**Arbeitskreis „Technische und organisatorische Datenschutzfragen“
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder**

21. September 2007

Technische Aspekte der Online-Durchsuchung

0 Vorbemerkung

Das vorliegende Dokument soll den Ablauf und die technischen Verfahren der geplanten Online-Durchsuchung erläutern und aus technischer Sicht bewerten.

In den Abschnitten 1 bis 4 wird die Online-Durchsuchung beschrieben. Diese Beschreibung basiert auf den Antworten des BMI vom 22. August 2007 zu den Fragenkatalogen des BMJ und der SPD-Bundestagsfraktion. In diesen Abschnitten werden vorwiegend Begriffe verwendet, die aus dem Fragenkatalog stammen, auch wenn sie nicht allgemein anerkannt bzw. akzeptiert sind.

Im Abschnitt 5 werden die Abläufe und Verfahren aus technischer Sicht bewertet. Die Beschreibungen und Schlussfolgerungen hat der AK Technik zusammengestellt. Die Bewertungen gehen von derzeit technisch grundsätzlich möglichen Szenarien aus. In vielen Punkten besteht allerdings noch erheblicher Klärungsbedarf.

1 Begriffe

Informationstechnisches System:	- Gegenstand der Online-Durchsuchung - System aus Hardware, Software und Daten, das der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient - kann bspw. Personalcomputer, Server, vernetzte Verbünde von Computern, Infrastrukturkomponenten (Router, Switche, DE-CIX-Einrichtungen), externe Speichermedien (z. B. CD-ROMs, DVDs, externe Festplatten, USB-Speicher), Fax-Geräte, Mobilgeräte (z. B. Handys, Smartphones, Blackberrys) betreffen
Online-Durchsuchung:	- Oberbegriff für Online-Durchsicht und Online-Überwachung
Online-Durchsicht:	- einmalige Durchsuchung eines informationstechnischen Systems
Online-Überwachung:	- Überwachung eines informationstechnischen Systems über einen gewissen Zeitraum - Inhalte aktueller Telekommunikationsvorgänge sind nicht Gegenstand der Online-Überwachung
Quellen-TKÜ:	- ausschließliche Erhebung von Telekommunikationsinhalten; betrifft nicht sonstige, auf der Festplatte abgelegte Inhalte
Remote-Forensic-Software (RFS):	- interne Bezeichnung des BKA für die zu verwendende Software

2 Phasen der Online-Durchsuchung

2.1 Technische Vorabklärung

2.1.1 Art der Informationsgewinnung

- Telekommunikationsüberwachung
- Portscan
- herkömmliche Ermittlungsmaßnahmen
- Einsatz von V-Leuten
- Einsatz von verdeckten Ermittlern

2.1.2 Art der zu beschaffenden Informationen über das Zielsystem

- Betriebssystemtyp und –version
- Internetzugang
- Browsertyp und –Version
- installierte Software (Produkte und Versionen)
- Online-Verhalten der Zielperson
- Möglichkeiten der Einbringung der RFS

2.2 Technische Vorbereitung

2.2.1 Einbringungsmöglichkeiten der RFS

2.2.1.1 Aussagen des BMI im Fragenkatalog vom 22. August 2007

Das BMI bleibt bei der Beantwortung der Fragen hinsichtlich der Möglichkeiten der Einbringung sehr unkonkret und beschränkt sich auf Aussagen wie:

„Es gibt eine Vielzahl von Einbringungsmöglichkeiten, die auf Tauglichkeit für den jeweiligen Einsatz überprüft und eventuell angepasst werden müssen."

„Eine generelle Aussage zur genauen Einbringungsmethode ist nicht möglich ..."

„Es besteht Einigkeit darüber, dass kein Interesse daran besteht, Hintertüren in Betriebs- und Anwendungssysteme einzubauen ..."

„Die Einbringung der RFS im Wege der E-Mail-Kommunikation kann je nach Einzelfall ein geeignetes Mittel darstellen."

2.3 Technische Umsetzung

2.3.1 Zielstellung

Online-Durchsicht:	Was hat die Zielperson bezogen auf ihr informationstechnisches System in der Vergangenheit gemacht?
Online-Überwachung:	Was macht die Zielperson bezogen auf ihr informationstechnisches System aktuell?

2.3.2 Informationen/Aktivitäten

Folgende Informationen sollen erhoben bzw. Aktivitäten durchgeführt werden:

Online-Durchsicht:
- Informationen über das System selbst
- auf dem Zielsystem gespeicherte Daten
- Suche nach Dateien mit bestimmten Namen

- Suche nach Dateien mit bestimmten Dateiendungen
- Suche nach Eigenschaften/Attributen (z. B. Zugriffsdaten)
- Schlüsselwortsuche
- Suche in bestimmten Verzeichnissen
- Suche nach Dateien eines bestimmten Dateityps

Online-Überwachung:
- alle Funktionen der Durchsicht und zusätzlich
- Erfassung flüchtiger Daten (Passworteingaben; Texte, die nicht übertragen werden; in Bearbeitung befindliche verschlüsselte Dateien)
- Erfassung von Klartexten vor einer Verschlüsselung
- Erfassung von Klartexten nach einer Entschlüsselung
- Einsatz von Key-Loggern zum Abfangen von Tatstatureingaben, beispielsweise von kryptographischen Schlüsseln

An den Computer angeschlossene oder mit diesem kommunizierende Geräte wie Mikrofone, Webcams oder Scanner sollen nicht überwacht werden. Mit diesen Geräten erhobene und auf dem informationstechnischen System gespeicherte Daten können jedoch Gegenstand der Durchsicht/Überwachung sein.

Online-Durchsicht und Online-Überwachung sollen sich ebenfalls nicht auf Telekommunikationsdaten erstrecken. Die technische Vorgehensweise ist vergleichbar und offensichtlich wird auch der gleiche „technische Baukasten“, wenn auch mit unterschiedlichen Bausteinen, genutzt.

Wie eine Vermischung beider Maßnahmen verhindert werden soll, wird nicht beschrieben.

2.3.3 Auswahl/Eingrenzung der zu erhebenden Informationen

Die zu sichernde Datenmenge soll anhand von vorher festgelegten Suchkriterien begrenzt werden. Folgende Möglichkeiten sollen dabei technisch umsetzbar sein:

- Erfassen der Inhalte von Dateien,
- Recherche mittels Suchbegriffen,
- Recherche in gelöschten Texten,
- Überwachung von Befehlen und genutzten Funktionen,
- Recherche nach und Erhebung von Passwörtern, Signaturen und –schlüsseln,
- Einschränkung auf ein tägliches Überwachungszeitfenster (z. B. 20 – 22.00 Uhr),
- Einschränkung auf bestimmte Nutzer.

2.3.4 Umgehungs-/Überwindungsmöglichkeiten von Kryptierungen

Das BMI sieht mehrere Möglichkeiten, Kryptierungen zu umgehen, von denen jedoch nicht alle genutzt werden sollen.

a) Abzweigen von Klar-Informationen vor der Ver- bzw. nach der Entschlüsselung
   - soll genutzt werden

b) Zugriff auf Schlüssel mit Sniffer-Software und/oder Key-Loggern
   - ist eine der vorgesehenen Online-Maßnahmen

c) Verwendung von absichtlich geschwächten Verschlüsselungsprodukten
   - „Der generelle Einbau von staatlichen Hintertüren ist derzeit politisch nicht gewollt.“

d) treuhänderische Hinterlegung von kryptographischen Schlüsseln (key escrow)
   - „... in Deutschland politisch nicht durchsetzbar... und technisch wenig erfolgversprechend...“

2.3.5 Ausleitung der Informationen

Die gewonnenen Ergebnisse werden so lange auf dem informationstechnischen System zwischengelagert, bis eine Internetverbindung durch die Zielperson hergestellt wird. Die Daten werden verschlüsselt abgelegt. Nach der Übertragung auf den Rechner der Sicherheitsbehörde werden die Daten auf dem informationstechnischen System gelöscht.

2.4 Dauer und Beendigung der Maßnahme

2.4.1 Dauer der Maßnahme

2.4.1.1 Online-Durchsicht

Die Dauer der Durchsicht und der anschließenden Übermittlung ist abhängig

- von dem Online-Verhalten der Zielperson,
- vom Durchsuchungszweck,
- von der Anzahl und der Größe der zu übertragenden Dateien,
- von der Bandbreite des TK-Anschlusses des Zielsystems,
- vom Betriebszustand des Systems,
- von den Sicherungsmaßnahmen, die die Zielperson getroffen hat.

Die Durchsicht und die anschließende Übertragung kann einen Zeitraum von wenigen Minuten bis zu mehreren Tagen in Anspruch nehmen.

2.4.1.2 Online-Überwachung

Die Überwachungsdauer ist in der Regel wesentlich länger als bei der Online-Durchsicht und soll sich aus dem dann gesetzlich festgelegten Überwachungszeitraum ergeben.

2.4.2 Zeitpunkt und Art der Beendigung

Die Maßnahme soll planmäßig beendet werden, wenn

- die erhobenen Daten als ausreichend angesehen werden,
- der ursprüngliche Verdacht entkräftet wurde,
- die Durchsuchungserlaubnis aufgehoben wurde oder
- der gesetzlich zulässige Überwachungszeitraum erreicht ist.

In diesen Fällen soll sich die RFS auf ein entsprechendes Kommando hin (manuelle Auslösung) selbst deinstallieren.

Darüber hinaus soll die RFS ein Verfallsdatum und Zähler erhalten, die eine Selbst-Deinstallation der Software gewährleisten. Auf diese Weise soll auch eine ungewollte, erneute Aktivierung der RFS etwa nach dem Wiederaufsetzen des Systems mittels Datensicherungen (Back-Up) verhindert werden.

Unter Umständen ist es erforderlich, dass die Maßnahme nicht planmäßig beendet werden muss, bspw.

- bei erfolgloser Kontaktaufnahme mit dem Zielsystem (falls bspw. keine Internetverbindung durch die Zielperson aufgebaut wird) oder bei
- (der eigentlich ausgeschlossenen) Entdeckung der RFS durch Antivirenprogramme, IDS-Systeme oder ähnliche Tools.

Die Deinstallation soll sich ausschließlich auf die RFS auswirken und keine Beeinträchtigungen des Zielsystems nach sich ziehen.

Es ist nicht beabsichtigt, den „Ursprungszustand“ des Zielsystems nach der Deinstallation der RFS herzustellen, da sich das Zielsystem während der Laufzeit der RFS ohnehin ständig verändert. Lediglich Änderungen, die die RFS an der Systemkonfiguration vorgenommen hat, sollen bei der Deinstallation der RFS rückgängig gemacht werden.

3 IT-Sicherheitsrisiko für Zielrechner

Mit der selbstentwickelten Software RFS sollen keine Daten auf dem Zielsystem manipuliert werden. Durch Hinterlegung des Quellcodes der RFS etwa beim genehmigenden Richter soll die Nachprüfbarkeit dieser Aussage in einem späteren Verfahren garantiert werden können.

Sensible Infrastrukturen in Staat und Wirtschaft sollen nicht gefährdet sein, da keine Online-Durchsuchung von Rechnern in Behörden oder Unternehmen vorgesehen ist.

Die Nutzung der RFS durch Dritte für eigene Zwecke soll nicht möglich sein, da „... die Software keine eigenen Verbreitungsroutinen und auch einen wirksamen Schutz gegen Missbrauch beinhaltet."

Es soll sichergestellt sein, dass die Software RFS „... nicht ohne erheblichen Aufwand ..." dazu veranlasst werden kann, an einen anderen als den von den Sicherheitsbehörden benutzten Server zurückzumelden und dass die Software weder von außen erkannt noch angesprochen werden kann.

Der generelle Einbau von „staatlichen Hintertüren" in Verschlüsselungsprodukte ist derzeit politisch nicht gewollt. Es besteht Einigkeit darüber, dass kein Interesse daran besteht, „Hintertüren" in Betriebs- und Anwendungssysteme einzubauen. Sie hätten nicht nur für die IT-Sicherheit, sondern auch für die deutsche Wirtschaft fatale Konsequenzen.

4 Beweissicherheit/Computer-Forensik

4.1 „Konventionelle" Beweiserhebung auf Computersystemen

Das BMI beschreibt die konventionelle Durchführung einer Datenträgeruntersuchung (DTU) nur sehr kurz:
- Kopie anfertigen,
- Verifizierung der Kopie,
- Erstellen einer Sicherheitskopie,
- Auswertungen anhand der Kopie, ausführliche Dokumentation.

4.2 Beweiskraft der Online-Durchsuchung

Das BMI hat keine Zweifel an der Beweiskraft der Online-Durchsuchung und verweist auf folgendes:

- Die Online-Durchsuchung soll lückenlos dokumentiert werden (z. B. die Einbringung der RFS, alle Remote-Zugriffe, alle auf dem Zielrechner durchgeführte Befehle).
- Die Integrität der übertragenen Daten soll durch Hash-, Verschlüsselungs- und Signaturverfahren sichergestellt werden.

Das BMI räumt jedoch ein, dass eine Wiederholung der Überwachungsaktivitäten „... wegen des dynamischen Charakters ..." der gesamten Maßnahme nicht möglich ist.

Nach Ansicht des BMI ist die Beweiskraft jedoch nicht immer relevant. Lediglich bei der Nutzung der Online-Durchsuchung im Bereich der Strafverfolgung ist die forensische Beweiserhebung Zweck der Maßnahme. Bei der Nutzung als Maßnahme zur Gefahrenabwehr ist die Erkenntnisgewinnung einziger Zweck.

5 Bewertung und Schlussfolgerungen

5.1 Einbringung der RFS

Der „Erfolg“ der Online-Durchsuchung hängt maßgeblich davon ab, ob es technisch und organisatorisch möglich ist, die RFS unbemerkt in das Zielsystem einzubringen. Nachfolgend werden die Erfolgsaussichten bei den bisher diskutierten Einbringungsmethoden diskutiert und generelle Schutzmaßnahmen erläutert.

5.1.1 Einbringungsmöglichkeiten

Da das BMI nicht detailliert auf Einbringungsmöglichkeiten eingeht (vgl. Punkt 2.2.1.1), werden hier einige Möglichkeiten vorgestellt, die – nach dem derzeitigen Stand der Technik – prinzipiell geeignet sind, fremde Rechner unbemerkt mit Software zu infiltrieren.

a) mit „Hilfe“ der Zielperson:

- verheißungsvolle E-Mails / Instant Messages mit der RFS als Anhang
- offizielle E-Mails von Behörden mit der RFS als Anhang
- E-Mails, bei denen der Absender gefälscht wurde, und dem Adressaten vertrauenswürdig erscheint
- manipulierte Web-Seiten, von denen die RFS heruntergeladen wird
- Herumliegenlassen / Zusenden von CDs, USB-Sticks und ähnlichen Datenträgern

b) ohne Hilfe der Zielperson:

- Ausnutzen von Software-Sicherheitslücken mit spezieller, auf die jeweilige Lücke zugeschnittener Software (sog. Exploits)
  - Zero-Day-Exploit: erscheint meist am selben Tag, an dem eine Sicherheitslücke allgemein bekannt wird
  - Less-Than-Zero-Day-Exploit: wird bereits vor bekannt werden einer Sicherheitslücke angeboten
- von Herstellern eingebaute Hintertüren
- Hintertüren in staatlichen E-Government-Anwendungen
- Infektion von Downloads „on the fly“
- physischer Zugriff auf den Zielrechner durch Eindringen in die von der Zielperson benutzten Räume

5.1.2 „Erfolgsaussichten“ bei der Einbringung

a) mit „Hilfe“ der Zielperson:

- verheißungsvolle E-Mails / Instant Messages mit der RFS als Anhang
  -> geringe Erfolgsaussichten, weil sensibilisierte Zielpersonen kaum solche E-Mails öffnen werden

- offizielle E-Mails von Behörden mit der RFS als Anhang
  -> geringe Erfolgsaussichten, weil sensibilisierte Zielpersonen kaum solche E-Mails öffnen werden

- E-Mails, bei denen der Absender gefälscht wurde, und dem Adressaten vertrauenswürdig erscheint
  -> mittlere Erfolgsaussichten, sofern die Zielperson dem Absender ungeprüft vertraut

- manipulierte Web-Seiten, von denen die RFS heruntergeladen wird
  -> mittlere Erfolgsaussichten, sofern die Zielperson keine Sandbox einsetzt und konfiguriert

- Herumliegenlassen / Zusenden von CDs, USB-Sticks und ähnlichen Datenträgern
  -> geringe Erfolgsaussichten, weil sensibilisierte Zielpersonen kaum ihnen unbekannte Datenträger auf Rechnern mit sensiblen Inhalten nutzen werden

b) ohne Hilfe der Zielperson:

- Ausnutzen von Software-Sicherheitslücken (bekannte Lücken oder Zero-Day-Exploits/Less-Than-Zero-Day-Exploits)
  -> mittlere Erfolgsaussichten bei bereits länger bekannten Lücken, sofern keine aktuellen Patches eingespielt wurden
  -> hohe Erfolgsaussichten bei Zero-Day-Exploits, weil Schutzmöglichkeiten noch nicht verfügbar sind
  -> sehr hohe Erfolgsaussichten bei Less-Than-Zero-Day-Exploits, weil praktisch kein Schutz möglich ist

- von Herstellern eingebaute Hintertüren
  -> geringe Erfolgsaussichten, sofern die Zielperson Open-Source-Software einsetzt

- Hintertüren in E-Government-Anwendungen
  -> geringe Erfolgsaussichten, weil die Zielpersonen solche Anwendungen kaum nutzen werden

- Infektion von Downloads „on the fly“
  -> hohe Erfolgsaussichten, da nur wenige Downloads digital signiert sind
  -> hohe Erfolgsaussichten auch bei signierten Downloads, sofern die Hersteller mitwirken

- physischer Zugriff auf die IT-Zielsysteme
  -> geringe Erfolgsaussichten bei Einzelsystemen, da ständig unter Kontrolle der Nutzer (z. B. Notebooks)
  -> hohe Erfolgsaussichten bei komplexen Systemen und Infrastrukturkomponenten, da Eingriffe nur schwer feststellbar sind

5.1.3 Generelle Gegenmaßnahmen und ihre Schutzwirkung

- Nutzung von zwei PCs (ein Online- und ein Offline-System)
  - Daten durchlaufen den Online-PC beim Senden und Empfangen nur verschlüsselt
  - Übertragung der Daten zum Bearbeiten (Lesen, Schreiben) bspw. per USB-Stick auf den Offline-PC
  -> verhindert das Auslesen mit hoher Wahrscheinlichkeit

- Live-System von CD/DVD
  - dauerhafte Änderungen am Betriebssystem mit Hilfe der RFS sind nicht möglich
  - nach jedem Neustart von CD/DVD ist der Originalzustand wieder hergestellt
  -> verhindert das Auslesen mit hoher Wahrscheinlichkeit

- Nutzung eines virtuellen Zweitsystems
  - geschützte Umgebung für das Betriebssystem
  - sicherer Kanal in das Gastsystem möglich
  -> verhindert das Auslesen aus der geschützten Umgebung mit hoher Wahrscheinlichkeit

- Einsatz von Virenscannern
  - einfache Scanner finden nur Schadsoftware mit bekannten Mustern (Signaturen)
  -> RFS soll hochspezialisiert sein und von handelsüblichen Scannern angeblich nicht entdeckt werden

  - gute Produkte suchen nicht nur nach bekannten Mustern, sondern versuchen, das Verhalten von Software zu analysieren (proaktive Verfahren wie Heuristik oder Sandbox-Technologie)
  -> ob hier die RFS unentdeckt bleibt, ist zumindest fraglich

- Einsatz von Intrusion Detection Systemen (IDS)
  - erkennen von Angriffsmustern und von Veränderungen der Systemkonfiguration
  - schon das Erkennen der Tatsache, dass ein System verändert wurde, könnte auf die RFS hindeuten
  -> ob hier die RFS unentdeckt bleibt, ist zumindest fraglich

- Einsatz von Firewalls
  - vom Nutzer zugelassene Kommunikation (E-Mails, Downloads) werden nicht unterbunden
  - verschlüsselter Datenverkehr ist ebenfalls nicht filterbar
  -> Schutz vor RFS kaum realisierbar

- Einsatz des TPM (Trusted Platform Modul)
  - erlaubt dem Betriebssystem, Veränderungen zu erkennen
  - gewollte Downloads werden möglicher Weise nicht als Risiko erkannt
  - Hintertüren von Softwareherstellern werden nicht erkannt
  -> Schutz vor RFS zur Zeit nicht abschließend bewertbar

- Nutzung des Systems ausschließlich nach Anmeldung mit Kennung und Passwort
  - bei Nutzerkennungen ohne Admin-Rechten können Installationsmöglichkeiten eingeschränkt werden
  - Software-Installation nur mit Admin-Rechten zulassen
  -> erschwert das Einbringen der RFS unter bestimmten Umständen

- komplette Festplattenverschlüsselung
  - Installationsmöglichkeiten insbesondere bei physikalischem Zugriff kaum gegeben
  -> erschwert das Einbringen der RFS unter bestimmten Umständen

5.2 Reichweite der Eingriffe

Die Tatsache, dass nicht nur Personalcomputer sondern beispielsweise auch Server (bspw. Mailserver), vernetzte Verbünde von Computern und komplexe Infrastrukturkomponenten (z. B. Router, Switche, DE-CIX-Einrichtungen) von der Online-Durchsuchung betroffen sein können (vgl. Punkt 1), verdeutlicht die Reichweite und damit die Eingriffstiefe dieser Maßnahme. Werden derartige IT-Komponenten überwacht muss davon ausgegangen werden, dass nicht nur Einzelpersonen, sondern immer eine kaum einzugrenzende Anzahl von Betroffenen überwacht wird. Das BMI weist zwar darauf hin, dass bei Systemen, die unter der administrativen Betreuung Dritter stehen, anstelle der Online-Überwachung grundsätzlich der direkte Weg zu den jeweiligen Stellen gesucht würde, der aktuelle Gesetzentwurf schließt den Einsatz der RFS jedoch auch hier nicht aus.

Zudem lässt sich die Reichweite schon deshalb kaum einschätzen, weil es einer konkreten Definition des Begriffs „Verbund“ mangelt. Es kann sich dabei sowohl um ein kleines lokales Netz handeln als auch um ausgedehnte Firmen-Netze (Intranets). Dass unter diesen Voraussetzungen die Online-Durchsuchung nicht einmal mehr auf Deutschland beschränkt werden kann, bleibt vom BMI völlig unerwähnt.

Im übrigen ist bereits bei der Online-Durchsuchung von Einzelsystemen wie Personalcomputern oder Laptops davon auszugehen, dass nicht nur Einzelpersonen überwacht werden. Auch in diesen Fällen ist nicht auszuschließen, dass mehrere Personen das System nutzen, und somit von der Maßnahme betroffen sind.

Die Reichweite der Eingriffe kann auch anhand der Art zu erhebenden Informationen (vgl. Punkt 2.3.2) verdeutlicht werden. Die Suche nach bestimmten Dateien bedeutet nämlich in der Praxis, dass bspw. gezielt nach E-Mail-Adressbüchern, Kontaktlisten, Logdateien, Schlüsselbünden, Konfigurationsdateien, Cache-Dateien, Browser-Historien oder Sicherheitskopien gesucht werden kann.

5.3 IT-Sicherheitsrisiko für den Zielrechner

Da grundsätzlich zu bezweifeln ist, dass eine komplexe Software wie die RFS vollständig fehlerfrei programmiert wurde, ist äußerst fraglich, ob

- die Software weder durch Antivirenprogramme noch durch IDS-Systeme entdeckt werden kann,
- die Nutzung der RFS durch Dritte für eigene Zwecke wirklich ausgeschlossen werden kann,
- die RFS nicht doch dazu veranlasst werden kann, Daten an einen anderen als den von den Sicherheitsbehörden benutzten Server zu senden und ob
- die Software tatsächlich einen wirksamen Schutz gegen Missbrauch beinhaltet (vgl. Punkt 3).

Im übrigen schließt das BMI nicht vollständig aus, dass die RFS missbraucht werden kann. Zitat: „Speziell wird sichergestellt, dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen als den von den Sicherheitsbehörden benutzten Server zurückzumelden und dass die Software weder von außen erkannt noch angesprochen werden kann.“ Wie hoch der Aufwand tatsächlich ist, wäre zu prüfen.

Jedenfalls ist das BMI in der Pflicht, belastbare Nachweise für die Behauptungen vorzulegen, dass

- tatsächlich keine Daten auf dem Zielsystem manipuliert werden,
- sensible Infrastrukturen in Staat und Wirtschaft nicht gefährdet sind,
- die Nutzung der RFS durch Dritte für eigene Zwecke nicht möglich ist,
- die Software nicht dazu veranlasst werden kann, an einen anderen als den von den Sicherheitsbehörden benutzten Server zurückzumelden,
- die Software weder von außen erkannt noch angesprochen werden kann und
- keine Hintertüren oder absichtlich eingebaute Schwachstellen in Hard- und Software verwendet werden.

5.4 Beweissicherheit

5.4.1 Konventionelle Computer-Forensik

Um elektronisch gespeicherte Daten auf Computersystemen als rechtskräftige Beweise verwenden zu können, sind eine Reihe technisch-organisatorischer Anforderungen umzusetzen. Hansen/Krause erläutern den Ablauf wie folgt:

In der Regel sind vier Schritte erforderlich:

1) Identifizierung
- Klärung, welche Informationen als Beweise erhoben werden sollen
- Festlegen der Vorgehensweise und der Mittel/Werkzeuge

2) Sicherstellung
- Sicherstellung der Zielrechner in Anwesenheit von Zeugen und ggf. Eigner
- ggf. Sicherstellung weiterer Dateninhalte aus flüchtigen Speichern vor der Abschaltung des Systems
- Sicherung der Datenträger gegen nachträgliche Veränderungen (z. B. Schreibschutz, kryptographische Verfahren zur digitalen Signatur)
- Erstellen eine Image Kopie

3) Analyse
- die Analyse durch sachverständige Kriminaltechniker
- Analyse nie am Originalsystem sondern immer an der Kopie

4) Aufbereitung und Präsentation
- Zusammenfassung der Analyse in einem Bericht

5.4.2 Beweissicherheit der Online-Durchsuchung

Im Gegensatz zur konventionellen Computer-Forensik, die auf die garantierte Unverändertheit des Untersuchungsgegenstandes setzt, ist bei der Online Durchsuchung die Veränderung des Untersuchungsgegenstandes – bedingt durch das Einbringen der RFS – die Voraussetzung für die Beweiserhebung. Schon diese Tatsache widerspricht allen Vorgaben der klassischen Computer-Forensik. Ob mit dem Start der RFS auf dem Zielsystem tatsächlich (weitere) Änderungen sicher ausgeschlossen werden können (vgl. Punkt 3), kann kaum zweifelsfrei bewiesen werden. Damit ist auch der Beweiswert der erhobenen Daten äußerst fraglich.

Ob es darüber hinaus möglich ist, die zu untersuchenden Daten bei der Übertragung zum Server der Sicherheitsbehörde verlässlich vor Manipulation und Veränderung zu schützen, ist fraglich. Es dürfte kaum möglich sein, auf einem fremdkontrollierten Zielsystem (nämlich durch die Zielperson) verlässlich kryptographische Verfahren wie etwa die digitale Signatur durchzuführen.

Auch die angeblich lückenlose Protokollierung aller Aktivitäten und die Hinterlegung des Quellcodes der RFS (vgl. Punkt 4.2) kann nicht garantieren, dass Daten auf dem Zielsystem verändert werden – und sei es durch Software-Fehler in der RFS oder im Betriebssystem des Zielsystems.

Der Nutzen der Hinterlegung des Quellcodes ist ohnehin mehr als fragwürdig. Mit dieser Maßnahme will das BMI offenbar sicherstellen, dass der Quellcode im Bedarfsfall vollständig analysiert werden kann. Zieht man jedoch in Betracht, dass eine Quellcodeanalyse einen erheblichen Aufwand an Zeit und hochqualifiziertem Fachpersonal erfordert, wird eine solche Analyse wohl kaum vor dem Einsatz der Software angefordert werden. Vielmehr ist anzunehmen, dass lediglich eine nachträgliche Quellcode-Analyse angefordert wird, um bspw. in einem strafrechtlichen Verfahren die „ordnungsgemäße" Funktion der RFS beweisen zu können.

Doch selbst dieser Beweis muss unvollständig bleiben. Es ist davon auszugehen, dass der Vorgang der Online-Durchsuchung von den Sicherheitsbehörden von außen „gesteuert" wird. So wird beispielsweise die Möglichkeit bestehen, durch „Nachladen" von Softwarekomponenten im Laufe der Online-Durchsuchung die Originalsoftware zu verändern, um sie aktuellen Anforderungen entsprechend anpassen zu können (etwa Nachladen erweiterter Suchkriterien). Dass durch diese Maßnahme der Beweiswert des hinterlegten Quellcodes nichtig ist, versteht sich von selbst.

Der Beweiswert der mit der Online-Durchsuchung erhobenen Daten bleibt daher in jedem Fall äußerst fragwürdig.

5.5 Schutz des Kernbereichs der privaten Lebensgestaltung

Dass eine Online-Durchsuchung solche Bereiche unberücksichtigt lässt, die durch bestimmte Dateinamen oder Dateiendungen adressiert werden, ist kaum anzunehmen. Allein die Tatsache, dass eine Datei mit „Liebesbrief.doc" bezeichnet ist, wird sicher nicht dazu führen, dass Inhalte dieser Datei nicht an den Server der Sicherheitsbehörde übertragen werden.

Auch die Suche nach Eigenschaften/Attributen wird kaum zu Einschränkungen führen, weil eine verlässliche Schlussfolgerung auf Inhalte nicht möglich ist.

Ebenso ist die Suche nach Schlüsselworten, die Suche in bestimmten Verzeichnissen oder die Suche nach Dateien eines bestimmten Dateityps keine geeignete Methode, Daten aus dem Kernbereich der privaten Lebensgestaltung zu schützen.

Selbst wenn Erkennungsalgorithmen entwickelt werden könnten, in deren Ergebnis der Kernbereich definiert werden kann, wäre immer eine Durchsuchung des Gesamtdatenbestandes nötig, um entsprechende Indexierungen zu ermöglichen. Es ist somit kein technisches Verfahren erkennbar, mit dem ein „automatisierter Kernbereichsschutz" realisiert werden kann.

Das BMI räumt folgerichtig ein, dass „... der Schutz des Kernbereichs anderer Nutzer wie auch des Beschuldigten allein mit technischen Mitteln nicht abschließend garantiert werden kann...", und dieser Schutz nur im Rahmen der Auswertung der erhobenen Daten gewährleistet werden kann.

Im Ergebnis ist festzustellen, dass der Kerbereich der privaten Lebensgestaltung bei einer Online-Durchsuchung durch technische Mittel nicht angemessen geschützt werden kann.

Die Erklärungen des BMI und des BKA zur Zahl der zu erwartenden Online-Durchsuchungen (bisher wird von maximal 10 Maßnahmen pro Jahr gesprochen) darf nicht dazu führen, den Eingriff in den Kernbereich der privaten Lebensgestaltung zu verharmlosen und in der Folge die Online-Durchsuchung zu legitimieren. Selbst wenn die Online-Durchsuchung – angesichts geringer Fallzahlen – als angemessenes Mittel zur Terrorismus- bzw. Extremismusbekämpfung angesehen werden würde, darf nicht außer acht bleiben, dass der technische Fortschritt sehr schnell dazu führen kann, dass die Online-Durchsuchung zu einem Standardwerkzeug der Sicherheitsbehörden werden kann. Dann wäre vor dem Hintergrund der

jetzigen technischen Möglichkeiten ein Eingriffsinstrument legitimiert worden, das bei fortschreitender Technikentwicklung völlig unangemessen wäre.

Im übrigen ist angesichts der künftig abnehmenden Anzahl der Festnetzanschlüsse und der zunehmenden Kommunikation per IP-Telefonie ohnehin zu hinterfragen, welche Fallzahlen künftig zu erwarten sind und ob die bisher vom BMI betonte Trennung der Online-Durchsuchung von der „Quellen-TKÜ“ Bestand haben wird. Aus den Aussagen des BMI zum Problem der verschlüsselten Kommunikation wird deutlich, dass die mit der RFS verbundenen technischen Möglichkeiten die Grundlage darstellen sollen, um angesichts der technischen Entwicklungen (Konvergenz der Netze, Verschlüsselung, Vielfalt der Kommunikationsdienste) die Strafverfolgungsbehörden technisch nicht den Anschluss verlieren zu lassen und ihnen die Möglichkeiten zu erhalten, über die sie gegenwärtig bei der TKÜ verfügen.

5.6 Auswirkungen auf das Vertrauen in die IT-Infrastruktur und Folgen für die Akzeptanz von E-Government-Verfahren

IT-Sicherheit und Datenschutz sind die zentralen Akzeptanzkriterien der sich herausbildenden Informationsgesellschaft und der weltweiten Daten- und Kommunikationsnetze. Eine Folge der heimlichen Online-Durchsuchung wird eine tiefgreifende Vertrauenskrise sein. Bürgerinnen und Bürger und möglicherweise auch Unternehmen werden nicht mehr bereit sein, staatliche E-Government-Angebote zu nutzen, da sie den Missbrauch dieser Verfahren für die Zwecke der Online-Durchsuchung befürchten.

So hat beispielsweise die Finanzverwaltung schon jetzt massive Bedenken geäußert, dass ihre Bemühungen um die breite Nutzung der elektronischen Steuererklärung (ELSTER) durch die Diskussionen um die Online-Durchsuchung konterkariert werden. Schon jetzt – vor dem Einsatz der Online-Durchsuchung – werden sinkende Nutzungszahlen erwartet.

Selbst die elektronische Kommunikation zwischen Bürgerinnen und Bürgern bzw. Unternehmen mit staatlichen Stellen per E-Mail wird künftig gemieden werden, weil das BMI nicht ausschließt, das die RFS mittels E-Mails verbreitet wird.

Auch die elektronische Kommunikation mit der Wirtschaft wird in Mitleidenschaft gezogen werden. Wenn Kunden sich nicht mehr der Vertraulichkeit der elektronischen Kommunikation sicher sein können, werden sie wieder auf die konventionelle Kommunikationswege zurückgreifen. Sie werden dann möglicherweise auf Anwendungen wie Online-Banking und E-Commerce-Verfahren verzichten.

Zudem ist zu befürchten, dass etwa Personalcomputer nicht mehr auf dem aktuellen Sicherheitsstand gehalten werden. Aus Furcht vor infiltrierten Downloads könnten Nutzer beispielsweise auf die regelmäßigen Sicherheits-Updates verzichten. Dies wird zu einem Anstieg der Computerkriminalität führen, da Sicherheitslücken nicht mehr beseitigt werden.

Das BMI weist zwar darauf hin, dass so genannte Hintertüren nicht eingebaut werden sollen. Es ist jedoch – zumindest aus technischer Sicht - mit ziemlicher Sicherheit davon auszugehen, dass vorhandene Hintertüren und unveröffentlichte Sicherheitslücken genutzt werden. Insbesondere damit konterkariert das BMI jedoch die Beteuerungen der Bundesregierung, den Bürgern und der Wirtschaft eine sichere und vertrauenswürdige IT-Infrastruktur zur Verfügung zu stellen. Es ist nämlich zu befürchten, dass (evtl. zunächst nur) dem BMI bekannte Sicherheitslücken nicht so schnell wie möglich publiziert werden, damit Schutzmaßnahmen ergriffen werden können, sondern dass diese Lücken bewusst über längere Zeit offen gehalten werden, um sie für die Zwecke der Online-Durchsuchung zu nutzen. Damit kann insbesondere der Wirtschaft erheblicher Schaden zugefügt werden (Stichwort Computer-Spionage). Die Wahrscheinlichkeit ist nämlich sehr hoch, dass das BMI gerade nicht exklusive „Nutzungsrechte“ an solchen Sicherheitslücken hat.

Fraglich ist in diesem Zusammenhang auch, welche Rolle das Bundesamt für Sicherheit in der Informationstechnik (BSI) künftig spielen soll bzw. noch spielen kann. Das BMI weist zwar ausdrücklich darauf hin, dass das BSI angewiesen wurde, sich nicht aktiv an der Entwicklung der für die Online-Durchsuchung einzusetzenden Software zu beteiligen. Ob das BMI tatsächlich dauerhaft auf den

Sachverstand des BSI verzichtet wird, darf zumindest bezweifelt werden. Das Vertrauen in das BSI als glaubwürdigem Berater in Fragen der IT-Sicherheit ist schon jetzt sowohl in der Wirtschaft als auch bei Bürgern nachhaltig beeinträchtigt.

Schließlich darf nicht außer acht gelassen werden, dass auch Kriminelle das Verfahren der Online-Durchsuchung oder zumindest bewusst in Kauf genommene Sicherheitslücken nutzen werden. Die Tatsache, dass Sicherheitsbehörden beharrlich davon ausgehen, dass die Online-Durchsuchung technisch durchführbar ist, wird Kriminelle in zunehmendem Maße veranlassen, sich diese Methode für ihre Zwecke nutzbar zu machen. Selbst wenn die Online-Durchsuchung für Sicherheitsbehörden nicht verwendet werden dürfte – etwa in Folge einer Entscheidung des Bundesverfassungsgerichts – ist selbstverständlich davon auszugehen, dass Kriminelle alle technischen Möglichkeiten künftig nutzen werden.

Schon allein dieser Aspekt verdeutlicht, wie wichtig es künftig sein wird, alle Nutzer von Informations- und Kommunikationstechnik weiter zu sensibilisieren. Es ist auch Aufgabe der Datenschutzbeauftragten des Bundes und der Länder, sowohl die Verantwortlichen in Wirtschaft und Verwaltung als auch Bürgerinnen und Bürger zu informieren und zu beraten, um auch dadurch ein höheres Sicherheitsbewusstsein zu erreichen.