Friedrich-Schiller-Universität Jena, Fakultät für Mathematik und Informatik

Proseminar Totale Überwachung

Der Bundestrojaner

Jens Kubieziel
<jens@kubieziel.de>

Die vorliegende Arbeit beschreibt verschiedene Gesichtspunkte der geplanten heimlichen Online-Durchsuchung, besser bekannt unter der Bezeichnung „Bundestrojaner“, unter verschiedenen Gesichtspunkten. Die verschiedenen Bezeichnungen werden definiert und Eingriffs- sowie Schutzmöglichkeiten diskutiert. Im Weiteren ist eine kurze rechtliche Bewertung sowie ein Überblick über die Situation in anderen Ländern zu finden. Im letzten Kapitel erläutert der Autor seine Ansicht zur Thematik.

Inhaltsverzeichnis

Abkürzungsverzeichnis

BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BKAG-E	Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
FDP	Freie Demokratische Partei
GG	Grundgesetz
ISP	Internet Service Provider
NRW	Nordrhein-Westfalen
NSA	National Security Agency
PC	Personal Computer
RAM	Random Access Memory
RFS	Remote Forensic Software
SIP	Session Initiation Protocol
STPO	Strafprozessordnung
TKÜ	Telekommunikationsüberwachung
TPM	Trusted Platform Module
VDS	Vorratsdatenspeicherung
VSG	Verfassungsschutzgesetz
VoIP	Voice over IP

1 Einleitung

Als Eris, die Göttin der Zwietracht, vor mehr als 3 000 Jahren mit den Zankapfel indirekt den Trojanischen Krieg auslöste, war ihr sicher nicht bewusst, welche Nachwirkungen das haben sollte.

Eris, beleidigt, weil sich nicht zu Peleus' und Thetis' Hochzeit eingeladen wurde, warf den goldenen Apfel der Zwietracht unter die Gäste. Die Inschrift „Der Schönsten“ (Kallisti, $\kappa\alpha\lambda\lambda\iota\sigma\tau\eta$) führte zum Streit zwischen Aphrodite, Athene und Hera. Erst das Urteil des Paris sollte klären, wer die Schönste sei. Aphrodite gewann die Wahl durch eine List, indem sie Paris versprach, mit der schönen Helena zusammenzukommen.

Diese List hatte Folgen. Helena war verheiratet und wurde von Paris entführt. Helenas Gatte zog mit seinen Gefolgsleuten in den Krieg gegen Troja. Erst zehn Jahre später gab es eine unerwartete Lösung für den Konflikt. Odysseus ersann eine List. Offensichtlich gab er die Belagerung auf und hinterließ ein riesiges hölzernes Pferd. Die Trojaner nahmen es mit in ihre Stadt und begannen eine Siegesfeier. Im Pferd waren jedoch Griechen verborgen. Dieses öffneten die Stadttore und auf diese Weise wurde der Krieg für die Griechen gewonnen.

Noch heute ist das Wort „Trojanisches Pferd“ in aller Welt bekannt und hat insbesondere im IT-Sektor neue Bedeutungen gefunden. Es bezeichnet Anwendungen, die nach gleichem Prinzip wie sein Namensgeber funktionieren. Scheinbar nützliche Programme werden zur Installation angeboten und danach entfalten sie ihre volle Wirksamkeit, indem sie weitere, meist unerwünschte Funktionen aktivieren. Dertige Trojaner dienen meist zur Verbreitung von Computerviren.

Eine besondere Art soll im Rahmen dieser Betrachtungen genauer untersucht werden: der so genannte Bundestrojaner. Dies ist ein Programm, welches von staatlicher Seite auf Computersysteme installiert werden und dort zur Verbrechensaufklärung dienen soll. Die vom Bundeskriminalamt (BKA) gewählte Bezeichnung für diese Software ist Remote Forensic Software (RFS) oder als Verfahren auch heimliche Online-Durchsuchung.

Im Rahmen der Untersuchungen wird zunächst ein Überblick über die verwendeten Begriffe gegeben und eine einheitliche Definition dieser versucht. Die folgenden Abschnitte diskutieren verschiedene Möglichkeiten der Umsetzung sowie des Schutzes gegen die Maßnahmen von seiten der Benutzer. Das Ziel der weiteren Betrachtungen ist auch ein Überblick über die rechtliche Situation. Insbesondere wie sich die Maßnahme in die bisherigen Gesetze einbettet. Der letzte Abschnitt gibt die Meinung des Autors zu den Maßnahmen wieder.

2 Definition der Begriffe

Im Verfassungsschutzgesetz (VSG) des Landes Nordrhein-Westfalen (NRW) wurde 2006 erstmals eine Gesetzesnorm zur heimlichen Online-Durchsuchung definiert. Das Gesetz erlaubt den heimlichen Zugriff auf informationstechnische Systeme mit dem Einsatz technischer Mittel. Seither werden diese Maßnahmen kontrovers in den Medien und der Bevölkerung diskutiert und im Verlauf der Diskussion entstanden viele Bezeichnun-

gen. Zu Beginn der Abhandlung sollen diese Begrifflichkeiten geklärt und für die weitere Arbeit definiert werden.

2.1 Informationstechnische Systeme

Das VSG[18] sowie diverse Veröffentlichungen des Bundes sprechen von informationstechnischen Systemen. Dieser Begriff beinhaltet nicht nur Personal Computer (PC) oder Server, sondern *alle* Systeme, die aus Hard- und Software bestehen und Daten auf irgendeine Weise be- oder verarbeiten[3]. Dies bedeutet, dass von der Regelung Mobiltelefone, digitale Anrufbeantworter, Faxgeräte etc. betroffen sind. In der Verhandlung zur Verfassungsbeschwerde gegen die Online-Durchsuchung im VSG NRW wies Prof. Dr. Andreas Pfitzmann vom Lehrstuhl für Datenschutz und Datensicherheit an der TU Dresden darauf hin, dass die Gesetzesnorm auch Geräte wie Herzschrittmacher, Hörhilfen und weitere, innerhalb des Körpers angebrachte Gegenstände umfasst[11].

Den Angaben aus dem Fragenkatalog des Bundesministerium der Justiz (BMJ) zufolge sollen jedoch keine Server, Faxgeräte oder Anrufbeantworter Gegenstand der heimlichen Online-Durchsuchung sein. Bei Servern oder anderen nicht unter der Kontrolle eines Verdächtigen stehenden Systemen ist geplant, sich an den jeweiligen Betreiber bzw. Administrator zu wenden, um die fraglichen Daten zu gewinnen. Faxgeräte und Anrufbeantworter sollen Gegenstand einer Telekommunikationsüberwachung sein und daher in gesonderten Maßnahmen überwacht werden.

2.2 Heimliche Online-Überwachung oder heimliche Online-Durchsuchung

Der Begriff der heimlichen Online-Überwachung kommt in der breiten Diskussion recht selten zum Einsatz. Vielmehr wird von der Online-Durchsuchung oder vom Bundestrojaner gesprochen. Nach der Einschätzung des Autors handelt es sich hierbei jedoch um die allgemeinste und zutreffenste Beschreibung des Sachverhaltes. Die Maßnahme soll immer heimlich, ohne Mitwissen des Anwenders bzw. Verdächtigen durchgeführt werden. Der Zugriff auf das informationstechnische System erfolgt online. Eine Überwachung schließt in diesem Szenario die Durchsicht mit ein. Insofern wäre der Begriff „Online-Überwachung“ eine passendere Formulierung.

Im Recht (siehe StPO [15, §§ 102–110]) wird zumeist zwischen der Überwachung und der Durchsuchung von Personen unterschieden. Ersteres kennzeichnet eine längerfristige Maßnahme, bei der verschiedene Werkzeuge zum Einsatz kommen können. Ähnlich ist dies bei der heimlichen Online-Überwachung zu sehen. Sie ist als ein Mittel geplant, informationstechnische Systeme von Verdächtigen über einen langen Zeitraum zu observieren.

2.3 Heimliche Online-Durchsicht

Die heimliche Online-Durchsicht ist ein Spezialfall der heimlichen Online-Überwachung. Hierbei handelt es sich um einen einmaligen Zugriff. Mit diesem soll ermittelt werden,

was der Verdächtige mit seinem Rechner in der Vergangenheit gemacht hat. Im Rahmen der Durchsicht ist geplant, das informationstechnische System nach den folgenden Informationen zu durchforsten[3]:

- Informationen über die eingesetzte Soft- und Hardware
- gespeicherte Dateien nach Namen, Dateiendungen, -attributen und -typ
- Suche nach Schlüsselworten

2.4 Remote Forensic Software

Die RFS ist die interne Bezeichnung des BKA für die softwareseitige Umsetzung der heimlichen Online-Überwachung. Sie stellt eine speziell angefertigte Software dar, die die Überwachungsmaßnahmen übernimmt. Der Wortbestandteil „Forensic“ legt die Vermutung nahe, dass es sich um eine computerforensische Maßnahme handelt. Der Beweiswert der gewonnenen Daten ist jedoch sehr begrenzt und reicht nicht an den von im Rahmen computerforensisch ermittelten Daten heran. Denn u. a. ist eine wesentliche Anforderung, dass die Daten von einem dritten unabhängigen Gutachter auf dieselbe Weise erlangt werden können, wie es beim Erstzugriff geschah. In der Regel ändern sich die Umgebungen eines informationstechnischen Systems laufend und somit ist ein gleichlautender Weg nahezu unmöglich. Es ist zu vermuten, dass statt des Begriffs „Bundestrojaner“ hier ein neutrales und nicht negativ besetztes Wort etabliert werden soll.

2.5 Quellen-Telekommunikationsüberwachung

In Abgrenzung zur RFS wurde die Quellen-Telekommunikationsüberwachung (TKÜ) als weiterer Begriff vom BMI festgelegt[3]. Durch die RFS soll angabegemäß keine Telekommunikation überwacht werden. Dies bedeutet, weder digitale Telekommunikationsgeräte sind Ziel der Online-Überwachung noch erfolgt eine Belauschung von Ferngesprächen an PCs. Der Leser denke hier an Telefonie per Session Initiation Protocol (SIP) oder Voice over IP (VoIP) (Skype). Diese Vorgänge werden von der Quellen-TKÜ erfasst.

Nach der Antwort der Bundesregierung auf eine Kleine Anfrage der Freie Demokratische Partei (FDP) beginnt die Telekommunikation jedoch erst nach der unumkehrbaren Einleitung des Übermittlungsvorgangs[4]. Also unterliegt alles, was zuvor auf dem Rechner bearbeitet oder gespeichert wird, der Überwachung durch die RFS.

2.6 Bundestrojaner oder Computerwanze

Schließlich kursieren diverse Begriffe, die auf umgangssprachliche Art und Weise die heimliche Online-Überwachung charakterisieren. Am häufigsten ist Bundestrojaner[1] zu hören. Diese Wortschöpfung spielt auf das trojanische Pferd aus der griechischen Mythologie an. Es bezeichnet ein Programm, welches vordergründig eine nützliche Funktion

[1] Entstammt wahrscheinlich einem Interview des Radiosenders Deutschlandfunk mit Manfred Kloiber, siehe hierzu `http://www.dradio.de/dlf/sendungen/forschak/590376/`

bringt. Diesselbe Software macht aber im Hintergrund und ohne das Wissen des Anwenders andere, in der Regel unerwünschte Aktionen. Der Bundestrojaner ist eine derartige Software, die vom Staat, also vom Bund, betrieben wird.

Computerwanze ist ein weiteres, seltener gebrauchtes Wort, als Umschreibung für die RFS. Damit kann die eventuelle Schadwirkung auch dem Teil der Bevölkerung nahe gebracht werden, die keine Affinität zu Computersystemen besitzt. Denn sowohl das Wort Computer wie auch die Wanze sind allseits bekannt. Eine Wanze bezeichnet sowohl ein Tier, dass mehrheitlich als Schädling auftritt, als auch eine Vorrichtung, die zum Abhören installiert wird. Früher wurden auch unangenehme Personen als Wanzen bezeichnet.

Mit beiden Begriffen soll die negative Konnotation transportiert werden. Nach der Meinung des Autors ist das in der bisherigen Situation gelungen.

3 Umsetzung der Maßnahmen

Dieses Kapitel diskutiert mögliche Realisierungen der heimlichen Online-Überwachung. Bisher gibt es kaum offizielle Verlautbarungen über die Art und Weise der geplanten Maßnahmen. In den Fragekatalogen des BMI ([3] und [2]), im Artikel in der Zeitschrift DuD – Datenschutz und Datensicherheit – von Prof. Dr. Hartmut Pohl[12] sowie in den Gutachten für das Bundesverfassungsgericht (BVerfG) werden verschiedene Möglichkeiten genannt. Im folgenden sollen diese vorgestellt werden.

3.1 Anforderungen an die heimliche Online-Durchsuchung

Die Vorgehensweise bei der heimlichen Online-Überwachung ist mit der der heimlichen Online-Durchsicht weitgehend identisch. Die untenstehenden Betrachtungen machen daher keinen Unterschied zwischen beiden Verfahren. Die Online-Durchsicht soll als aufklärende Maßnahme folgende Informationen erheben:

- Informationen über das Zielsystem
  - verwendetes Betriebssystem (Version, Patchlevel etc.)
  - Art des Internet-Zugangs
  - installierte Schutz-Software (Virenscanner, Paketfilter, Einsatz von Verschlüsselungsprogrammen etc.)
  - genutzte Software auf dem Zielsystem (E-Mail-Software, Browserversion etc.)
- Informationen zu den gespeicherten Dateien
  - Name
  - Dateiendung
  - Dateiattribute
  - Dateityp
- Suche nach Schlüsselworten

Zusätzlich dazu erfasst die Online-Überwachung noch:

- flüchtige Daten (Dateien in Bearbeitung, Eingaben über Tastatur, im Random Access Memory (RAM) befindliche Informationen etc.)
- Klartext vor *Ver*schlüsselung und nach *Ent*schlüsselung

Somit ist zu sehen, dass die Maßnahmen der heimlichen Online-Überwachung eine Obermenge der Maßnahmen der heimlichen Online-Durchsicht sind.

In den bisherigen Veröffentlichungen wird ausschließlich eine softwareseitige Überwachung beschrieben. Im Rahmen dieses Abschnittes zu den Anforderungen werden daher auch nur diese Maßnahmen diskutiert. Die folgenden Abschnitte beleuchten auch andere mögliche Maßnahmen.

Vor der Aufbringung auf das System eines Verdächtigen steht die Analyse. Es müssen diverse Angaben zur Soft- und Hardware vorhanden sein, wie auch Informationen zum Verhalten des Nutzers. Dazu gehören insbesondere die Art und die Häufigkeit der Internetnutzung. Angaben zur Software lassen sich mit Port- oder Fingerprintscannern ermitteln. Derartige Programme versuchen, Computersysteme zu testen und Programme mit Versionsnummern zu identifizieren. Je nach Programm und Kenntnisstand der Zielperson kann diese Angabe unvollständig oder verfälscht sein. Falls mobile Geräte benutzt werden, wäre der „Blick über die Schulter“ eine weitere Variante zur Aufklärung oder zur Bestätigung von Vermutungen.

Vielversprechend ist eine Befragung des Internet Service Provider (ISP). Diesem liegen die Daten zur Nutzung des Internetanschlusses spätestens mit der Umsetzung der Regelungen zur Vorratsdatenspeicherung (VDS) vor. Gerade zur Ermittlung des Nutzerverhaltens sind diese von unschätzbarem Vorteil. Weitere Erkenntnisse können über klassische Observationen oder Auskünfte bei Behörden gewonnen werden.

Nach der Auskundschaftung sowie der Anpassung an das Zielsystem muss die Software installiert werden. Die Installation kann manuell oder automatisch erfolgen. Diese Varianten werden im Abschnitt 3.4 detailliert besprochen.

3.2 TEMPEST

Als TEMPEST oder auch Van-Eck-Phreaking bezeichnet man die Aufnahme oder Wiederkenntlichmachung der Abstrahlung elektronischer Geräte. Der Begriff TEMPEST ist der Deckname eines Programms der National Security Agency (NSA)[2]. Die öffentliche Forschung auf dem Gebiet setzte 1985 ein. Der niederländische Forscher Wim van Eck beschrieb die Abstahlungen in einer Veröffentlichung[16] und warnte darin auch vor möglichen Folgen.

Anfang des Jahres 2008 veröffentlichte die NSA mehrere Dokumente, die bis dahin der Geheimhaltung unterlagen. Eines, „TEMPEST: A Signal Problem“[10], geht u. a. auf die Geschichte ein. Demnach liegen die Anfänge bereits zu Zeiten des Zweiten Weltkrieges. Die Armee nutzte Maschinen der Bell Labs zur Verschlüsselung der Nachrichten. In

[2] amerikanischer Inlandsgeheimdienst

Laborversuchen entdeckten die Ingenieure, dass der Oszillograph spezifische Ausschläge zeigte und sie konnten später bei einer Demonstration des Problems einen Großteil der unverschlüsselten Nachrichten wieder gewinnen:

> Bell Telephone faced a dilemma. They had sold the equipment to the military with the assurance that it was secure, but it wasn't. The only thing they could do was to tell the Signal Corps about it, which they did. There they met the charter members of a club of skeptics who could not believe that these tiny pips could really be exploited under practical field conditions. They are alleged to have said something like: „Don't you realize there's a war on? We can't bring our cryptographic operations to a screeching halt based on a dubious and esoteric laboratory phenomenon. If this is really dangerous, prove it." So, the Bell engineers were placed in a building on Varick Street in New York. Across the street and about 80 feet away was Signal Corps' Varick Street cryptocenter. The engineers recorded signals for about an hour. Three or four hours later, they produced about 75 % of the plain text that was being processed–a fast performance, by the way, that has rarely been equalled.

Mittels des Van-Eck-Phreaking versucht man die Strahlung von Monitoren auszulesen und das Monitorbild wiederherzustellen. Zuletzt erlangten die Methoden öffentliches Gehör, als Wahlcomputer von privaten Forschern untersucht worden. Dabei stellten diese fest, dass die Wahlcomputer über größere Entfernungen Strahlungen emittieren und diese relativ einfach auszulesen sind[3]. Dies ist insofern bedenklich, als das damit das Wahlgeheimnis deutlich eingeschränkt oder sogar zunichte gemacht werden könnte. Mit derartigen Wahlcomputern wäre es denkbar, dass Wähler erpresst werden, bestimmte Parteien zu wählen und das Ergebnis kann dann vom Erpresser „geprüft" werden.

Diese Methoden können angewendet werden, um den Bildschirm eines Verdächtigen zu betrachten und seine Arbeit zu verfolgen. Der Vorteil liegt insbesondere darin, dass es sich um Leseoperationen handelt und kein Zugriff auf das informationstechnische System direkt erfolgt. Im Falle einer gerichtlichen Verwertung könnten die gewonnenen Informationen zweifelsfrei verwendet werden. Dies ist bei einem Lese- und Schreibzugriff auf das System wahrscheinlich nicht gegeben.

Eine weitere, weniger exotisch anmutende Variante ist das Auslesen von drahtlosen Eingabegeräten. Funk- und Bluetoothtastaturen übertragen die Tastenanschläge an ein Empfangsgerät. Das wandelt die Signale um und gibt sie an die Hardware weiter. Ein weiterer Empfänger könnte ebenfalls die Signale empfangen und daraus jeden Tastendruck rekonstruieren. Hierfür ist meist relative Nähe zum Sender erforderlich. Denn viele Geräte überbrücken nur Distanzen von unter 10 m.

3.3 Hardware

Die Sicherheit eines informationstechnischen Systems hängt sowohl von der Sicherheit der Hard- wie auch von der der Software ab. In den meisten Veröffentlichungen

[3] Informationen auf den Seiten der Initiative „Wij vertrouwen stemcomputers niet" und bei `http://www.youtube.com/watch?v=B05wPomCjEY`

wird jedoch mehr auf die Software abgestellt. Einige Forschungsarbeiten weisen darauf hin, dass es mit entsprechend modifizierter Hardware recht einfach ist, auch Software in vertrauenswürdiger Umgebung zu täuschen. Beispielhaft sei hier die Rückgewinnung kryptografischer Schlüssel aus dem RAM eines ausgeschaltenen Rechners[8] oder die Einbringung von Hardware zur Errichtung eines verdeckten Informationskanals („JitterBug“)[6] genannt. Daher ist anzunehmen, dass die Möglichkeiten weit über das unten beschriebene Maß hinaus reichen.

Die wohl am häufigsten genutzten Variante, um über Manipulationen der Hardware, an Informationen zu gelangen, besteht in der Einbringung eines so genannten Keyloggers[4]. Dies ist ein Bauteil, welches alle Tastatureingaben aufzeichnet. Mit den Aufzeichnungen kann später jede Eingabe rekonstruiert werden. Die momentan kommerziell erhältlichen Keylogger steckt man als Modul vor den PS2-/USB-Anschluss oder tauscht das Originalkabel gegen ein manipuliertes. Schwerer erkennbare Geräte sind direkt in die Tastatur eingebaut. Nach den Angaben verschiedener Hersteller speichert ein Standardgerät eine halbe bis eine Million Anschläge. Etwa 300 Anschläge pro Minute gab ein Personalberater im persönlichen Gespräch als guten Wert für eine Schreibkraft an. Wenn diese Person pro achtstündigem Arbeitstag ununterbrochen schreibt, reicht die Kapazität demnach für mehr als drei Arbeitstage. In der Praxis reicht der Speicher sicher wesentlich länger.

Grundsätzlich könnte die Einbringung eines Keyloggers eine Methode zur Aufklärung sein. Hierdurch erhält man mit hoher Wahrscheinlichkeit relevante Login-Daten und kann später eine manipulierte Software auf das System spielen. Die gesammelten Informationen beinhalten eventuell auch Benutzernamen sowie Passworte für andere Zugänge (E-Mail, Online-Chats etc.). Falls der Verdächtige Verschlüsselung einsetzt, gewinnt man mittels eines Keyloggers auch diese Zugangsdaten und kann diese später im Rahmen einer Beschlagnahmung zur Gewinnung des Klartextes einsetzen.

3.4 Software

Der größte Anteil an bisherigen Veröffentlichungen und wahrscheinlich auch die ersten Realisierungen beziehen sich auf eine zu installierende Software. Die bisher durchgeführten Maßnahmen aus [17] und [13] basierten ebenfalls auf softwareseitigen Lösungen.

In Abschnitt 3.1 wurden bereits diverse Anforderungen an die RFS und die Auskundschaftung der Systeme vorgestellt. Nunmehr muss die Software auf den PC aufgebracht werden. Im Allgemeinen kann das direkt über eine manuelle Installation oder auf dem automatischen Weg erfolgen.

3.4.1 Manuelle Installation

Manuelle Installation bedeutet sowohl, dass der Ermittlungsbeamte direkt am betreffenden System sitzt und die Software aufbringt, wie auch, dass über eine Online-Verbindung installiert wird.

[4] wird teils auch als Software eingesetzt

Der erste Weg ist der erfolgversprechendste. Hier hat der Beamte direkten Zugriff auf das System und kann die Funktionen nach Abschluss der Installation testen. Nach der Einigung über das BKA-Gesetz[1] ist es nicht erlaubt, in die Wohnung eines Verdächtigen einzubrechen, um den Trojaner zu installieren. Wenn bekannt ist, das die Person fremde Hilfe bei Problemen mit seiner Infrastruktur benötigt, könnte versucht werden, Fehler am Rechner vorzutäuschen und so den Rechner in die Hände einer dritten Person zu geben. Dabei ergeben sich unter Umständen Möglichkeiten, direkten Zugriff zu erlangen. Weiterhin könnten mobile Geräte „geliehen“ werden, um die Installation vorzunehmen. Das bedeutet, dass es trotz des gesetzlichen Verbotes, in die Räume des Betroffenen einzudringen, denkbare Varianten für eine manuelle Installation gibt.

Ein zweiter gangbarer Weg ist die Installation über eine entfernte Verbindung zum System. Hierbei nutzt man eine Schwachstelle in der Software aus, um weitergehende Rechte (Vollzugriff auf das System) zu erhalten. Ausgestattet mit diesen Rechten kann nun Software nach Belieben installiert werden. Pohl diskutiert in [12] die Möglichkeit, so genannte (Less-than)-Zero-Day-Exploits einzusetzen. Damit werden Sicherheitslücken bezeichnet, die bisher nicht veröffentlicht sind und für die es somit keine Korrekturen (Patch) gibt. Das System ist dem Angriff ungeschützt ausgesetzt und die entfernte Installation verläuft erfolgreich.

Falls beide Varianten nicht machbar sind, muss zu einer automatischen Installation gegriffen werden.

3.4.2 Automatische Installation

Die automatische Installation kommt dem Prinzip des in der Einleitung beschriebenen trojanischen Pferdes am nächsten. Dem Verdächtigen wird vorgespiegelt, eine nützliche Software zu bekommen. Diese enthält im Hintergrund die RFS.

In der Vergangenheit gab es bereits Versuche, die Software über eine verschenkte CD zu installieren[7]:

> Einem Antrag wurde stattgegeben, und die Fahnder haben dann den Verdächtigen eine CD in den Briefkasten geworfen, die aussah wie die Zugangssoftware eines großen Internet-Providers. Die Verdächtigen haben die Software aber nicht installiert.

Nach dem Einlegen der CD oder DVD versucht diese die Autostart-Funktion auszuführen und im Hintergrund das Programm zu installieren.

Im Rahmen eines Audits legte ein IT-Sicherheitsdienstleister mehrere USB-Sticks in einer Bank aus. Die Angestellter nahmen diese zum Großteil auf und steckten diese in ihre Arbeitsrechner[14]. Bei dem Versuch gab es ein Programm auf dem Stick, welches ähnlich zu der obigen Autostart-Funktion beim Einstecken ausgeführt wurde. Das Verfahren lässt sich in gleicher Weise auch auf die RFS anwenden.

Eine beliebte Methode, um Schadsoftware auf Computersysteme zu installieren, ist der Versand infizierter E-Mails. Diese Nachrichten enthalten Anhänge, die entweder Schwachstellen im Zielsystem ausnutzen und sich selbstständig installieren oder den

Nutzer gezielt manipulieren, um zu erreichen, dass dieser die Installationsroutine startet (Social Engineering). Ein besonders erfolgreiches Beispiel in dieser Hinsicht ist der Stormworm[5]. Holz et al. fanden in einer kürzlich veröffentlichten Studie heraus, dass bis zu 1,8 Millionen Rechner weltweit mit diesem Virus infiziert sind[9].

Wenn das Nutzerverhalten bekannt ist, lassen sich auch oft besuchte Webseiten speziell manipulieren. Eine Schadsoftware nutzt eine Sicherheitslücke im Browser aus und installiert ein fremdes Programm.

Schließlich lässt sich bei der Aktualisierung eines Programms eingreifen, indem manipulierte Software übertragen wird. Diese führt das gewünschte Update aus und installiert zusätzlich die Schadsoftware. Vielfach werden kryptografisch signierte Pakete zum Herunterladen bereitgestellt. In diesem Fall ist die Manipulation nicht einfach und kann nur mit der Mitarbeit des Softwareanbieters geschehen.

3.4.3 Hintertüren in Verschlüsselungsprodukte

Neben den oben vorgestellten Maßnahmen gäbe es die Möglichkeit, Hersteller verbreiteter Softwareprodukte zu überzeugen, eine Hintertür in ihre Software einzubauen. Beispielsweise gab es in der Vergangenheit immer wieder Debatten, ob Microsoft mit der NSA zusammen arbeitet und einen Generalschlüssel eingebaut hat.

Im Fragenkatalog des Bundesministeriums der Justiz[3] wird zu der Frage, ob absichtlich geschwächte Verschlüsselungsprodukte eingesetzt werden, wie folgt geantwortet:

> ... der generelle Einbau von „staatlichen Hintertüren“ in Verschlüsselungsprodukte ist derzeit politisch nicht gewollt.

Daher ist von dieser Variante vorerst nicht auszugehen. Auch wurde die Frage nach der Manipulation von Virenscannern verneint.

3.4.4 Gewinnung der Daten

Nach der erfolgreichen Installation des Bundestrojaners besteht umfangreicher Zugriff auf das System des Verdächtigen. Insbesondere kann jegliche Datei im Zielsystem ausgelesen und übertragen werden. Weiterhin ist geplant, Tastatureingaben aufzuzeichnen und auszuwerten. Dadurch erhalten die Behörden unter Umständen Zugriff auf Zugänge bei anderen Diensten (StudiVZ, MySpace etc.). Theoretisch möglich, ist die Aktivierung von eventuell vorhandenem Mikrofon und Kamera, um die Online-Durchsuchung auf visuelle und akustische Wohnraumüberwachung zu erweitern. Das BMI verneint diese Möglichkeiten ausdrücklich.

Falls eine Online-Verbindung besteht, werden die gewonnenen Daten sofort übertragen. Andernfalls werden die Daten verschlüsselt zwischengespeichert. Nach Aktivierung der Online-Verbindung werden die Dateien dann übertragen.

3.4.5 Deinstallation der Software

Nach Beendigung der Maßnahme muss die Software wieder entfernt werden. Dies kann sowohl aufgrund eines vorher eingestellten Ablaufdatums passieren wie auch wegen der

Aufhebung des entsprechendes richterlichen Beschlusses oder aus anderem wichtigem Grund. Im ersten Fall ist keine Steuerung von außen nötig. Für die anderen Fälle muss es jedoch zwingend, eine Steuerung von außen geben können. Diese Steuerung kann naturgemäß auch von nicht berechtigten Personen benutzt werden. Dies eröffnet ein erhebliches Missbrauchspotenzial.

Weiterhin ist die Deinstallation einfach, denn (aus [2]):

> Sollte der Kommunikationsport während eines laufenden Einsatzes geschlossen werden und keine Kommunikation mit dem Steuerungssystem möglich sein, deinstalliert sich die Software selbständig.

4 Schutzmöglichkeiten der Anwender

Dieser Abschnitt diskutiert die Schutzmöglichkeiten, die jedem Anwender zur Verfügung stehen. Es wird sowohl betrachtet, wie man eventuelle Eingriffe erkennen kann als auch wie diese abgewehrt werden können.

4.1 Verschleierung

Wie in Abschnitt 3.1 dargestellt wurde, soll dem eigentlichen Eingriff in das System eine Phase der Informationsgewinnung vorhergehen. Das Ziel ist, genaue Erkenntnisse über das betreffende System zu erhalten, um später speziell angefertigte Software aufzuspielen.

Bereits hier kann der Selbstschutz beginnen. Der Nutzer kann versuchen, sowohl das Betriebssystem selbst wie auch die benutzte Software zu verschleiern.

Eine Möglichkeit, Betriebssysteme zu identifizieren, ist das so genannte Fingerprinting. Dabei wird der Netzverkehr eines Zielsystems abgehört. Jedes Betriebssystem konstruiert die Pakete oder spezielle Angaben in den Netzpaketen in einer speziellen Weise. Dies ermöglicht es, verschiedene Betriebssysteme bis hin zu deren Versionsnummern zu erkennen.

Durch den Austausch des Netzwerkstacks im eigenen Betriebssystem oder auch durch Änderungen einzelner Eigenschaften des Netzwerkstacks kann der Angreifer über das eigene System getäuscht werden. Dies kann einerseits die Vorspiegelung eines falschen Betriebssystems wie auch Unidentifizierbarkeit sein. Diese Maßnahme lässt sich nur bei Systemen anwenden, die diese Modifikationen erlauben. Alternativ lassen sich auch Programme vorschalten, die spezielle Eigenschaften der Pakete entsprechend ändern. Dadurch kann unter Umständen das gleiche Ziel erreicht werden. Jedoch ist dabei zu beachten, dass die Modifikationen dieser Programme eventuell detektiert werden können.

Ähnlich wie dies soeben bei Betriebssystemen beschrieben wurde, lässt sich auch das Verhalten von Programmen ändern. Viele bieten von Haus aus an, dass man nur bestimmte Informationen zur verwendeten Version angibt oder auch komplett andere Angaben setzen kann.

Allen diesen Maßnahmen ist gemein, dass sie letztlich keinen Sicherheitsgewinn bringen. Denn spätestens wenn Ermittlungsbeamte hardwareseitig Zugriff auf das System

haben, können sie die benötigten Informationen gewinnen. Im Rahmen des Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BKAG-E) wurde ausdrücklich der Einsatz von diversen Arten von Ermittlern erlaubt. Diese dürfen sich, wenn auch mit der Zustimmung der betroffenen Personen, Zugriff zu Räumen verschaffen. Daher ist zu vermuten, dass spätestens in schwierigen Fällen, dieser Weg gegangen wird.

4.2 Schutz vor TEMPEST-Angriffen

In Abschnitt 3.2 wurde die Funktionsweise erklärt. Ein Schutz vor dem unbeobachteten Auslesen der Abstrahlung ist in der Praxis mit Aufwand verbunden. Üblicherweise wird versucht, einen Faradayschen Käfig zu errichten. Dies wird mit Einarbeitung von Kupferdrähten realisiert. Dies kann direkt in den Wänden wie auch in der Wandverkleidung sein. Für Privatanwender sind derartige Maßnahmen schwer umzusetzen.

Eine andere oft genutzte Schutzmöglichkeit sind Störquellen. Das heißt, gleichzeitig werden mehrere ähnliche Aktionen gestartet. Ein Ziel ist, dass entfernte Beobachter nicht mehr die Originalabstrahlung feststellen kann. Wie schon beim obigen Punkt kann bemerkt werden, dass es für den Privatanwender recht schwer wird, solche Maßnahmen einzusetzen.

Eine letzte Schutzmaßnahme ist die Überwachung der Umgebung. Sowohl das Bundesamt für Sicherheit in der Informationstechnik (BSI) wie auch die NATO legen Schutzzonen fest. Dort ist definiert, dass die Umgebung auf verdächtige Gegenstände zu überprüfen ist.

Die oben genannten Maßnahmen sind für Privatanwender wie auch für andere nur schwer oder gar nicht einzusetzen. Weiterhin erfolgt der Eingriff nicht invasiv. Insofern wird der TEMPEST-Angriff zu einem wirkungsvollen Einsatzmittel. Daher und auch weil es sich immer um Nur-Lese-Zugriffe handelt, wurde das Verfahren von Experten als das am besten für die heimlichen Online-Durchsuchungen geeignete besprochen. Denn auf diese Weise lassen sich Verdachtsmomente erhärten und gleichzeitig werden unter Umständen gerichtsverwertbare Beweise gesammelt.

4.3 Schutz vor Manipulation der Hardware

Wie bereits gezeigt, kann die Manipulation der Hardware auf verschiedenen Wegen erfolgen. Einerseits können Bauteile mit Schadfunktionen engebaut werden, andererseits können auch Bauteile durch andere, gleichaussehende ausgetauscht werden.

Eine einfache, wie effektive Schutzmöglichkeit besteht in der Versiegelung der Bauteile oder ihrer permanenten Verbindungsstellen. Beispielsweise ließe sich eine Mischung aus zwei oder mehreren Farben herstellen. Diese wird so angefertigt, dass die Farben nicht komplett vermischt sind, sondern Schlieren zu sehen sind. Wichtige Stellen werden sodann mit Farbpunkten markiert und fotografiert. Das entstandene Muster ist schwer nachzubilden, kann jederzeit durch einen Vergleich mit der Aufnahme validiert werden und im Falle eines Einbruchs wird das Siegel zerstört oder beschädigt. Andere, gleichwertige Maßnahmen sind denkbar. Allen ist gemein, dass sie regelmäßige Prüfungen

voraussetzen, um eventuelle Einbrüche zu erkennen.

Tragbare Geräte können des Weiteren in Tresoren oder anderen sicheren Einrichtungen verwahrt werden. Gerade in Bereichen, die hohen Sicherheitsstandards unterliegen, ist das bereits jetzt Usus.

Eine Einbruchserkennung lässt sich auch Softwarebasis durchführen. Es sind verschiedene Ansätze denkbar, die beim Systemstart alle an das informationstechnische System angeschlossene Hardware prüft und bei Veränderungen warnt oder den Start verweigert. Einen ähnlichen Ansatz verfolgt auch das Trusted Platform Module (TPM). Hierbei prüft ein Chip die Vertrauenswürdigkeit des Systems und löst in Abhängigkeit Aktionen aus. Bisher kamen diese Lösungen stark in die Kritik, da die Fähigkeiten der Chips zur Einengung der Benutzerrechte eingesetzt wurden. Gerade Freie Betriebssysteme könnten durch eine entsprechende Nutzung des Chips einen hohen Sicherheitsvorteil für Nutzer bieten.

4.4 Schutz vor Manipulation der Software

Die unentdeckte Manipulation von Software ist ein sehr weites Feld. Die vollständige Diskussion dieses Bereichs würde den Rahmen dieser Anhandlung sprengen. Daher soll nur auf Einzelaspekte eingegangen werden.

Allgemein ist es wünschenswert, bereits das Aufspielen der Schadsoftware zu verhindern. In Abschnitt 3.4.1 wurde diskutiert, dass der direkte Weg durch einen Ermittlungsbeamten oder dessen Erfüllungsgehilfen nicht erlaubt ist. Daher verbleibt für eine manuelle Installation nur der Weg über eine Schwachstelle in der Software.

Einerseits ist es vorstellbar, dass speziell ein so genannter Exploit, d. h. ein Programm, welches eine Schwachstelle ausnutzt, angekauft und dann eingesetzt wird. Es existiert ein „grauer Markt“ für derartige Produkte und insbesondere dann werden sehr hohe Preise erzielt, wenn die Schwachstelle nicht öffentlich bekannt ist. Weiterhin aktualisieren viele Nutzer die eigene Software nicht regelmäßig, so dass lange Zeit Angriffsstellen vorhanden sind. Sollte der Exploit erfolgreich eingesetzt worden sein, geht damit meist ein Vollzugriff auf das System einher und es kann dann beliebige weitere Software auf dem Zielsystem installiert werden.

Schutz bietet die regelmäßige Aktualisierung der verwendeten Software. Weiterhin sollten Nutzer darauf die Schnittstellen zu öffentlichen Netzwerken gering halten und darauf achten, dass sie Software einsetzen, die bekanntermaßen sicher ist oder zumindest Entwickler hat, die hohen Wert auf Sicherheit und diesbezügliche Transparenz legen.

Sollten die Rechner in größeren Netzwerken eingesetzt werden, ist auch die Benutzung von Filtermechanismen (Paketfilter, Firewall etc.) oder Einbruchserkennung hilfreich. Diese können Angriffe abwehren oder erkennen und melden.

Sofern nicht unbedingt notwendig, ist es weiterhin empfehlenswert, offline zu arbeiten. Denn laut den Antworten der Bundesregierung sollen in diesem Falle Dateien auf dem Speichermedium angelegt werden, die dann bei einer späteren Netzwerkverbindung an die Ermittlungsbehörden versandt werden. Das Dateisystem lässt sich jedoch

durch Hilfsprogramme auf neu angelegte Dateien durchforsten oder Programme warnen sofort, wenn eine neue Datei angelegt wurde. Somit gelangt man recht schnell in Kenntnis und kann den Vorgang prüfen. Eine wesentliche Eigenschaft dieser fremd erzeugten Dateien ist die Verschlüsselung des Inhalts. Wenn also eine Datei erzeugt wird, deren Inhalt eine hohe Entropie besitzt und deren Herkunft Misstrauen erweckt, kann der Nutzer Gegenmaßnahmen treffen. Beispielsweise wäre es ratsam, mit einer Notfall-CD, wie KNOPPIX oder grml, zu booten, die Datei zu suchen und unter Quarantäne zu stellen oder zu löschen. Insofern ist der Eingriffsversuch vereitelt worden.

Wenn das informationstechnische System nur auf eine begrenzte, im Vorfeld bekannte Zahl anderer Rechner zugreift, ist weiterhin denkbar, mittels eines Paketfilters den Zugriff nur auf diese Ressourcen zu erlauben. Verbindungsversuche zu fremden Rechnern wären dann ausgeschlossen und somit könnte der Bundestrojaner nicht seine Aufgabe erfüllen.

Weiterhin wurde die automatische Installation angesprochen. Dies setzt voraus, dass der Nutzer leichtfertig handelt und sich der dadurch entstehenden Risiken nicht bewusst ist. Hier hilft nur fortwährende Schulung und Aufklärung der Anwender.

Persnen, die von vornherein ein hohes Schutzprofil besitzen und PCs nutzen, können noch andere Wege beschreiten. Denkbar wäre die Anschaffung eines Rechners, der später dauerhaft von einer nur lesbaren CD betrieben wird. Alle Nutzerdaten befinden sich auf einem verschlüsselten USB-Stick. Derartige Lösungen sind für interessierte Anwender schon heute herzustellen und einsatzbereit. Durch den Einsatz wird die erfolgreiche Aufbringung der RFS deutlich erschwert, wenn nicht unmöglich gemacht.

Anhand der oben diskutierten Punkte lässt sich eindeutig festhalten, dass es für Anwender, die über genaueres Wissen über die Arbeitsweise des zugrundeliegenden Systems verfügen, sehr wohl möglich ist, sich vor dem Befall durch Schadsoftware zu schützen oder den Befall rechtzeitig zu entdecken.

5 Rechtliche Einschätzung

Die rechtliche Bewertung fällt derzeit schwer. Denn einerseits wurden Rechtsnormen vom BVerfG verworfen und andererseits werden gerade neue aufgestellt, die Ihrerseits wieder vom Gericht geprüft werden. Daher soll dies nur ein Abriss sein. Dieser beginnt bei einer Dienstanweisung aus dem BMI und endet bei Betrachtungen zum Grundgesetz.

5.1 Dienstanweisung aus dem BMI

Die erste Rechtsvorschrift stammt aus dem Hause des Bundesinnenministeriums. Der damalige Innenminister Otto Schily ermächtigte das Bundesamt für Verfassungsschutz per Dienstanweisung, Computer von Verdächtigen zu untersuchen. Dr. Wolfgang Schäuble annulierte diese Vorschrift später. Denn wegen des großen Eingriffes in die Grundrechte kann eine derartige Maßnahme keinesfalls per Dienstanweisung durchgesetzt werden.

5.2 Verfassungsschutzgesetz in Nordrhein-Westfalen

Das Bundesland Nordrhein-Westfalen legte im VSG eine Rechtsvorschrift nieder. Das Gesetz schreibt in § 5 Abs. 2 Nr. 11 ([18]):

> (2) Die Verfassungsschutzbehörde darf nach Maßgabe des § 7 zur Informationsbeschaffung als nachrichtendienstliche Mittel die folgenden Maßnahmen anwenden:
> ...
> 11. heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel. Soweit solche Maßnahmen einen Eingriff in das Brief-, Post- und Fernmeldegeheimnis darstellen bzw. in Art und Schwere diesem gleichkommen, ist dieser nur unter den Voraussetzungen des Gesetzes zu Artikel 10 Grundgesetz zulässig;
> ...

Gegen die Rechtsnorm wurde Verfassungsbeschwerde eingelegt. Das Bundesverfassungsgericht verhandelte die Klage am 2008-02-27 und kam zu dem Ergebnis, dass der oben aufgeführte Artikel nicht mit dem Grundgesetz vereinbar ist. Ferner wurde ein neues Grundrecht, das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, definiert. Damit bestehen starke Einschränkungen. Insbesondere darf eine Online-Durchsuchung nur dann durchgeführt werden, wenn „tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen“. Mit überragend wichtig sind Leib, Leben und Freiheit einer Person oder Güter, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren, definiert.

Im Jahresverlauf 2008 legte das Bundesland Bayern einen weiteren Gesetzesentwurf für eine heimliche Online-Durchsuchung vor. Die Rechtmäßigkeit dieses Gesetzes muss noch geprüft werden.

5.3 BKAG-E

Das BKAG-E verschafft dem BKA weitgehende Befugnisse in der Verbrechensbekämpfung. Neben der heimlichen Online-Durchsuchung gehören dazu die teilweise Abschaffung des Rechtes auf Zeugnisverweigerung (§20c Abs. 3), Einsatz verdeckter Ermittler (§20g Abs. 2 Satz 5), Benutzung der Rasterfahndung (§20j), verdeckte Eingriffe in informationstechnische Systeme (§20k) sowie viele weitere. Das Gesetz wurde im Juni 2008 vom Bundeskabinett beschlossen.

Bereits jetzt bezweifeln viele Juristen die Verfassungmäßigkeit des Gesetzes. Eine Klage beim Bundesverfassungsgericht wird das Gesetz prüfen und ein abschließendes Ergebnis wird von dieser Stelle veröffentlicht werden.

5.4 Strafprozessordnung

Die heimliche Online-Durchsuchung ist in keinen weiteren Vorschriften definiert. Daher soll im folgenden auf bestehende Normen eingegangen werden.

In der Strafprozessordnung (STPO) gibt es verschiedene Paragrafen, die unter Umständen die heimliche Online-Durchsuchung regeln könnten. Der § 100 a regelt die Telekommunikationsüberwachung. Die Durchsuchung bzw. Übertragung der Daten erfolgt zwar mittels Telekommunikation, jedoch wird das informationstechnische System selbst nicht überwacht. Daher findet die Vorschrift keine Anwendung.

Der § 100 c regelt die Abhörung des nichtöffentlich gesprochenen Wortes mit technischen Mitteln. Genau dies wird von der heimlichen Online-Durchsuchung nicht beabsichtigt. Daher findet auch diese Vorschrift keine Anwendung.

Die Abhörung des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen ist in § 100 f festgelegt. Hier greift dieselbe Begründung wie schon im vorhergehenden Absatz.

In § 102 werden Bedingungen für die Durchsuchung des Wohnraumes definiert. Es gab bislang keine eindeutige Haltung der Gerichte, ob dieser Paragraf anzuwenden ist. Verschiedene Ermittlungsrichter des Bundesgerichtshof (BGH) befürworteten bzw. lehnte Online-Durchsuchungen auf dieser Basis ab. Die hauptsächliche Begründung für diese Ablehnung ist die in STPO geforderte Offenheit der Maßnahmen. Demgegenüber steht ganz klar, die heimliche Online-Durchsuchung.

Somit gibt es im Rahmen der Strafprozessordnung keine anwendbaren Paragrafen. Auch andere, gleichrangige Gesetze beinhalten keine Regelungen.

5.5 Grundgesetz

Da es offensichtlich keine gesetzliche Grundlage gibt, ist zu klären, ob heimliche Online-Durchsuchungen verfassungsmäßig gerechtfertigt sind. Das Bundesverfassungsgericht legte schon 1957 im so genannten Elfes-Urteil einen unantastbaren Bereich menschlicher Freiheit fest. Dieser leitet sich aus Art. 1 Abs. 1 des Grundgesetzes ab. In späteren Entscheidungen nahm das BVerfG immer wieder Bezug auf den unantastbaren Bereich privater Lebensgestaltung. Dies wurde in der Entscheidung zum Großen Lauschangriff von 2004 wieder aufgegriffen. Die Richter legten fest, dass in diesem Bereich *keine* Abwägung zwischen den Grundrechten der Einzelperson und der öffentlichen Gefahrenabwehr bzw. den Interessen der Strafverfolgung stattzufinden hat.

Der Rechner wird heutzutage nicht mehr nur als bessere Schreibmaschine benutzt, sondern findet in allen Lebenslagen Verwendung. Neben den Programmen finden sich eine Vielzahl an äußerst privaten, schützenswerten Daten auf Computern. Dazu gehören beispielsweise private E-Mails, Bilder, Einträge in Tagebüchern, Kontoinformationen sowie eventuell auch Informationen zur Gesundheit des Betroffenen. In aller Regel fällt die Abgrenzung zu Dateien, die nicht dem Kernbereich der privaten Lebensgestaltung angehören, sehr schwer. Der Name einer Datei ist manchmal ein Anhaltspunkt. Jedoch ist nicht garantiert, dass eine Datei `tagebuch.txt` oder `windows.exe` wirklich eine Text- oder ausführbare Datei sind. Gewissheit erlangt der Beobachter nur durch eine Einsicht-

nahme. Laut der Entscheidung des Bundesverfassungsgericht darf jedoch nicht in den Kernbereich eingegriffen werden, um einzuschätzen, ob Daten in den Kernbereich gehören. Dieses Dilemma ist in der Praxis nur sehr schwer aufzulösen. Sollte der Gesetzgeber hier keine verfassungskonforme Regelung finden, ist die Maßnahme als Ganzes nicht anwendbar.

Mit der heimlichen Online-Überwachung könnte auch ein weiteres Grundrecht, das auf die Unverletzlichkeit der Wohnung nach § 13 **GG!** (**GG!**), berühren. In der Regel befinden sich die Rechnersysteme innerhalb einer Wohnung und damit findet nach einschlägiger Meinung wie auch nach höchstrichterlicher Rechtsprechung der Paragraf Anwendung. Lediglich der Bundesinnenminister Dr. Wolfgang Schäuble wurde mit anderer Meinung zitiert[5]:

> „Es wäre aus verfassungsrechtlicher Sicht noch umfassend zu diskutieren, ob die derzeitige Fassung des Artikels 13 Grundgesetz das heimliche Betreten einer Wohnung zulässt."

In der Diskussion wird immer wieder angeführt, dass Privatrechner, die mit einem öffentlichen Netzwerk verbunden sind, nicht mehr dem Schutz des Grundgesetzes unterliegen. Denn, so wird argumentiert, der Wohnraum wird durch eine Online-Durchsuchung nicht angerührt. Diese Argumente lassen jedoch auch auf akustische oder optische Wohnraumüberwachung anwenden. Weiterhin arbeiten Bauplaner am so genannten „intelligenten Haus". Dort werden mittels Sensoren und Steuerungsmechanismen so viele Aufgaben wie möglich automatisiert. Fenster und Jalousien werden automatisch geöffnet und geschlossen, die Heizung wird reguliert etc. Mit der obigen Argumentation könnten die Sensoren ausgelesen und detaillierte Informationen zum Nutzerverhalten gewonnen werden. Wenn dieser Gedanke konsequent weiterverfolgt wird, könnte der § 13 bald ausgehebelt werden, obwohl sich die zu beobachtende Person innerhalb einer Wohnung oder eines Hauses befindet.

Daher muss auch bei einem Computer innerhalb privater Wohnungen der § 13 des Grundgesetzes Anwendung finden. Der Paragraf bietet in Absatz 1 keine Einschränkungen, sondern sagt eindeutig: „Die Wohnung ist unverletzlich.". Außer speziell definierten Eingriffen wird nichts weitergehendes erlaubt.

Wie zu sehen ist, wird es äußerst schwierig, eine dem Grundgesetz konforme Rechtsnorm zu gestalten. Weder bisher bestehende Gesetze noch das Grundgesetz selbst haben ausreichende Regelungen und gerade der Kernbereich privater Lebensgestaltung stellt für künftige Gesetze eine starke Hürde dar.

6 Fazit

In den vorigen Abschnitten wurde das Mittel der heimlichen Online-Durchsuchung aus verschiedenen Aspekten beleuchtet. Es konnte einerseits gezeigt werden, dass ein technisch versierter Anwender An- oder Eingriffe in das informationstechnische System ab-

[5] aus `http://www.bmi.bund.de/nn_662998/Internet/Content/Nachrichten/Medienspiegel/2008/04/BM__LVZ.html`

wehren und erkennen kann. Lediglich TEMPEST-Angriffe sind schwer beherrschbar und liefern zudem wahrscheinlich gerichtsverwertbare Ergebnisse.

Es ist anzunehmen, dass die Gruppe, auf die Gesetze abzielen, nämlich Schwerstkriminelle und Terroristen, das benötigte Fachwissen vorhalten oder aus externer Quelle zukaufen. Daher ist mit großer Wahrscheinlichkeit die Mehrzahl der obigen Maßnahmen wirkungslos. Also werden Ermittler, die sich auf die heimliche Online-Durchsuchung verlassen, keine oder sehr wenige Ergebnisse erzielen können.

Auch aufgrund der rechtlichen Betrachtungen ist es fraglich, ob heimliche Online-Durchsuchung verfassungsgemäß gestaltet werden kann. Nach dem Urteil des BVerfG werden sehr starke Anforderungen an diese Ermittlungsmethoden gestellt und derzeit ist nicht klar, ob diese verfassungskonform gestaltet werden können.

Daher sollte auf die oben besprochenen Maßnahmen verzichtet werden. Alternativ ist aus Sicht des Autors vorstellbar, dass eine zeitliche beschränkte und grundgesetzkonforme Regelung geschaffen wird. Der Ergebnisse sollten dann bei Ablauf des Gesetzes unabhängig geprüft werden. So ließe sich feststellen, ob das Mittel der heimlichen Online-Durchsuchung wirklich derart schlagkräftig ist, wie derzeit behauptet.

Aus Sicht des Schutzes der Bürgerrechte sowie der Erfolgsaussichten ist jedoch ein Komplettverzicht eindeutig zu bevorzugen.

Literatur

[1] Bundesministerium der Justiz. Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt. April 2008.

[2] Bundesministerium des Innern (BMI). Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien. http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf, August 2007.

[3] Bundesministerium des Innern (BMI). Fragenkatalog des Bundesministerium für Justiz. http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, August 2007.

[4] Bundesregierung. Drucksache 16/7279: Antwort der Bundesregierung auf eine kleine Anfrage der FDP. http://dip21.bundestag.de/dip21/btd/16/072/1607279.pdf, November 2007.

[5] Brandon Enright. Exposing Stormworm. http://noh.ucsd.edu/~bmenrigh/exposing_storm.ppt, Oktober 2007.

[6] Andres Molina Gaurav Shah and Matt Blaze. Keyboards and covert channels. http://www.crypto.com/papers/jbug-Usenix06-final.pdf, Oktober 2006.

[7] Günter Hack. Zur Prüfung deutscher Online-Fahnder. *ORF Futurezone*, August 2007.

[8] Alex Halderman et al. Lest We Remember: Cold Boot Attacks on Encryption Keys. April 2008.

[9] Thorsten Holz et al. Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm. pages 1—9, http://honeyblog.org/junkyard/paper/storm-leet08.pdf, April 2008.

[10] NSA. TEMPEST: A Signal Problem. declassified document, NSA, April 2008.

[11] Andreas Pfitzmann Prof. Dr.˙ Rede vor dem Bundesverfassungsgericht. http://dud.inf.tu-dresden.de/literatur/BVG2007-10-10.pdf, Oktober 2007.

[12] Hartmut Pohl Prof. Dr.˙ Zur Technik der heimlichen Online-Durchsuchung. *Datenschutz und Datensicherheit*, 31 (2007) 9:684—688, September 2007.

[13] Achim Sawall. BND infizierte afghanisches Ministerium mit Spähsoftware. *golem.de*, April 2008.

[14] Prof. Dr. Ulrich Sieber. Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen. Technical report, Max-Planck-Institut für ausländisches und internationales Strafrecht, http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf, Oktober 2007.

[15] StPO. *Strafprozessordnung*. in der Fassung vom 19. April 2008.

[16] Wim van Eck. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? *Computers & Security*, 4:269—288, 1985.

[17] Redaktion von Tagesschau. Rund ein Dutzend Mal wurde geschnüffelt. *tagesschau.de*, April 2007.

[18] VSG NRW. *Gesetz über den Verfassungsschutz in Nordrhein-Westfalen (Verfassungsschutzgesetz Nordrhein-Westfalen)*. in der Fassung vom 20. Dezember 2006.