gesamten Überwachungs-Infrastruktur. Diese muss ständig überprüft und verbessert werden, um Angreifer vom System fernzuhalten und Missbrauch vorzubeugen.

Zur Verwendung der Software muss Personal geschult werden. Es müssen gegebenenfalls Kooperationen mit Softwareherstellern eingegangen oder Man-In-The-Middle Angriffe geplant werden. Eine Marketing-Kampagne zur Stärkung des Vertrauens der Bürger in das System würde ebenfalls Kosten verursachen.

Einkalkuliert werden müssen auch die Kosten, die ein Informationsverlust durch eine Sicherheitslücke nach sich zieht. Ein solcher Informationsverlust könnte dazu führen, dass ein terroristischer Anschlag zu einem bestimmten Prozentsatz weniger verhindert werden kann.

Zu den Kosten zählt auch menschliches Versagen. Es muss einkalkuliert werden, dass möglicherweise ein Fehler gemacht wird, beispielsweise beim Einschleusen des Trojaners über einen E-Mail-Anhang, was sehr stark von den Social Engineering Fähigkeiten des ausführenden Beamten abhängt. Ein Missgeschick an dieser Stelle könnte die Wachsamkeit eines Verdächtigen erhöhen, sodass auch in diesem Fall die Wahrscheinlichkeit der Anschlagsverhinderung sinkt.

B. Nutzen

Die Möglichkeiten der Online-Durchsuchung sind zwar vielfältig, allerdings kristallisiert sich inbesondere das Ziel heraus, Daten vor der Verschlüsselung mitzuschneiden. In Ergänzung der Vorratsdatenspeicherung ist die Online-Durchsuchung ein hervorragendes Werkzeug zur Überwachung.

In Zeiten von Internet, verschlüsselten Verbindungen und dezentralisierten Daten auf ausländischen Servern könnten bisherige Ermittlungsverfahren zu langsam sein oder scheitern, was in letzter Konsequenz Menschenleben fordern kann. Die Online-Durchsuchung könnte dabei helfen, mit der technischen Entwicklung Schritt zu halten, um Ermittlungsprozesse flexibel zu halten und Menschenleben zu schützen.

Das Vertrauen von Terroristen in Verschlüsselung kann dabei helfen an wirklich relevante Informationen zu kommen. Bei allem Schutz, den Anonymisierung und Verschlüsselung bieten, nimmt auch das Vertrauen in die Technik zu. Möglicherweise lassen sich ganze Terrorzellen oder -netzwerke aufdecken, obwohl nur einige wenige Verdächtige überwacht werden.

Geheimdienste haben die Aufgabe, Gefahren frühzeitig zu erkennen. Online-Durchsuchung könnte die Prävention von Straftaten verbessern. Ein Anschlag, vielleicht sogar nuklearer oder biologischer Natur, könnte hunderttausende Menschenleben fordern, der mit Online-Durchsuchung möglicherweise verhindert werden kann.

IX. Aktuelle Entwicklung

Der Chaos Computer Club (CCC), dessen Mitglieder als Sicherheitsexperten und Datenschützer gelten, veröffentlichte im August 2007 einen heftig umstrittenen Gesetzesentwurf [12] zur Online-Durchsuchung und schreibt über die Online-Durchsuchung:“Wenn das BKA-Gesetz in der vorliegenden Fassung verabschiedet wird, entsteht de facto eine Geheimpolizei, wie sie in Deutschland zuletzt in der DDR existierte”. Er plädiert dafür, dass das Trennungsgebot von Polizei und Geheimdiensten nicht weiter ausgehöhlt werden darf [13].

Unter dem Trennungsgebot versteht man die Trennung der Befugnisse von Polizei und Geheimdienst, um der Bildung eines Geheimpolizeiapparates vorzubeugen. So dürfen deutsche Geheimdienste keine polizeilichen Maßnahmen gegenüber Bürgern treffen und so weiter (siehe §8 III BVerfSchG, §2 III BNDG, §4 II MAD-Gesetz).

Laut dem Präsidenten des BKA Jörg Ziercke ist es keine Frage des “Ob”, sondern eine Frage des “Wie”, denn seiner Meinung nach gibt es keine Alternative zur Online-Durchsuchung [1]. Die Entwicklung des Bundestrojaners war aufgrund des Urteils des Bundesgerichtshofs vom Februar 2007 über den Sommer 2007 auf Eis gelegt worden. Bundesinnenminister Schäuble lässt den Trojaner nun weiterentwickeln.

Sowohl die SPD als auch das Innenministerium plädieren für eine Erweiterung des Grundrechtsschutzes auf das Internet. Dabei sollen der Online-Durchsuchung jedoch keine Steine in den Weg gelegt werden [14].

Die Entscheidung des Bundesverfassungsgerichts zur Rechtmäßigkeit des Verfassungseintrags zur Online-Durchsuchung in Nordrhein-Westfalen, die für Januar 2008 angesetzt ist, wird das weitere Vorgehen Schäubles entscheidend beeinflussen [15].

X. Fazit

Online-Durchsuchung ist ein wichtiges Thema. Auf der einen Seite steht der Staat, der den Auftrag hat, seine Bürger zu schützen. Das 21. Jahrhundert stellt neue Anforderungen sowohl an technische Systeme, um diese Aufgabe zu erfüllen, als auch an die dazugehörigen rechtlichen Grundlagen. Das Internet kennt kaum internationale Grenzen, die derzeitige Rechtsprechung berücksichtigt diese Grenzen allerdings sehr stark. Um Zugriff auf Daten auf ausländischen Servern zu erhalten, sind langwierige bürokratische Prozesse vonnöten. Die Diskrepanz zwischen Recht und Technik ist nicht zu übersehen und erfordert eine Neuorientierung.

Auf der anderen Seite steht die Freiheit eines jeden einzelnen Bürgers. Die oft gestellte Frage “Welche Freiheit wollen wir noch schützen, wenn wir jegliche Freiheit der Überwachung aufgeopfert haben?” spiegelt das Stimmungsbild der Bevölkerung wider und stellt in erster Linie die Art und Weise der Neuorientierung des Rechts an der Technik in Frage. Die Etablierung einer freiheitsorientierten Demokratie wird durch die Einführung einer scheinbar willkürlichen Überwachung in Frage gestellt. Auch wenn zunächst die Rede davon ist, dass Online-Durchsuchung nur durch richterlichen Beschluss in Einzelfällen ermöglicht werden soll, so kennt man bereits aus dem Bereich Mobilfunküberwachung eine ganz andere Entwicklung. Anstelle von Einzelfällen entwickeln sich mit

der Zeit immer weitreichendere Abhör- und Überwachungsmechanismen — es scheint sich eine gewisse Willkür einzuschleichen.

Was in der Theorie vielversprechend klingt, sieht in der Realität oftmals ganz anders aus. Die kaum vorhandene Transparenz seitens offizieller Stellen trägt ein Übriges dazu bei. Aussagen wie "Es kann nicht sein in einem Rechtsstaat, dass Menschen schwerste Straftaten im Internet vorbereiten durch das Herunterladen von Bombenbauanleitungen [...]" von BKA-Chef Jörg Ziercke [10] lassen die Frage nach dem Nutzen der Online-Durchsuchung aufkommen und stellen die oben bereits beschriebene Verhältnismäßigkeit in Frage.

Ob die Online-Durchsuchung eine Verbesserung der Ermittlungsmethoden nach sich zieht, bleibt offen. Tatsache ist jedoch, dass eine einmal etablierte Überwachungsfunktion nicht mehr abgeschafft wird, selbst wenn sie keine Effizienzsteigerung mit sich bringt. Darüber hinaus besteht für die Bevölkerung das Risiko, dass Überwachungsfunktionalitäten mit der Zeit verändert werden. Vertreter der Musikindustrie möchten beispielsweise die Vorratsdatenspeicherung, die zur Verbrechensaufklärung gedacht ist, dazu nutzen, kleinere Vergehen, wie das illegale Herunterladen von Musik, zu verfolgen. Eine ähnliche Forderung könnte sich auch bei der Online-Durchsuchung ergeben, sodass die einmal etablierten Überwachungsstrukturen für ganz andere Zwecke verwendet werden, was eine Abschaffung zusätzlich erschwert.

Der Schritt in Richtung Online-Durchsuchung ist ein großer Schritt und will wohlüberlegt sein, denn er zieht weitreichende Veränderungen nach sich, die möglicherweise gar nicht benötigt werden. Eine Verbesserung der bisherigen Ermittlungsmethoden könnte bereits eine Effizienzsteigerung in Ermittlungsverfahren mit sich bringen und sowohl der Bevölkerung als auch dem Staat viel mehr nützen, als eine Online-Durchsuchung dies zum gegenwärtigen Zeitpunkt erreichen könnte, denn es passieren zum gegenwärtigen Zeitpunkt immer wieder Pannen bei den bereits vorhandenen Ermittlungsverfahren [16].

LITERATUR

[1] Detlef Borchers, "BKA-Chef: Zur Online-Durchsuchung gibt es keine Alternative," 15.11.07. [Online]. Available: {http://www.heise.de/newsticker/meldung/99034}

[2] Konrad Lischka, "Bundes-Trojaner sind spähbereit," 28.08.07. [Online]. Available: {http://www.spiegel.de/netzwelt/web/0,1518,502542,00.html}

[3] DPA , "Merk: Online-Durchsuchung im Kampf gegen Kinderpornografie nötig," 26.07.07. [Online]. Available: {http://www.heise.de/newsticker/meldung/93364}

[4] Bundesrepublik Deutschland, "Grundgesetz." [Online]. Available: {http://www.bundestag.de/parlament/funktion/gesetze/grundgesetz/gg_01.html}

[5] , "." [Online]. Available: {http://www.disc-gmbh.com/Strafverfolgung__Verfassungsschutz.vm06.0.html?&L=1}

[6] Andreas Förster, "Beamter unter Verdacht," 31.08.07. [Online]. Available: {http://www.berlinonline.de/berliner-zeitung/archiv/.bin/dump.fcgi/2007/0831/politik/0062/index.html}

[7] DPA, "Geheimdienste spitzeln schon seit Jahren," 25.04.07. [Online]. Available: {http://www.stern.de/computer-technik/internet/587865.html?nv=ct_mt}

[8] Bundesgerichtshof , "Erlaubnis zur Online-Durchsuchung, 21. Februar 2006." [Online]. Available: {http://www.hrr-strafrecht.de/hrr/3/06/3-bgs-31-06.php}

[9] Bundesgerichtshof, "Verbot der Online-Durchsuchung, 25. November 2006." [Online]. Available: {http://www.hrr-strafrecht.de/hrr/1/06/1-bgs-184-2006.php}

[10] Fredrik Roggan, "Privatsphöre muss vor heimlichen Online-Durchsuchungen geschützt bleiben!" 09.02.07. [Online]. Available: {http://www.humanistische-union.de/aktuelles/presse/pressedetail/back/aktuelles/article/privatsphaere-muss-vor-heimlichen-online-durchsuchungen-geschuetzt-bleiben/}

[11] ORF Österreich, "Skeptiker nicht überzeugt," 17.10.07. [Online]. Available: {http://orf.at/071017-17734/index.html}

[12] Bundesregierung, "Gesetzesentwurf zur Gefahrenabwehr." [Online]. Available: {https://www.ccc.de/lobbying/papers/terrorlaws/20070711-BKATERROR.pdf}

[13] Stefan Krempl , "CCC veröffentlicht umkämpften Gesetz-Entwurf zu Online-Durchsuchungen," 31.08.07. [Online]. Available: {http://www.heise.de/newsticker/meldung/95269}

[14] Stefan Krempl, "Schäuble lässt Bundestrojaner weiterentwickeln," 17.11.07. [Online]. Available: {http://www.heise.de/newsticker/meldung/99150}

[15] Stefan Krempl , "Schäuble schaltet bei Online-Razzien einen Gang zurück," 14.12.07. [Online]. Available: {http://www.heise.de/newsticker/meldung/100624}

[16] Detlef Borchers, "Heimliche Online-Durchsuchung: Eine stumpfe polizeiliche Waffe?" 12.12.07. [Online]. Available: {http://www.heise.de/newsticker/meldung/100441}