Onlinedurchsuchung versus Virenscanner – Eine Aufwandsabschätzung

Ulrich Greveler[1] · Christian Puls[2]

[1]Fachhochschule Münster, Labor für IT Sicherheit, 48565 Steinfurt
greveler@fh-muenster.de

[2]Advanced Nuclear Fuels GmbH, 49811 Lingen
christian.puls@areva.com

Zusammenfassung

Der Beitrag betrachtet technische Aspekte der Online-Durchsuchung, wie sie nach dem kürzlich in Kraft getretenen BKA-Gesetz in Deutschland ermöglicht werden soll. Da auf einem Zielsystem regelmäßig Sicherheitstools (*Virenscanner*, *Personal Firewalls*) installiert sind, muss die Schutzwirkung dieser Programme für die Online-Durchsuchung umgangen werden. Der Beitrag zeigt, dass – entgegen der Aussage von Herstellern dieser Programme – eine Umgehung mit geringem Aufwand möglich ist, insbesondere ist keine Kooperation der Ermittlungsbehörden mit Herstellern von Sicherheitstools Voraussetzung für eine erfolgreiche Online-Durchsuchung. Vorgaben des Bundesverfassungsgerichtes in Bezug auf die Online-Durchsuchung können – soweit sie technischer Natur sind – durch eine *Remote Forensic Software* umgesetzt werden, die mit geringem Aufwand für den Einzelfall erstellt werden kann.

1 Einführung

Wir beziehen uns mit dem Begriff der Online-Durchsuchung auf den *verdeckten Eingriff in informationstechnische Systeme* wie sie nach dem (am 01.01.2009 in Kraft getretenen) BKA-Gesetz (hier: §20k) ermöglicht werden soll. Das Gesetz regelt die Voraussetzungen, unter denen „*das Bundeskriminalamt ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben*“ darf.

Unter dem Eingriff mit technischen Mitteln wird in diesem Beitrag die Kompromittierung des Systems, d. h. die Installation einer komfortablen *Backdoor* bzw. eine Installation eines *Remote Administration Tools* (in diesem Zusammenhang auch *Remote Forensic Software*, RFS, genannt) verstanden, das einer fremden Partei umfangreiche Möglichkeiten bietet, Daten zu lesen bzw. zu verändern und das System für diverse Zwecke zu manipulieren. Die technischen Möglichkeiten gehen dabei über die juristisch gesetzten Grenzen hinaus.

Dieser Beitrag bezieht sich nicht auf die politischen und juristischen Aspekte der Online-Durchsuchung, die seit dem Bekanntwerden einer bundesdeutschen Dienstvorschrift zur „of-

fensiven Beobachtung des Internets“ im April 2007 und der Verabschiedung eines Verfassungsschutzgesetz des Landes Nordrhein-Westfalen (mit Regelungen zur Online-Durchsuchung) Gegenstand einer intensiven öffentlichen Debatte und breiter Berichterstattung in den Medien waren und zum Urteil des Bundesverfassungsgerichtes vom 27. Februar 2008 führten, welches ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme begründete. Vielmehr werden besondere technische Aspekte beleuchtet: So gehen Hersteller von Anti-Viren-Software davon aus, dass die Software zur Onlinedurchsuchung von ihren Anti-Viren-Systemen als potenziell gefährlich gemeldet würde, da auch eine RFS mit den gleichen Methoden wie andere Spyware arbeite. Ein Industrievertreter wird mit der Aussage zitiert, dass *„ein Trojaner eine Spionage-Software [ist und bleibt]. Sobald seine Struktur den Software-Herstellern bekannt wird, wird er in das Verzeichnis bekannter Viren aufgenommen und von den Programmen blockiert.*“ Eine Zusammenarbeit mit staatlichen Behörden bei den Online-Durchsuchungen lehnen die Software-Hersteller ab [Gra07]. Diese Aussagen könnten zur Annahme Anlass geben, dass der Schutz, der mit Anti-Virus-Produkten erreicht wird, eine Online-Durchsuchung erheblich erschwert bzw. dass die Aufwände, die zur Umgehung des Schutzes notwendig sind, nur mit bedeutenden personellen Ressourcen geleistet werden können. Unsere Untersuchungen zeigen jedoch, dass diese Annahme unbegründet ist: Der Beitrag stützt sich dabei auf ein empirisches Modell und nutzt Laborergebnisse, die in praktischer Hinsicht zeigen, inwieweit ein „typischer“ Privatanwender-PC einer sog. Online-Durchsuchung bzw. einer Online-Überwachung aus der Ferne unterworfen werden kann.

2 Technische Umgebung der Online-Durchsuchung

2.1 Begriffsdefinitionen zur Remote Forensic Software

2.1.1 Digitale Forensik

Die *Digitale Forensik* ist eine junge Teildisziplin der IT-Sicherheit. Erst seit Mitte der neunziger Jahre werden durch *Interpol* Weiterbildungen für polizeiliche Ermittler in Bezug auf die Beweissicherung bei Computerstraftaten angeboten; zu dieser Zeit kam es bei Ermittlungen noch zu schwerwiegenden Ermittlungspannen, weil beispielsweise sichergestellte Disketten zu den Akten geheftet und damit unbrauchbar gemacht wurden [Con97]. Häufig wird *Digital Forensic* synonym mit den Begriffen *Computer-Forensik* oder *IT-Forensik* verwendet, jedoch geht je nach Definition der Begriff Digitale Forensik über den Begriff Computer-Forensik hinaus. So wird je nach Autor beispielsweise eine Eingrenzung auf den Computer vorgenommen oder nur von binären Daten gesprochen. Wir orientieren uns an der Definition des *Digital Forensic Research Workshop* [Dfrws01]: “*The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.*”. Eine Online-Durchsuchung ist demnach als IT-forensische Maßnahme zu betrachten, sofern die verwendete Methode den geforderten wissenschaftlichen Ansprüchen genügt. Dabei ist es unerheblich, ob sich die Ermittlungen auf die Aufklärung von Computer-Straftaten (wie Computerbetrug) oder um die Abwehr von Terrorismus-Gefahren (wie es das BKA-Gesetz benennt) beziehen.

2.1.2 Malware

Malware ist ein Oberbegriff für bösartige Software, sowohl selbstreplizierende (Viren) oder nicht selbstreplizierende. Das Wort Malware setzt sich aus den Wörter **mal**icious (engl. für bösartig) und Soft**ware** zusammen. Die OECD definiert Malware [OECD08]: "*Malware is a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners.*" Auch wenn die Malware keine beabsichtigten Schadfunktionen bereitstellt, kann schon von einer Beeinträchtigung gesprochen werden, wenn Systemressourcen verbraucht werden, ohne einen vom Nutzer gewünschten bzw. spezifizierten Zweck zu erfüllen.

2.1.3 Backdoors & Rootkits

Unterarten der Malware stellen nicht nur Viren oder Trojaner, sondern auch *Backdoors* und *Rootkits* dar. Eine Backdoor erlaubt es, vorgesehene Authentifizierungsmechanismen und Sicherheitsrichtlinien zu umgehen, um Zugriff auf den Rechner zu erhalten. Backdoors können als eigenständige Programme (wie z. B. *Back Orifice*), Modifikation von bestehenden Programmen oder der Hardware oder durch nur dem Ersteller des Systems bekannte Passwörter bzw. undokumentierte Login-Funktionen auf ein System gelangen. Häufig gelangen Backdoors als Payload von Viren, Würmern oder Trojanern in ein System.

Das „Einsatzgebiet" für ein Rootkit ist das Verstecken von Prozessen und Dateien, um Beispielsweise eine Backdoor zu verschleiern oder einen Keylogger zu tarnen. Auch das Überlagern von Systemfunktionen ist möglich, um so beispielsweise den Taskmanager zu deaktivieren oder Tastatur- und Mauseingaben abzufangen. Rootkits bieten gewöhnlich zwei Hauptfunktionen: die Fernsteuerung des Systems und das Ablauschen von Daten. Unter Fernsteuerung (*remote access*) versteht man u. a. die Kontrolle über Dateien und Prozesse, das Auslösen von Neustarts oder vorsätzliche Systemabstürze. Ablauschen von Daten beinhaltet das Mitschneiden von Tastatureingaben und Netzwerkkommunikation (z. B. Lesen von Emails).

2.1.4 Remote Forensic Software

Software für den Fernzugriff bietet zumeist Funktionen, um einen Rechner, welcher in diesem Fall als Server fungiert, fernzusteuern oder zu überwachen. Hierzu können Maus- und Tastatureingaben aus der Ferne übernommen werden und der Bildschirm des Servers auf dem entfernten Client angezeigt werden. Dieser Fernzugriff ist bei den meisten Produkten dieser Art durch ein Symbol oder eine Abfrage wahrnehmbar. Ist diese Information nicht vorhanden und wird die Fernsteuerung heimlich vollzogen, so wird diese Art von Software als Backdoor oder generell als Malware angesehen. Sind Datei- und Registry-Zugriffe oder sonstige Zugriffsmöglichkeiten gegeben, so spricht man häufig von *Remote Administration Tools* (RAT). Bekannte Tools die sich selbst als RAT bezeichnen sind z. B. *Back Orifice*, *Nuclear RAT*, *SubSeven*, *Bitfrost* oder *NetBus*.

Die vom Bundesministerium des Inneren (BMI) geforderten Funktionalitäten einer Software für Online-Durchsuchungen werden durch RATs abgedeckt. Das geeignete Tool um solche Online-Durchsuchungen durchzuführen wird vom BMI-Präsidenten als *Remote Forensic Software* [Zie07] oder kurz RFS bezeichnet. Inwiefern die von Ermittlern genutzte RFS den im Abschnitt 2.1 zitierten Anforderungen der Digitalen Forensik gerecht wird, ist bisher nicht bekannt, da dokumentierte Einsätze fehlen.

2.2 Sicherheitstools

Privatanwender verwenden – nicht zuletzt wegen der Sensibilisierung für Themen der IT-Sicherheit – i. a. Sicherheitstools (aktualisierter Virenscanner mit Anti-Spyware-Funktionalität, *Personal Firewall*), die zur Durchsetzung eines mittleren Sicherheitsniveaus beitragen sollen. Tatsächlich konnten wir Ergebnisse vorlegen, die zeigen, dass bereits ein Angreifer mit durchschnittlichen Fähigkeiten in der Lage ist, die Schutzwirkung dieser Sicherheitstools auszuhebeln und den PC zu kompromittieren [GrPu09]; eine technische Hürde für die Online-Durchsuchung ist daher aufgrund der Existenz von Sicherheitstools nicht gegeben, sofern der Nutzer dazu veranlasst werden kann, eine Datei auszuführen bzw. die Ausführung durch andere Hilfsmittel (z. B. die sog. Implantierung der RFS in Downloadverbindungen [Birk07]) ausgelöst wird.

Die im Rahmen einer Abschlussarbeit [Puls08] ermittelten empirischen Ergebnisse über den „Normalfall“ eines Privatanwender-PCs bestätigen allgemeine Erwartungen, über eine typische Konfiguration und sicherheitstechnische Ausstattung eines privat genutzten PCs. So ist dieser nicht völlig ungeschützt und wir können von der Verwendung eines Virenscanners und einer *Personal Firewalls* (inkl. so genannten Malware-Detektoren) ausgehen. Es ergibt sich ein Referenzmodell eines (zu durchsuchenden) privaten PCs: Windows-basierte Installation (XP oder Vista), Virenscanner (*Avira*, *Kaspersky*, *Norton* waren häufigste Nennungen) und eine *Personal Firewall* (z. B. *Zone Alarm, Sygate*). Dieses Ergebnis lag im Erwartungsrahmen und deckt sich mit Untersuchungen zu Marktanteilen [Schü08].

2.3 Technische Umgehbarkeit der Schutzwirkung

Die Autoren haben gezeigt [GrePu09], dass ein Demonstrator auf der Basis des frei verfügbaren Fernwartungstools Back Orifice 2000 mit geringem Aufwand entwickelt werden kann, der trotz der allgemeinen Bekanntheit dieses Werkzeugs eine Erkennung durch verbreitete und aktualisierte Virenscanner und Personal Firewalls verhindert. Die Funktionalität des Demonstrators, der eine vollständige und komfortable Kontrolle des PCs von außen ermöglicht, umfasst neben dem Übertragen von Dateien, die Übermittlung von Tastatureingaben, das *Keylogging*, eine Maussteuerung und das Anfertigen von Screenshots.

Der staatliche Ermittler, der eine Onlinedurchsuchung durchführen möchte, steht vor der Herausforderung, genau diese beiden in unserer Untersuchung berücksichtigten Schutzmechanismen (Virenscanner und Personal Firewall) zu umgehen. Wir fassen die technischen Ergebnisse in den beiden folgenden Abschnitten zusammen.

2.3.1 Virenscanner

Eine Umgehung des Virenscanners (die Untersuchung wurde für 36 verschiedene, aktuelle Scanner vorgenommen, die zum Teil auch eine *Anti-Spyware*-Funktionalität aufwiesen) erwies sich – trotz angenommener geringer Ressourcen seitens des Angreifers – als technisch möglich [GrePu09]. Um sowohl die Virensignaturerkennung als auch die heuristische Erkennung zu vermeiden, wurde ein Verfahren angewandt, das mit einer Intervallschachtelung relevante Offset-Positionen in der Datei bestimmte bis kurze Fragmente (wenige oder einzelne Bytes) ermittelt wurden, die zur Erkennung durch Virenscanner relevant waren. Nachdem diese Fragmente identifiziert wurden, konnte durch Modifikation des Binärcodes (bzw. des hier frei verfügbaren Quellcodes des Administrationstools) eine Erkennung durch sämtliche betrachteten Virenscanner gänzlich unterbunden werden, ohne dass erhebliche funktionelle

Einbußen des Demonstrators akzeptiert werden mussten. Zur Erstellung einer erfolgreichen RFS sind – nach den vorliegenden Ergebnissen – nur einfache Programmierkenntnisse auf Seiten des Angreifers erforderlich [GrePu09].

2.3.2 Personal Firewall

Die zweite Hürde, die der Ermittler, dem eine Installation des RFS am Zielsystem trotz Virenscanner gelungen ist, überwinden muss, wenn er nicht vom Verdächtigen entdeckt werden möchte, ist die *Personal Firewall* (PFW). PFWs sollen i. a. verhindern, dass unzulässige Netzwerkverbindungen nach außen aufgebaut werden bzw. dass ein unerwünschter Serverdienst („offener Port“) gestartet wird. Das PFW-Konzept wird in der Literatur kritisch betrachtet, da es dem Nutzer eine oft nur scheinbar vorhandene Sicherheit vermittelt, die in der Vergangenheit in vielen zitierten Fällen umgangen werden konnte.[1]

Auch dem von uns modellierten Ermittler (mit geringen Ressourcen und durchschnittlichen technischen Fähigkeiten) gelingt die Umgehung der PFW mit einem einfachen Trick: Die RFS bestätigt automatisiert das Dialogfenster mit der Firewall-Warnung und lässt das Öffnen der Backdoor zu Ermittlungszwecken zu. Die PFW-Funktionalität wird also nicht im engeren Sinne unterdrückt; der Verdächtige bemerkt sie aber nicht mehr, da die Bestätigung ohne sein Zutun (innerhalb von Sekundenbruchteilen) erteilt wird. Technisch wurde das Bestätigen des PFW-Dialogs im Laboraufbau mit Hilfe des *windows-message*-Systems realisiert, mit dem Fensternachrichten generiert und Nutzereingaben simuliert werden können (technische Details werden von den Autoren in [GrePu09] beschrieben).

2.4 Aufwände

Die Erstellung einer RFS, die eine umfangreiche Funktionalität für Fernzugriffe auf das zu untersuchende System ermöglicht und für Ermittlungszwecke geeignet[2] ist, ist mit geringem Aufwand möglich: Eine Nutzung vorhandener Softwarekomponenten, die über Internetquellen frei verfügbar sind (auf Basis des RATs *Back Orifice 2000*), und eine Modifikation des Quellcodes, die gemäß der Untersuchungsergebnisse [GrePu09] ohne besondere Fachkenntnisse möglich ist, führt bereits zu einem funktionsfähigen RFS-Tool (hier *Demonstrator* genannt), das von keinem der getesteten Virenscanner erkannt wurde. Zudem ist es dem Demonstrator ebenfalls möglich, die Funktionalität der betrachteten *Personal Firewalls* zu umgehen, so dass einer „Installation“ des Demonstrators auf einem zu durchsuchenden Zielsystem (hier als Laborumgebung realisiert) trotz vorhandener Sicherheitstools nichts mehr im Wege stand.

Zur Ermittlung der Aufwände unterteilen wir den Vorgang der Vorbereitung einer Online-Durchsuchung in drei Abschnitte:

---

[1] „Ein Problem von Desktop-Firewalls [wird] deutlich: Sie wiegen den Anwender in Sicherheit, die sie jedoch letztlich nicht bieten können. Bis jetzt ließ sich mit etwas Phantasie noch jede Personal Firewall umgehen und Daten unerkannt vom Rechner ins Internet senden. Außerdem erhöht jede zusätzliche Software die Komplexität eines Systems und somit auch dessen Fehleranfälligkeit.“ Zitiert aus einer Heise-Meldung vom 18.07.2006 12:55.

[2] Eignung bezieht sich hier auf die technischen Möglichkeiten; der Software-Demonstrator, der im Rahmen der Untersuchungen entwickelt wurde, warnte den Benutzer vor einem Fernzugriff durch dritte, da das Tool die technischen Möglichkeiten nur *demonstrieren* sollte und zum Nachweis der Umgehbarkeit der Sicherheitstools diente.

1. Ermittlung des Betriebssystems und der Systemparameter des Systems des Verdächtigen
2. Erstellung des RFS für diesen Verdächtigen (siehe Abschnitt 2.5)
3. Einbringung (Installation) des RFS auf dem Zielsystem

Die vorliegenden Untersuchungsergebnisse [Puls08] lassen eine Aufwandsabschätzung für den Fall zu, dass der Abschnitt (1) einen in „üblicher Weise“ konfigurierten PC als Zielsystem ergibt. Nach Ermittlung dieser Ausgangsbasis ist die Erstellung des RFS (als Unikat) dann mit einem Aufwand von wenigen Personentagen möglich. Die Ergebnisse liegen für *MS-Windows*-basierte PCs vor (diese sind derzeit bezogen auf den Marktanteil „üblich“), lassen sich aber konzeptionell auf *Linux*- oder *Mac*-basierte Systeme übertragen, sofern die dort verbreiteten Binärtypen genutzt werden [Birk07] und keine Sicherheitsmechanismen aktiviert wurden, die eine Kommunikation der RFS mit dem Ermittler behindern und sich nicht auf einfache Weise umgehen lassen, wie es bei den verbreiteten PFWs für Windows-PCs der Fall ist.

Bei der Einbringung ins Zielsystem ist zu unterscheiden, ob ein etablierter Kanal der Einbringung zur Verfügung steht (z. B. Implantierung über eine Download-Verbindung) oder der Verdächtige selbst erfolgreich getäuscht werden kann, so dass er eine Datei ausführt, die die RFS (in verdeckter Weise) enthält. In beiden Fällen ist von einem geringen Aufwand (weniger als 1 Personentag) für die Einbringung auszugehen; von einem deutlich höheren Aufwand ist auszugehen, falls ein physikalischer Zugriff (z. B. nach Öffnung der Wohnung) erfolgen oder ein bisher nicht etablierter technisch-organisatorischer Kanal zur Einbringung aufgebaut werden muss, dessen Erfolgswahrscheinlichkeit zudem unbekannt ist; dies war jedoch kein Aspekt unserer Untersuchungen.

Eine Zusammenarbeit mit Herstellern von Antivirus- bzw. Antispyware-Produkten ist jedoch in keinem dieser unterschiedenen Fälle nötig, da die Schutzwirkung der Produkte (soweit der Markt von uns betrachtet wurde) unzureichend ist. Aus dem Blickwinkel der Hersteller dieser Sicherheitstools (und auch aus Sicht des Verdächtigen) stellt die RFS (in der Laborumgebung: der *Demonstrator*) eine „unerkannte“ Malware da, die ihre Schadfunktion ausführen kann, ohne dass sie von den Sicherheitsmechanismen gehindert wird. Für den Ermittler ist es eine RFS mit umfangreicher Funktionalität gegeben, die für Ermittlungen auf dem Zielsystem geeignet ist.

2.5 RFS für den Einzelfall

Im Vorfeld der gesetzlichen Neuregelung zur Online-Durchsuchung äußerte sich das Bundeskriminalamt zur (geplanten) Vorgehensweise bei Ermittlungen. Der BKA-Präsident Ziercke spricht dabei von einer „*[eigenen] Software, die immer nur für den Einzelfall erarbeitet wird, ein Unikat, das speziell auf die Rechnerumgebung eines Verdächtigen zugeschnitten ist*“ und nennt diese selbst eine *Remote Forensic Software (RFS).*

Die RFS soll für jeden Einzelfall berücksichtigen, welches Betriebssystem der Verdächtige verwendet, welche „*Umgebung*“ (so die Aussage) vorliegt und „*wie [der Verdächtige] kommuniziert*“ [Zie07]. Inwieweit die Erstellung von Unikaten für jeden Einzelfall einer Online-Durchsuchung tatsächlich die Praxis bei der Anwendung der gesetzlichen Neuregelung darstellen wird, ist bisher nicht abzusehen; die Vorgehensweise erscheint aber nach den im Abschnitt 2.3 dargestellten technischen Untersuchungsergebnissen für das dort zugrunde gelegte

Modell eines privat genutzten PCs realistisch, da die RFS mit geringem Aufwand erstellt werden kann und Software-Unikate insbesondere nicht von der Erkennung durch Virenscanner auf der Basis von Signaturdatenbanken bedroht werden.

Ob jedoch der überschaubare Personenkreis der Verdächtigen (Ziercke spricht von „*maximal zehn solcher Maßnahmen im Jahr*“), die einer solchen Maßnahme unterzogen werden, eine vergleichbare Rechnerkonfiguration verwendet oder auf spezielle Umgebungen ausweicht, wird erst die Praxis der Strafverfolgungsbehörden aufzeigen.

3 Vorgaben und technische Umsetzbarkeit

3.1 Vorgaben des Bundesverfassungsgerichtes

Das Urteil des Bundesverfassungsgerichtes hat den heimlichen Zugriff auf informationstechnische Systeme als zulässiges Mittel zur Gefahrenabwehr unter engen Voraussetzungen anerkannt. Es wurden Vorgaben formuliert, welche ein Gesetz zur Regelung des Zugriffs erfüllen muss [BVerfG07]. Da mit gewissen Erfolgsaussichten versucht werden kann, geeignete Maßnahmen gegen einen heimlichen Zugriff auf ein Zielsystem mit Hilfe einer Zugriffssoftware zu vereiteln, wurde die Eignung der Online-Durchsuchung als wirkungsvolles Ermittlungsinstrument in Frage gestellt (vgl. Buermeyer HRRS 4/2007, [Buer07]). Das BVerfG äußert hierzu seine Auffassung, dass es nicht als selbstverständlich unterstellt werden kann, dass jede mögliche Zielperson eines Zugriffs bestehende Schutzmöglichkeiten dagegen nutzt und diese auch tatsächlich fehlerfrei implementiert. Des Weiteren könnten sich in Zukunft für die Verfassungsschutzbehörde Zugriffsmöglichkeiten auftun, welche sich nur schwer oder gar nicht unterbinden lassen. Es ist also nicht zu fordern, dass diese Art von Zugriff immer oder im Regelfall Erfolg versprechend ist.

Nach dem Urteil dient der Online-Zugriff nicht „unmittelbar der Gewinnung revisionsfester Beweise für ein Strafverfahren, sondern soll der Verfassungsschutzbehörde Kenntnisse verschaffen, an deren Zuverlässigkeit wegen der andersartigen Aufgabenstellung des Verfassungsschutzes zur Prävention im Vorfeld konkreter Gefahren geringere Anforderungen zu stellen sind als in einem Strafverfahren.“ Somit ist für die Eignung der Maßnahme eine Revisionssicherheit der Beweismittel nicht zwingend gegeben.

Zu beachten ist, dass eine heimliche technische Infiltration, welche die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten ermöglicht einen Grundrechtseingriff von besonderer Schwere darstellt. Faktoren für die besondere Schwere des Grundrechtseingriffs laut Ziffern 234ff sind:

- langfristige Überwachung

  Eine Profilbildung erscheint möglich oder Sicherheitsmaßnahmen werden unterlaufen (Passwörter, Verschlüsselung), was eine Vereitelung des informationellen Selbstschutzes darstellt.

- Streuung

Sollte das Zielsystem in ein (lokales) Netzwerk eingebunden sein, so ist es denkbar, dass sich die Streubreite der Ermittlungsmaßnahme erhöht, womit sich der Wirkungsbereich der Maßnahme vergrößern kann.

- Kommunikationsüberwachung

  Eine längerfristige Überwachung der Internetkommunikation stellt gegenüber einer einmaligen Erhebung von Kommunikationsinhalten und Kommunikationsumständen einen Eingriff von wesentlich schwererem Gewicht dar.

- Heimlichkeit

  Durch die Unkenntnis der Maßnahme kann ein Betroffener keine rechtlichen Schritte ergreifen und hat keine Möglichkeit durch sein Verhalten Einfluss auf den Gang der Ermittlung zu nehmen.

- Gefahren für die Integrität des Zugriffsrechners sowie für Rechtsgüter des Betroffenen

  Gemäß den in der Verhandlung angehörten sachkundigen Auskunftspersonen besteht die Möglichkeit, dass der Zugriff selbst bereits Schäden am Zielsystem verursachen kann. So kann es z. B. zu Datenverlust kommen oder zu Schäden durch den Missbrauch der Zugriffssoftware.

- Gefahren für Rechtsgüter Dritter

  Sollte das Programm an Dritte weitergeben werden, würden deren Systeme in der Folge ebenfalls geschädigt. Des Weiteren kann es zu einem Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme geben. Es wäre möglich, dass die Ermittlungsbehörde keine Maßnahmen zur Schließung von Sicherheitslücken anregt oder aktiv darauf hinarbeitet Lücken unerkannt zu lassen. Dies könnte das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist.

Damit eine solche Maßnahme angemessen ist, müssen bestimmte Tatsachen im Einzelfall auf eine „drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt.“ (Ziffer 242)

Der Zugriff ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Dies dient der „kompensatorischen Repräsentation" der Interessen des Betroffenen im Verwaltungsverfahren, da der Betroffene im Allgemeinen auf Grund der Heimlichkeit der Durchsuchung nicht selbst von der Maßnahme weiß und somit seine Interessen nicht vertreten kann.

Für Maßnahmen wie den heimlichen Zugriff auf informationstechnische Systeme müssen hinreichende gesetzliche Vorkehrungen getroffen werden, um Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung zu vermeiden.

Dies bedeutet gemäß Ziffer 271, dass heimliche Überwachungsmaßnahmen staatlicher Stellen einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren haben, dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in ihn nicht rechtfertigen. Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und

Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen.

Für eine Überwachungsmaßnahme welche den Kernbereich privater Lebensgestaltung berühren kann, ist so weitgehend wie möglich sicherzustellen, dass Daten mit Kernbereichsbezug nicht erhoben werden. Ist es - wie bei dem heimlichen Zugriff auf ein informationstechnisches System - praktisch unvermeidbar, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann, muss für hinreichenden Schutz in der Auswertungsphase gesorgt sein. Insbesondere müssen aufgefundene und erhobene Daten mit Kernbereichsbezug unverzüglich gelöscht und ihre Verwertung ausgeschlossen werden. In der Praxis kann es jedoch zu einigen Schwierigkeiten beim Erkennen und Ausschließen des Kernbereiches kommen. Diese Schwierigkeiten ergeben sich dadurch, dass

- Daten überwiegend automatisiert erhoben werden
- technische Such- oder Ausschlussmechanismen nicht zuverlässig genug sind
- selbst bei einem Datenzugriff unmittelbar durch Personen sich praktische Schwierigkeiten ergeben, da
    - der Inhalt der erhobenen Daten nicht sicher vorhersehbar ist
    - es Schwierigkeiten geben kann Daten inhaltlich während Erhebung zu analysieren (z. B. bei fremdsprachlichen Textdokumenten oder Gesprächen)

Zur Wahrung des Kernbereichs privater Lebensgestaltung soll ein zweistufiges Schutzkonzept zum Einsatz kommen.

Die erste Stufe sieht vor, dass die Erhebung kernbereichsrelevanter Daten soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt. Hierzu sollen verfügbare informationstechnische Sicherungen eingesetzt werden und wenn Anhaltspunkte gegeben sind, dass die Datenerhebung den Kernbereich berühren wird, so hat sie grundsätzlich zu unterbleiben.

Eine Ausnahme hiervon ist dann möglich, wenn Anhaltspunkte vorhanden sind, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden die dem Ermittlungsziel unterliegen, um eine Überwachung zu verhindern.

Die zweite Stufe kommt dann zum Einsatz, wenn sich die Kernbereichsrelevanz nicht vor oder bei der Datenerhebung klären lässt. Hierfür sind geeignete Verfahrensvorschriften zu erlassen, welche die Intensität der Kernbereichsverletzung und Auswirkungen für die Persönlichkeit und Entfaltung des Betroffenen so gering wie möglich halten, falls Daten mit Bezug zum Kernbereich erhoben wurden. Sollten kernbereichsrelevante Daten erhoben worden sein, so sind diese unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Daten ist auszuschließen.

3.2 Technische Umsetzbarkeit der Vorgaben

Bei Betrachtung einer durch deutsche Ermittlungsbehörden entwickelten RFS ist die Umsetzbarkeit der technischen Vorgaben des Bundesverfassungsgerichtes an eine Remote Forensic Software zu untersuchen. Viele der in Abschnitt 3.1 genannten Punkte beziehen sich auf verfahrenstechnische Vorgaben, welche die Schwierigkeiten in der technischen Umsetzbarkeit

auffangen sollen. Ein Beispiel hierfür ist die Wahrung des Schutzes des Kernbereichs privater Lebensgestaltung, die laut den Vorgaben durch geeignete Verfahrensvorschriften sicherzustellen ist. Ebenso ist der Richtervorbehalt eine verfahrenstechnische Vorgabe und keine Vorgabe an die RFS selbst.

Insbesondere die nicht zwingend gegebene Revisionssicherheit erleichtert die Umsetzbarkeit der RFS und führt die zu entwickelnde Software weg von einer forensischen Software im klassischen Sinn hin zu einem Remote Administration Tool. Die möglicherweise vorhandene Streuwirkung der Software und die Gefahren für die Integrität des Zugriffsrechners wurden vom BVerfG bereits betrachtet und zur Kenntnis genommen. Auch hier wurde kein expliziter Mechanismus gefordert, der eine solche Streuwirkung unterbinden könnte und die Umsetzbarkeit der RFS erschweren würde.

Die Erhebung kernbereichsrelevanter Daten soll, soweit informationstechnisch und ermittlungstechnisch möglich, unterbleiben, wobei nach Möglichkeit verfügbare informationstechnische Sicherungen eingesetzt werden sollen. Hier könnten Filter- oder Suchbegriffe zum Einsatz kommen, welche jedoch nicht notwendigerweise zu den gewünschten Ergebnissen führen. Da das Sicherungskonzept jedoch zweistufig ausgelegt ist, kann eine entsprechende Wahrung des Kernbereichs auch durch verfahrenstechnische Vorschriften gesichert werden, so dass auch hier keine erhebliche technische Hürde entsteht.

Die Software muss jedoch, z. B. durch Einsatz von Verschlüsselungstechnologie, sicherstellen, dass eine Weitergabe oder Verwertung der erhobenen Daten insbesondere der kernbereichsrelevante Daten ausgeschlossen ist. Dies lässt sich jedoch durch bekannte, wissenschaftlich untersuchte Verschlüsselungsverfahren umsetzen.

4 Schlussfolgerungen

Eine Onlinedurchsuchung ist trotz üblicherweise vorhandener Sicherheitstools technisch möglich, nachdem die Installation eines RFS durch Täuschung des Verdächtigen (Nutzerseitiges Ausführen einer Datei), durch technische Hilfsmittel (Implantierung über eine Download-Verbindung) oder durch physikalischen Zugang zum PC oder einzelner Komponenten vorgenommen wurde. Trotz gegenteiliger Äußerungen seitens der Hersteller von Anti-Virus-Software stellen die Sicherheitstools keine wirksame Hürde einer Online-Durchsuchung dar, auch dann nicht, wenn die Hersteller nicht mit den Ermittlern zur Erleichterung der Durchsuchung kooperieren.

Dabei kann diese RFS durchaus für den einmaligen Einsatz mit geringem technischen Aufwand (wenige Personentage) erstellt und nur einmalig genutzt werden, um eine Erkennung durch zukünftige Versionen der Virenscanner (und ihrer Signaturdatenbanken) und Personal Firewalls zu vermeiden. Die Erstellung des RFS gelingt auch einem Ermittler, der über durchschnittliche technische Fähigkeiten und Hilfsmittel verfügt; besondere Ressourcen (außer einem eigenen PC) oder spezielles Expertenwissen sind nicht vonnöten, da die Software-Bestandteile im Internet verfügbar sind.

Bemerkenswert ist das Ergebnis aus Sicht der Autoren in der Hinsicht, dass die vielzitierten Sicherheitshinweise (Nutzer werden aufgefordert, Virenscanner und PFW *zu* installieren) nur einen geringen Schutz bieten: nicht nur gegen Online-Durchsuchungen sondern auch gegen kriminelle Angreifer, die ohne rechtliche Grundlage Durchsuchungen vornehmen, ist der Schutz gering. Zwar ist grundsätzlich zunächst dem Anwender selbst der Vorwurf zu machen,

Dateien zu öffnen, deren Herkunft er nicht zweifelsfrei verifizieren kann, die Schutzmechanismen der Sicherheitstools sind jedoch für dieses Fehlverhalten vorgesehen.

Für die technische Wirksamkeit der Online-Durchsuchung ist die tatsächliche Systemkonfiguration des zu untersuchenden Systems neben dem Nutzerverhalten des Verdächtigen von erheblicher Bedeutung. Wir konnten zeigen, dass ein in üblicher Weise konfigurierter PC trotz vorhandener Sicherheitstools unter Nutzung eines RFS-Unikates mit geringem Aufwand einer Online-Durchsuchung unterzogen werden kann, sofern ein etablierter Kanal zur Einbringung der RFS zur Verfügung steht. Inwieweit die Systemlandschaft der Verdächtigen aber diesem Modell entspricht, kann nur durch praktische Erfahrungen verifiziert werden.

Literatur und Quellen

[Birk07] Volker Birk: *Der Staat als Einbrecher: Heimliche Online-Durchsuchungen sind möglich.* Telepolis. März 2007.

[Buer07] Buermeyer, Ulf: *Die 'Online-Durchsuchung'. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme.* In: HRRS 4 (2007), S. 154-166. URL: http://www.hrr-strafrecht.de/hrr/archiv/07-04/index.php?sz=8

[BVerfG07] Bundesverfassungsgericht: *1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333).* URL: http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html. (Stand: 27.02.2008)

[Con97] Patrick Conley: *Zwischen Festplatte und Fingerabdruck.* Der Tagesspiegel vom 14.8.1997. URL: http://www.tagesspiegel.de/zeitung/Archiv;art1291,2051236

[Dfrws01] Digital Forensic Research Workshop: *A Road Map for Digital Forensic Research*, URL http://www.dfrws.org/2001/dfrws-rm-final.pdf

[Gra07] Anna Grabenströer: *„Der Bundestrojaner ist nicht vorstellbar“*. Meldung in *tagesschau.de* vom 29. August 2007 (zuletzt geändert: 15:29 Uhr). URL: http://www.tagesschau.de/inland/meldung488832.html.

[GrPu09] Ulrich Greveler und Christian Puls: *Über den Aufwand, Malware auf einem privaten PC zu installieren – Wie einfach lassen sich Virenscanner und Personal Firewalls umgehen?* 11. Deutscher IT-Sicherheitskongress des BSI. SecuMedia Verlag. Erscheint im Mai 2009 (nach Redaktionsschluss dieses Beitrages).

[OECD08] OECD: OECD Ministeral Meeting on the Future of the Internet Economy. *Malicious Software (Malware): A Security Threat to the Internet Economy*, URL http://www.oecd.org/dataoecd/53/34/40724457.pdf, 2008

[Puls08] Christian Puls: *Entwicklung und Analyse einer Remote Forensic Software*. Masterarbeit am Fachbereich Elektrotechnik und Informatik der Fachhochschule Münster, Labor für IT-Sicherheit. September 2008.

[Schü08] Anja Schütz: *Vista und Mac OS gewinnen Marktanteile*. Meldung von silicon.de, 8. Juli 2008. URL: http://www.silicon.de/mittelstand/0,39038986,39193148,00 (Stand: 11.12.2008).

[Zie07] Jörg Ziercke (Präsident des Bundeskriminalamts): *„Wir haben nichts zu verbergen“*. Stern-Interview vom 30.08.2007. Elektronisch veröffentlicht vom Bundesministerium des Innern, URL: http://www.bmi.bund.de (Stand: 01.02.2009).