Bundesministerium des Innern Berlin, den 22. August 2007

Fragenkatalog des Bundesministeriums der Justiz

Vorbemerkung

Die Antworten beziehen sich auf die vorgesehenen Tätigkeiten des Bundeskriminalamtes im Rahmen seiner Präventivbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus.

Ferner stehen die in der Folge getätigten Aussagen zu der Funktionsweise der Remote Forensic Software (RFS), so die interne Bezeichnung des Bundeskriminalamtes für die dabei zu verwendende Software, unter dem Vorbehalt, dass sich diese Software im Rahmen eines Projektes (Proof of concept) noch in der Entwicklung befindet und aufgrund des gegenwärtig verfügten Entwicklungsstopps noch nicht fertig gestellt ist. Die Antworten basieren daher auf bisher festgelegten Designkriterien und bereits fertig gestellten Teilmodulen.

Zudem wird angemerkt, dass im Fragebogen selbst durch eine Unterscheidung zwischen der Online-Durchsicht als einmaligem Akt und der Online-Überwachung als Überwachung über einen gewissen Zeitraum eine strikte Trennung vorgenommen wird. Diese Unterscheidung basiert auf den bisherigen Ergebnissen der Arbeitsgruppe des Bundesministeriums des Innern und des Bundesministeriums der Justiz. Diese Sichtweise ist indes nicht zwingend, da die Online-Überwachung, sofern sie keine Telekommunikation erfasst, als eine auf eine gewisse Dauer angelegt Maßnahme in erster Linie eine Vertiefung des Grundrechtseingriffs darstellt, jedoch keine substanzielle Wesensänderung der Maßnahme hervorrufen würde. Insoweit müsste lediglich zwischen einer Online- Durchsuchung und der Quellen- Telekommunikationsüberwachung (Quellen-TKÜ) unterschieden werden. Gleichwohl wird die bisherige Unterscheidung zwischen Online-Durchsicht und Online-Überwachung bei der Beantwortung der Fragen zugrunde gelegt. Im Folgenden wird daher der Begriff **Online-**

Durchsuchung als Oberbegriff für die **Online-Durchsicht** und die **Online-Überwachung** verwendet.

Unter der **Online-Durchsuchung** wird die verdeckte Suche unter Einsatz elektronischer Mittel nach verfahrensrelevanten Inhalten auf informationstechnischen Systemen verstanden, die sich nicht im direkten physikalischen Zugriff der Sicherheitsbehörden befinden, aber über Kommunikationsnetze erreichbar sind. Die zu erlangenden Inhalte sind nicht Gegenstand eines aktuellen Telekommunikationsvorgangs, wie etwa Dateien die nicht für einen elektronischen Versand bestimmt sind.

Von der Online-Durchsuchung ist die **Quellen-TKÜ** zu unterscheiden, bei der Telekommunikationsinhalte und nicht sonstige, etwa auf der Festplatte abgelegte, Daten erhoben werden, die anderen rechtlichen Regelungen unterliegt.

Fragenkatalog

I. Online-Durchsicht ➔ ein „informationstechnisches System“[1] soll einmalig durch- sucht werden

Was ist Gegenstand der Durchsicht?

- ***Was ist unter einem informationstechnischen System zu verstehen?***

  Der Begriff „informationstechnisches System“ wurde bewusst weit gewählt, um der derzeitigen und zukünftigen technischen Entwicklung Rechnung tragen zu können. Darunter wird ein System verstanden, welches aus Hard- und Software sowie aus Daten besteht, das der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient.

[1] Der Begriff wird vom BMI im Rahmen der Überlegungen zur Regelung der „Online-Durchsuchung“ im BKAG-E gebraucht.

- ***Sind „nur“ Personal-Computer“ (PC) gemeint (wie wird dieser Begriff technisch definiert?)***

  Ein Personal Computer, kurz PC, ist ein Einzelplatzrechner, der im Gegensatz zu einem Großrechner/Server zu einem bestimmten Zeitpunkt von einer einzelnen Person bedient, genutzt und gesteuert werden kann. Von der Online-Durchsuchung ist allerdings nicht nur der PC umfasst, sondern vielmehr alle informationstechnischen Systeme im Sinne der Definition.

- ***Sollen auch „Server“ durchsucht werden können (wie wird dieser Begriff technisch definiert?)***

  Der Begriff „Server“ (engl. to serve = bedienen) bezeichnet einen Computer, der anderen Computern bzw. deren Benutzern Dienste anbietet. So stellt z. B. ein Web-Server Internetseiten zur Verfügung. Auf einen Server greifen in der Regel mehrere Benutzer zu. Je nach Fallkonstellation können auch Server von der Online-Durchsuchung umfasst werden, die nach der o. a. Definition „informationstechnische Systeme“ darstellen.

  Der Einsatz der RFS auf Systemen, die der Kontrolle unbeteiligter Dritter unterstehen (Administratoren), scheidet indes grundsätzlich bereits aus taktischen Erwägungen und fehlender Erforderlichkeit aus. Insoweit ist darauf hinzuweisen, dass etwa in Fällen, in denen eine Zielperson den Rechner einer Behörde, einer Universität oder in eines Unternehmens nutzt, aus taktischen Gründen keine verdeckte Online-Durchsuchung veranlasst würde. Vielmehr würde eher die Einbindung der dortigen Systemadministration erfolgen.

- ***Sollen auch externe Speichermedien durchsucht werden können, z. B.***
  - ***CD-Roms, DVDs, die in entsprechende PC-Laufwerke eingelegt sind***
  - ***in einem Homenetwork eingebundene externe Festplatten***

  Ja, es ist grundsätzlich beabsichtigt, lokal angeschlossene externe Speichermedien durchsuchen zu können. In einem lokalen Netzwerk wird technisch keine Unterscheidung getroffen zwischen physikalisch angeschlossenen ex-

ternen oder internen Speichermedien und über Netzwerkverbindungen angeschlossene Speichermedien. Es können grundsätzlich alle ins System eingebundenen Speichermedien durchsucht werden.

- ***Sollen auch Faxgeräte und Anrufbeantworter erfasst werden? Sind dies informationstechnische Systeme?***

  Bei Faxgeräten und Anrufbeantwortern handelt es sich auch um informationstechnische Systeme, sofern sie Daten in digitaler Form abspeichern. Diese Geräte wären aber, sofern es sich bei den zu erlangenden Daten um Telekommunikationsdaten handelt, Ziel einer Telekommunikationsüberwachung und nicht einer Online-Durchsuchung.

- ***Lässt sich auch das Internet als Ganzes als informationstechnisches System verstehen?***

  Im Sinne der obigen Definition eines „informationstechnischen Systems“ handelt es sich auch beim Internet um ein solches System. Zielrichtung der Online-Durchsuchung ist aber nicht die Überwachung oder Durchsuchung des gesamten Internet. Eine solche Maßnahme wäre weder technisch noch organisatorisch durchführbar. Grundsätzlich muss die Maßnahme dem Gebot der Verhältnismäßigkeit entsprechend geeignet sein, um die Gefahr abwehren zu können.

- ***Sollen nur privat genutzte informationstechnische Systeme oder auch anderweit genutzte informationstechnische Systeme erfasst werden? Ggf.: Wie lassen sich diese unterscheiden?***

  Die Online-Durchsuchung soll sich gemäß ihrem Zweck als Maßnahmen der Gefahrenabwehr gegen das von einer bestimmten Zielperson genutzte informationstechnische System richten, das im Wege vorheriger Ermittlungen bestimmt wurde. Im Zuge dieser Vorermittlungen würden auch Informationen darüber erlangt, ob das informationstechnische System ausschließlich privat genutzt wird. Eine Beschränkung auf rein privat genutzte informationstechnische Systeme wäre unter dem Gesichtspunkt der Effektivität der Gefahrenabwehr aber in bestimmten

Fällen nur unzureichend. Ausschlaggebend muss vielmehr sein, ob Informationen erlangt werden, die zur Abwehr der Gefahr erforderlich sind. Auch im Rahmen einer Telekommunikationsüberwachung wird eine Beschränkung auf etwa rein privat genutzte Telekommunikationsanschlüsse nicht vorgenommen. Selbstverständlich wären die Regelungen zum Schutz der Berufsgeheimnisträger aber auch hier zu beachten.

- ***Sind die in einem Internetcafe vorhandenen Computer in ihrer Gesamtheit <u>ein</u> informationstechnisches System?***

  Gemäß der obigen Definition ist jeder einzelne Computer als auch ein vernetzter Verbund von Computern ein informationstechnisches System.

- ***Wie lange kann eine „Durchsicht“ und die anschließende Übermittlung an die Bedarfsträger insgesamt dauern?***

  Die Dauer der „Durchsicht“ und der Übermittlung ist abhängig
  - vom Onlineverhalten des von der Maßnahme Betroffenen,
  - vom Durchsuchungszweck,
  - von der Anzahl und der jeweiligen Größe der zu übertragenden Dateien,
  - von der zur Verfügung stehenden Bandbreite des Telekommunikationsanschlusses über den die Daten übertragen werden sollen,
  - vom Betriebszustand des Systems und
  - den von der Zielperson getroffenen Sicherungsmaßnahmen.

  Dabei muss Sorge dafür getragen werden, dass sowohl die Suche als auch die Übertragung der Ergebnisse dieser Suche keine Auffälligkeiten im Zielsystem entwickeln, um das Entdeckungsrisiko möglichst gering zu halten. Die Übertragung der Daten wie auch die Durchsicht des Datenbestandes kann jeweils von wenigen Minuten bis hin zu mehreren Tagen dauern.

II. Online-Überwachung ➔ ein „informationstechnisches System“ soll über einen gewissen Zeitraum überwacht werden

Soll eine solche Überwachung ermöglicht werden? Wenn ja:

- ***Was soll genau Gegenstand der Überwachung sein? Derselbe Gegenstand wie bei der Online-Durchsicht? Unterschiede?***

  Der Gegenstand der Online-Überwachung ist identisch mit dem der Online-Durchsicht. Es handelt sich auch dabei um ein „informationstechnisches System“ im Sinne der obigen Definition. Die Maßnahmen unterscheiden sich lediglich in Bezug auf den Zweck: Bei der Online-Durchsicht soll der Status Quo ermittelt werden („Was hat die Zielperson bezogen auf ihr Informationssystem/ihren Rechner in der Vergangenheit gemacht?“). Bei der Online-Überwachung sollen über einen gesetzlich festgelegten Zeitraum die Aktivitäten des Nutzers protokolliert werden („Was macht die Zielperson bezogen auf ihr Informationssystem/Rechner aktuell?“). Dabei können folgende Informationen erhoben und Aktivitäten durchgeführt werden:

  Online-Durchsicht

  - Sysinfo (Informationen über das System an sich)
  - auf dem Zielsystem gespeicherte Dateien
  - Suche nach Dateien mit bestimmten Namen
  - Suche nach Dateien mit bestimmten Dateiendungen
  - Suche nach Eigenschaften/Attributen (Zugriffdaten etc.)
  - Schlüsselwortsuche
  - Suche in bestimmten Verzeichnissen
  - Suche nach Dateien eines bestimmten Dateityps

  Online-Überwachung

  Alle Funktionen der Durchsuchung, zusätzlich

  - Erfassung flüchtiger Daten (Passworteingaben, Texte, die nicht übertragen werden, in Bearbeitung befindliche verschlüsselte Dateien)
  - Erfassung von Klartextdaten vor einer Verschlüsselung
  - Erfassung von Klartextdaten nach einer Entschlüsselung

- ***Sollen alle Eingaben / Ausgaben beim jeweiligen System erfasst werden? Wenn nein: Welche konkreten Eingaben / Ausgaben sollen erfasst werden?***

  Abhängig vom Überwachungszweck können alle Ein- und Ausgaben, je nach Bedarf und an die jeweilige Maßnahme angepasst, erfasst werden. Auch hierbei ist zu berücksichtigen, dass die Erfassung der Ein- und Ausgaben keine Auffälligkeiten im Zielsystem entwickeln sollen, um das Entdeckungsrisiko möglichst gering zu halten. Aus dem gleichen Grund soll auch hier die Datenmenge gering gehalten werden.

- ***Soll sich die Überwachung auch auf Ein- und Ausgaben erstrecken, die Gegenstand der Telekommunikation sind (z. B. bei der Internettelefonie oder dem Versand/Empfang von E-Mails?)***

  Online-Durchsicht und Online-Überwachung sollen sich nicht auf Telekommunikationsdaten erstrecken. Darin liegt die inhaltliche Abgrenzung zur Quellen-TKÜ. Bei der Überwachung der Telekommunikation, etwa bei Skype (Voice over IP, Übertragung erfolgt grundsätzlich verschlüsselt) handelt es sich um eine Telekommunikationsüberwachung, die sich entsprechend der bestehenden gesetzlichen Regelungen gestaltet. Eine Online-Durchsuchung oder eine Online-Überwachung stellt dies nicht dar, auch wenn die technische Vorgehensweise vergleichbar ist. Damit werden im Rahmen einer Online-Durchsuchung oder Online-Überwachung keine Ein- und Ausgaben erfasst, die Gegenstand eines Telekommunikationsvorgangs sind. Hierfür stehen andere Rechtsgrundlagen zur Verfügung.

- ***Soll die Überwachung auch Eingaben einbeziehen, die über an den Computer angeschlossene oder mit diesem kommunizierende Mikrofone, Webcams und Scanner erfolgen? Ggf.: Wie kann die Abgrenzung zur technischen (optischen und akustischen) Wohnraumüberwachung erfolgen?***

  Eine Überwachung dieser Geräte soll nicht stattfinden. Wenn jedoch unter Zuhilfenahme dieser Geräte vom Benutzer Dateien erstellt werden, etwa durch Eins-

cannen und Abspeichern von Dokumenten oder durch die Aufnahme einer Webcam, könnten diese Daten (später) im Rahmen der Online-Durchsuchung erfasst werden. Es ist allerdings technisch möglich, solche Daten, die durch angeschlossene Geräte erzeugt werden, im Selektionsvorgang auszuschließen.

Eine Wohnraumüberwachung wird dem Ziel der Erfassung bestimmter Vorgänge innerhalb der Wohnung durchgeführt, während es bei der Online-Durchsuchung und Online-Überwachung um die Erhebung von Daten aus einem informationstechnischen System geht. Die Maßnahmen sind bereits von ihrer Zielrichtung her unterschiedlich wie auch vom Einsatz der technischen Mittel.

- ***Wenn nein*: *Was ist der Grund für diese Beschränkung des Anwendungsbereichs?***

  Wie bereits ausgeführt ist die Zielrichtung einer Wohnraumüberwachung eine andere. Welche Maßnahme zu wählen ist, richtet sich nach dem Vorliegen der jeweiligen rechtlichen Voraussetzungen sowie der taktischen Möglichkeiten und Gegebenheiten.

- ***Ist es richtig, dass die Internettelefonie zunehmend verschlüsselt erfolgt und eine solche Verschlüsselung bei der Internettelefonie zwischen zwei Nutzern der Internettelefoniesoftware „Skype“ der Regelfall ist?***

  Sowohl bei kommerziellen VOIP-Lösungen als auch bei den sogenannten Messengerprogrammen kommen vermehrt Verschlüsselungsmodule zum Einsatz. Die Software Skype überträgt die Sprachdaten generell verschlüsselt.

- ***Auf welche technische Weise soll solche verschlüsselte Internettelefonie so überwacht werden, dass hieraus verwertbare (unverschlüsselte) Ergebnisse erzielt werden?***

  Unverschlüsselte Ergebnisse der Internettelefonie lassen sich nur durch Abgreifen der Kommunikationsdaten am Entstehungsort, dem Aufnahmegerät beziehungsweise PC des Absenders, vor der Verschlüsselung beziehungsweise nach

der Entschlüsselung, am Ausgabegerät beziehungsweise PC des Empfängers, erzielen. Dies wäre nach hiesiger Auffassung eine Quellen-TKÜ.

- ***Besteht eine Möglichkeit darin, die Kommunikation noch vor ihrer Verschlüsselung zu erfassen? Wie kann dies technisch umgesetzt werden? Ist dazu die Installation einer Überwachungssoftware auf einem informationstechnischen System (welchem?) erforderlich?***

  Das gesprochene Wort muss an der Audioschnittstelle beziehungsweise die Kommunikationsdaten vor der Verarbeitung durch die Verschlüsselungssoftware abgegriffen und der überwachenden Behörde übertragen werden. Dazu ist die Installation einer speziellen Überwachungssoftware auf dem Zielrechner der zu überwachenden Zielperson *notwendig*

- ***Welche sonstige Planungen und Möglichkeiten gibt es, verschlüsselte Kommunikation überwachbar zu machen? Gibt es dazu strategische Konzepte der Bedarfsträger? Ggf. Was ist deren Inhalt?***

  Entsprechende Überlegungen sind derzeit Gegenstand von Konzeptionen der Bedarfsträger. Im übrigen wird auf die Ausführungen weiter unten verwiesen.

- ***Wie lässt sich der Unterschied zwischen Online-Durchsuchung und Online-Überwachung technisch definieren?***

  Siehe hierzu die Vorbemerkung und Ausführungen zu II, Punkt 1. Eine technische Definition der Unterscheidung bezogen auf den Einsatz der technischen Mittel ist nicht möglich. Das Unterscheidungskriterium liegt eher in der Zielrichtung der Maßnahme und dem Element der Dauer.

III. Technische Vorabklärung von Online-Durchsuchung und Online-Überwachung

Wie gestaltet sich die Planung für eine solche Maßnahme:

- ***Welche genauen Informationen werden benötigt, insbesondere hinsichtlich der Technik und der Software beim Zielsystem?***
  Für eine erfolgversprechende Maßnahme werden in der Regel folgende Informationen benötigt:
  - verwendetes Betriebssystem
  - Möglichkeiten zur Einbringung der RFS

  In Abhängigkeit der gewählten Methode, die Software auf das Zielsystem zu verbringen, können folgende weitere Informationen nötig sein:
  - genaue Betriebsystemversion
  - vorhandener Internetzugang
  - Browsertyp und Version
  - Angaben zu installierten Softwareprodukten und deren Versionen
  - Angaben zum Onlineverhalten des Benutzers

  Die Auswertung der Informationen kann ergeben, dass in diesem Fall eine Online-Durchsuchung mit den aktuell verfügbaren technischen Mitteln nicht realisierbar ist.

- ***Auf welche Weise lassen sich diese Informationen gewinnen? Gibt es insoweit Besonderheiten, die aus der Art des informationstechnischen Systems? Kann eine Telekommunikationsüberwachung insoweit hilfreich sein, bedarf es ggf. ergänzender Informationserhebung?***

  Die im vorgenannten Punkt aufgezählten Informationen zu den technischen Bedingungen lassen sich im Zuge einer Telekommunikationsüberwachung und sonstiger Gewinnung von technischen Daten ohne Kontaktaufnahme mit dem Zielsystem, etwa einem sogenannten Portscan, erheben. Weiterhin kommen her-

kömmliche Ermittlungsmaßnahmen in Betracht. Die zu treffenden Maßnahmen sind lageabhängig und lassen sich hier nicht abschließend aufzählen.

- ***Welche Möglichkeiten bestehen im Bereich des islamistisch motivierten Terrorismus, durch den Einsatz von V-Leuten oder verdeckten Ermittlern, relevante Informationen zu gewinnen? Gibt es insoweit Beispiele für den erfolgreichen Einsatz dieser Ermittlungsinstrumente?***

  Einsatz von Vertrauens-Personen (V-Personen)

  Die Maßnahme ist sowohl zu Zwecken der Strafverfolgung als auch im Bereich der Verhütung von schweren Straftaten in vergleichbarer Weise taktisch möglich. Da das Bundeskriminalamt bislang über eine entsprechende Befugnis im Bereich der Gefahrenabwehr nicht verfügt, soll nachfolgend auf die Strafverfolgungspraxis abgestellt werden:

  Es ist grundsätzlich möglich, eine V-Person im Rahmen eines Ermittlungsverfahrens auf der Grundlage einer Geheimhaltungszusage und Einsatzgenehmigung der Staatsanwaltschaft einzusetzen beziehungsweise zu beauftragen, solche Informationen zu Beschuldigten/Zielpersonen zu beschaffen, die für die technische Realisierung einer verdeckten Online-Durchsuchung/-Überwachung notwendig wären. Dabei kommt sowohl der Einsatz einer V-Person, die bereits Kontakte zu Beschuldigten/Zielpersonen unterhält, als auch der Einsatz einer V-Person in Betracht, die noch nicht über diesen Zugang verfügt und an die Beschuldigten/Zielpersonen "herangespielt" wird. Es ist im jeweiligen Einzelfall zu prüfen, inwieweit ein entsprechender VP-Einsatz realisierbar ist. Wenngleich hier bisher kein VP-Einsatz in diesem Phänomenbereich durchgeführt wurde, der auf die Gewinnung entsprechender technischer Informationen ausgerichtet war, erscheint dies in der Zukunft durchaus realisierbar.

  Einsatz verdeckter Ermittler (VE)

  Verdeckte Ermittler, in der Regel Polizeibeamte, an religiös/ethnisch abgeschottete Gruppierungen heranzuführen, kommt allenfalls im Rahmen langfristig geplanter und angelegter Maßnahmen in Betracht. Darüber hinaus stehen geeignete Personen nur in sehr beschränktem Umfang zur Verfügung.

- ***In welcher Abfolge gestalten sich die einzelnen Informationserhebungsschritte? Welche genauen Schritte müssen bei der Vorbereitung einer Online-Durchsuchung/-Überwachung erfolgen und welche Zeit nehmen diese in Anspruch? Es stellen sich insbesondere folgende Fragen:***

  - ***Welche polizeiliche Ermittlungsarbeit ist im Vorfeld nötig, welche Zeit nimmt diese in Anspruch?***

    Die Ermittlungsarbeiten sind sehr stark vom jeweiligen Fall abhängig und zeitlich nicht einschätzbar. Grundsätzlich wird die Ermittlungsarbeit im Vorfeld jedoch einen hohen zeitlichen Einsatz erfordern.

  - ***Was genau muss über den betroffenen Rechner ermittelt werden (z.B. welches Betriebssystem, welche Programme)? Wie kann dies ermittelt werden, wie aufwendig ist dies?***

    Siehe die Ausführungen zu III, Punkt 1.

  - ***Muss der Rechner während der gesamten Vorbereitungsphase "beobachtet" werden, um mögliche Änderungen festzustellen? Ist dies überhaupt leistbar?***

    Eine „Beobachtung“ des Zielrechners ist während der Vorbereitungsphase hilfreich. Die „Beobachtung“ ist leistbar, da sich einige Auswertevorgänge automatisieren lassen. Wenn alle notwendigen Informationen gesammelt sind, kann die RFS kurzfristig eingesetzt werden.

IV. Technische Vorbereitung von Online-Durchsuchung und Online-Überwachung

- ***Welche genauen technischen Möglichkeiten gibt es und welche davon sollen genutzt werden, um die Maßnahmen umzusetzen, differenziert nach***
  a) dem Aufbringen der Überwachungssoftware auf das informationstechnische System

  Es gibt eine Vielzahl von Einbringungsmöglichkeiten, die nunmehr auf Tauglichkeit für den jeweiligen Einsatz überprüft und eventuell angepasst werden müssen. Grundsätzlich ist dabei die unwissentliche Mitwirkung der Zielperson notwendig, um einen Entdeckung der Maßnahme zu verhindern. Eine generelle Aussage zur genauen Einbringungsmethode ist nicht möglich, da sie jeweils vom Einzelfall und vom Nutzungsverhalten der Zielperson sowie der vorliegenden technischen Bedingungen abhängig ist.

  b) der Ausleitung von Inhalten aus dem informationstechnischen System Bitte jeweils vollständige Auflistung.

  Die gewonnenen Ergebnisse werden so lange verschlüsselt auf dem informationstechnischen System zwischengelagert, bis eine Internetverbindung durch die Zielperson hergestellt wird. Bei aktiver Internetverbindung werden die verschlüsselten Daten auf einen von den Sicherheitsbehörden genutzten Server übertragen. Nach erfolgreicher Übertragung dieser zwischengelagerten Daten an den Server werden sie auf dem Zielrechner gelöscht. Die dann in die Sicherheitsbehörde übertragenen Daten werden entschlüsselt und für die Ermittler zur Auswertung entsprechend aufbereitet.

- ***Wie lange dauert die Entwicklung der Software? Ist die Dauer unterschiedlich, je nachdem, was die Software leisten soll (Durchsuchung oder Überwachung)?***

  Die Entwicklung einer einsetzbaren Version der RFS könnte bei Aufhebung des gegenwärtig verfügten Entwicklungsstopps unverzüglich abgeschlossen sein.

Nach der Fertigstellung muss eine solche Software laufend an neue Entwicklungen, etwa im Bereich Antiviren- und Firewallsoftware, angepasst werden. Eine Unterscheidung zwischen Durchsuchung und Überwachung ist dabei nicht erforderlich.

V. Technische Umsetzung von Online-Durchsuchung und Online-Überwachung

- ***Will das BKA wirklich nicht auf die laufende Kommunikation zugreifen? (Dies wurde in der BMI/BMJ-Arbeitsgruppe anders geschildert.)***

  Zur Abgrenzung von Quellen-TKÜ und Online-Durchsuchung siehe oben. Ein Zugriff auf Telekommunikation im Rahmen einer Online-Durchsuchung und Online-Überwachung ist nicht gewollt.

- ***Auf welchen Wegen will das BKA den Trojaner auf dem Zielrechner installieren? Ist auch geplant, Mails unter dem Namen einer anderen Behörde zu versenden, um Vertrauen in die Mail zu wecken (was aber generell das Vertrauen in Mails von staatlichen Stellen beeinflussen könnte)?***

  Das Versenden von E-Mails unter dem Namen einer anderen Behörde wäre mit großen Risiken verbunden und könnte nur in begründeten Ausnahmefällen in Absprache mit der betroffenen Behörde zum Einsatz kommen. Zu den Einbringungstechniken wird auf IV, Punkt 1, a) verwiesen.

- ***Wie gezielt kann eine Durchsicht oder Überwachung erfolgen?***

  Bei Durchführung eines Fernzugriffs auf ein informationstechnisches System muss die zu sichernde Datenmenge grundsätzlich anhand von vorher festgelegten klaren Suchkriterien eng begrenzt werden. Dies ist einerseits technisch bedingt, da die für eine Übertragung zur Verfügung stehende Zeit und Bandbreite des Teilnehmeranschlusses grundsätzlich als gering anzusehen ist. Andererseits besteht das taktische Erfordernis, das Zielsystem so wenig als möglich zu belasten, damit die aufgespielte Software und deren Aktivitäten nicht auffallen. Da-

mit ist bereits im Vorfeld einer jeden Maßnahme der Online-Durchsuchung garantiert, dass nur ein bestimmter, gezielt ausgewählter Ausschnitt der verfügbaren Daten sichergestellt wird und zur Auswertung gelangt. Eine solche gezielte Durchsicht oder Überwachung ist möglich.

- **Recherche anhand von Dateibezeichnungen?**
  - ***Erfassen auch der Inhalte von Dateien?***
  - ***Recherche mittels Suchbegriffen?***
  - ***Recherche auch bei gelöschten Texten?***
  - ***Überwachung auch von Befehlen/genutzten Funktionen?***
  - ***Recherche nach und Erhebung von Passwörtern, Signaturen und Signaturschlüsseln?***
  - ***Gleichzeitige (akustische und optische) Überwachung des Raums, in dem sich das Datenverarbeitungssystem befindet per Web-Cam?***
  - ***Bestehen Möglichkeiten zur Beschränkung der Überwachung, z. B. alle Aktionen abends zwischen 20.00h und 22.00h?***
  - ***Bestehen Möglichkeiten zur Beschränkung auf bestimmte Nutzer (z.B. beim Homenetwork oder beim Internetcafe)?***

Alle genannten Möglichkeiten wären technisch umsetzbar. Zu Punkt 7 (Webcam) wird auf die obigen Ausführungen zu II, Punkt 4 verwiesen.

VI. Zeitlicher und sonstiger Aufwand für Online-Maßnahmen

- ***Welcher Aufwand entsteht im Rahmen***
  - ***der technische Vorabklärung***
  - ***der technische Vorbereitung***
  - ***der technische Umsetzung***
  - ***der Auswertung***

  von je einer
  - ***Online-Durchsuchung***
  - ***Online-Überwachung***

  in

- ***zeitlicher Hinsicht (Angaben von Tagen/Wochen/Monaten/Jahren)***
- ***personeller Hinsicht (Angabe von Personentagen)***
- ***sachlicher Hinsicht (welche Technik ist nötig)***
- ***sonstiger Hinsicht***

Bitte jeweils auch mit Angaben zu den damit verbundenen finanziellen Kosten.

Bei den folgenden Aufzählungen können noch keine konkreten Angaben gemacht werden. Mangels praktischer Erfahrungswerte handelt es sich bei den Angaben lediglich um Schätzungen.

Die technischen Vorabklärungen (Auswertung der Internetaktivitäten durch TKÜ-Maßnahmen zur Erlangung von Erkenntnissen über das Zielsystem wie verwendetes Betriebssystemversion u.ä.) sind für Online-Durchsicht und Online-Überwachung gleich.

Der Zeitfaktor ist abhängig vom Onlineverhalten des Betroffenen und liegt zwischen einigen Stunden und erstreckt sich maximal über die Dauer der begleitenden Internetüberwachung. Der Personalfaktor ist ebenfalls abhängig vom Onlineverhalten, vom Umfang der technischen Vorabklärungen und vom Datenvolumen. Auch die erforderlichen Sachmittel sind abhängig vom Onlineverhalten. Bei großen Datenmengen werden unter Umständen mehrere Rechner zur Beschleunigung der Auswertung der Überwachungsprotokolle erforderlich sein, eventuell werden mehrere Speichermedien zur Speicherung der Übertragungsprotokolle benötigt. Diese technischen Vorbereitungen sind für Online-Durchsicht und Online-Überwachung gleich.

Zur Konfiguration und Bedienung (Schichtdienst möglich) werden zwei Personen benötigt. Für die Wahl der Einbringungsmethode können mehrere Personentage /-wochen notwendig werden. Je nach gewählter Einbringungsmethode werden Beschaffungen von Hard- und Software nötig

Die technische Umsetzung unterscheidet sich bei Online-Durchsicht und Online-Überwachung in der zeitlichen Komponente. Online-Durchsicht: Der Zeitbedarf ist

abhängig vom Zeitaufwand, der zum Erreichen des Durchsuchungszieles benötigt wird. Online-Überwachung: Der Zeitrahmen ergibt sich aus dem gesetzlich festgelegten Überwachungszeitraum. Als Personal werden mindestens zwei Personen aufzuwenden sein, die den Controller bedienen, dazu unter Umständen Ermittler und Dolmetscher. An Sachmitteln werden ein oder mehrere Server (Multiserver), ein Rechner auf dem der Controller läuft, und eine bestehende Internetverbindung des Controllerrechners zum Server einzusetzen sein.

Die Auswertung obliegt den jeweiligen Fachbereichen und ist stark abhängig vom Datenaufkommen.

Grundsätzlich ist zu sagen: der Aufwand verdeckter Maßnahmen ist generell vor Durchführung kaum abschätzbar.

- ***Kann eine Online-Maßnahme hiernach geeignet sein, eine - in zeitlicher Hinsicht - dringende Gefahr abzuwehren?***

  Eine Online-Durchsuchung ist geeignet in zeitlicher Hinsicht dringende Gefahren abzuwehren. Dabei sind folgende Fallkonstellationen zu unterscheiden:

  - die RFS ist bereits installiert und eine Gefahr wird erkannt
  - bei akut auftretender Gefahrenlage müssen die Umfeldabklärungen mit höherem Ressourceneinsatz ablaufen; reicht der zeitliche Vorlauf dennoch nicht aus, müssen konventionelle Maßnahmen die Gefahr beseitigen
  - bei einer Dauerlage (Dauergefahr) kann eine Online-Durchsuchung zur Verhinderung weiterer Gefahren beitragen oder die Gewinnung wichtiger Erkenntnisse ermöglichen

  Auch eine Wohnraumüberwachung ist zur Abwehr dringender Gefahren zulässig, hier können die vorzunehmenden Vorbereitungen für eine solche Maßnahmen indes grundsätzlich ebensoviel Zeit in Anspruch nehmen.

VII. Speziell zur Kryptographie

- ***Welche jeweils systemspezifischen Arten der Kryptierung gibt es?***

  „Systemspezifische Arten der Kryptierung“ gibt es allenfalls für dedizierte Kryptogeräte. Auf den Systemen „PC“ beziehungsweise „Internet-Server“ gibt es in der Regel mehrere Verschlüsselungsmöglichkeiten (deren Umfang individuell stark variiert). Zum Verständnis: nachrichtentechnisch gesehen wird der Transport von Information in verschiedenen Schichten („OSI-Referenzmodell“) durchgeführt, wobei die Daten einer höheren Schicht für eine darunter liegende Schicht keine inhaltliche Bedeutung haben. Auf vielen PCs gibt es Programme zur Verschlüsselung von Daten auf der Vermittlungsschicht (etwa IPSec, VoIP), auf der Transportschicht (SSL/TLS in Internet-Browsern) und auf der Anwendungsschicht („Ende-zu-Ende“-Verschlüsselung, etwa Datei- und E-Mail-Verschlüsselung). In fast allen dieser „Verschlüsselungen“ findet man eine Kombination der grundlegenden Arten der Verschlüsselung, d. h. man findet „symmetrische“ und „asymmetrische“ (= Public Key) Verfahren.

- ***Welche Entwicklungen sind absehbar?***

  Schon heute können verbreitete kommerziell oder im Internet erhältliche Algorithmen, wie sie insbesondere in Ende-zu-Ende Szenarien verwendet werden, bei sauberer Implementierung häufig nicht entziffert werden. Bereits heute schützen Programmierer passwortbasierter Verschlüsselungsprogramme ihre Implementierungen durch künstliche Arbeitslast gegen „Durchprobieren“.

- ***Wie kann man technisch Kryptierung umgehen/überwinden? Gibt es insoweit Alternativen zu Online-Maßnahmen? Wurden Alternativen in Betracht gezogen und geprüft?***

  Grundsätzlich bestehen folgende Umgehungs/-Überwindungsmöglichkeiten:

  i) „Abzweigen“ der Klar-Information vor bzw. nach Ver-/Entschlüsselung
  ii) Verwendung von absichtlich „geschwächten“ Verschlüsselungsprodukten

iii) treuhänderische Hinterlegung von kryptographischen Schlüsseln („key escrow“)
iv) Zugriff auf im System gespeicherte oder über Tastatur eingegebene Schlüssel durch Einsatz von „Sniffer“-Software

zu ii): der generelle Einbau von „staatlichen Hintertüren“ in Verschlüsselungsprodukte ist derzeit politisch nicht gewollt.
zu iii): die Vergangenheit („Kryptodebatte“ der neunziger Jahre) hat gezeigt, dass Maßnahmen zum Key-Escrow in Deutschland politisch nicht durchsetzbar sind. Angesichts der freien Erhältlichkeit sicherer Ende-zu-Ende-Verschlüsselungsprogramme im Internet dürften entsprechende nationale Regelungen auch wenig erfolgversprechend sein.
zu iv) Dies wäre ein Spezialfall einer Online-Maßnahme

- ***Ist bei einer Eingabe erkennbar, ob Daten kryptiert werden sollen, insbesondere auch dann, wenn keine systembedingte Kryptierung erfolgt?***

  Bei der Beantwortung wird davon ausgegangen, dass mit Eingabe die „Tastatureingabe“ auf dem PC bezeichnet wird. Tastatureingaben lassen in aller Regel nicht erkennen, ob Daten anschließend verschlüsselt werden sollen. Ausnahmen könnten etwa Kommandozeilenaufrufe von Verschlüsselungsprogrammen oder die Eingabe von „verdächtigen“ Dateinamen bilden, aber auch nur, wenn diese Daten auf einer Metaebene interpretiert werden können. Hierdurch wird deutlich, dass die Überwindung einer Kryptierung auf technischem Wege nahezu nicht möglich ist. Aus diesem Grund erscheint die Online-Durchsuchung die einzig geeignete Maßnahme, um Dateien im Klartext zu erlangen.

VIII. Technische Risiken der „Online-Durchsuchung“

- ***Was sind die mögliche Risiken unerwünschter Nebenwirkungen einer „Online-Durchsuchung“?***
  - ***für den Betroffen?***
  - ***für unbeteiligte Dritte?***

  Es soll bei der Online-Durchsuchung eine selbst entwickelte Software eingesetzt werden, die auch unter den Gesichtspunkten möglicher Risiken für Betroffene und unbeteiligte Dritte entsprechend hinreichend geprüft sein wird (u.a. aufgestellte Designkriterien, Vorgabe von Sicherheitsstandards durch das Bundesamt für Sicherheit in der Informationstechnik). Ausgeschlossen werden kann, dass Daten auf dem Zielsystem durch den Einsatz der RFS manipuliert werden, da der Einsatz umfangreich und nachvollziehbar dokumentiert wird. Eine später behauptete Manipulation des Zielsystems durch Dritte könnte mit hoher Wahrscheinlichkeit durch forensische Untersuchungen verifiziert/falsifiziert werden.

- ***Unterscheiden sich bei der Online-Durchsicht (oben I.) und der Online-Überwachung (oben II.) die Risiken unerwünschter Nebenwirkungen?***
  - ***für den Betroffen?***
  - ***für unbeteiligte Dritte?***

  Nein. Siehe auch Ausführungen unter VIII, Punkt 1.

- ***Besteht die Gefahr, dass Sensible Infrastrukturen durch eine staatliche Online-Maßnahme gefährdet werden (z. B. das Informationssystem eines Krankenhauses oder Wasserwerkes, weil die Zielpersonen der Maßnahmen „Teil“ dieses Informationssystems ist)?***

  Der Einsatz der RFS auf dem System einer Behörde/eines Unternehmens wird bereits aus taktischen Erwägungen und fehlender Notwendigkeit ausscheiden. Es ist darauf hinzuweisen, dass etwa in Fällen, in denen eine Zielperson den Rechner einer Behörde, einer Universität oder eines Unternehmens nutzt, aus takti-

schen Gründen keine Online-Durchsuchung veranlasst würde. Vielmehr würde eher die Einbindung der Behörde, der Universitätsverwaltung oder des Unternehmens mit Hilfe der dortigen Systemadministration erfolgen.

- ***Besteht die Gefahr, dass Dritte (z. B. Kriminelle) die staatliche Online-Maßnahme für ihre eigenen Zwecke missbrauchen? Falls ja, wie würde so ein Missbrauch technisch aussehen?***

  Im Rahmen der Designkriterien für die RFS ist unter anderem auch festgelegt, dass die Software keine eigenen Verbreitungsroutinen und auch einen wirksamen Schutz gegen Missbrauch beinhaltet (siehe oben zu den Sicherheitsstandards). Speziell wird sichergestellt, dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen Server als den vom Bundeskriminalamt verwendeten zurückzumelden, und dass die Software weder von außen erkannt noch angesprochen werden kann. Das Entdeckungsrisiko kann durch technische Maßnahmen reduziert werden. Eine anschließende Manipulation der RFS wäre im Vergleich zu anderen Möglichkeiten zudem extrem aufwendig. Niemand ist darauf angewiesen, eine RFS zu analysieren und für eigene Zwecke zu verändern, da entsprechende Produkte mit sehr großem Missbrauchspotenzial im Internet frei erhältlich sind.

IX. Internationale Erfahrungen

- ***Gibt es in anderen Ländern Erfahrungen mit der Online-Durchsuchung?***

  Das BKA hat innerhalb der EU eine Umfrage zur Online-Durchsuchung durchgeführt. Bislang liegt noch keine vollständige Rückmeldung vor, jedoch können folgende Aussagen getroffen werden:
  - Explizite Regelungen zur Online-Durchsuchung bestehen in den Ländern Rumänien, Zypern, Lettland und Spanien.
  - In der Schweiz hat der Bundesrat am 22. Juni 2007 den Entwurf für die Änderung des Bundesgesetzes über Maßnahmen zur Wahrung der inneren Sicherheit verabschiedet. Danach sollen Schweizer Sicherheitsbehörden künftig un-

ter anderem zur Terrorabwehr Abhörgeräte und Kameras in Privaträumen installieren sowie Post, Telefon, E-Mail und PCs präventiv überwachen beziehungsweise durchsuchen dürfen.

- Einige Staaten besitzen keine explizite Befugnisnorm, gleichwohl wäre eine Online-Durchsuchung rechtlich zulässig (etwa Slowenien) oder sind derzeit mit der Schaffung einer expliziten Befugnisnorm im Gesetzgebungsverfahren befasst (etwa Schweden).

In den USA setzte das FBI laut Presseberichten im Juni 2007 eine Software mit der Bezeichnung CIPAV ein, um einen Internetnutzer zu identifizieren, der mehrere Bombendrohungen an eine Schule im US-Bundesstaat Washington geschickt hatte. Die Berichte gehen nur begrenzt auf technische Details ein. Im Vergleich zur Online-Durchsuchung und verwandten Maßnahmen handelt es sich bei dem (öffentlich bekannten) Funktionsumfang und der Zielsetzung in diesem Fall eher um eine Art der Benutzer-/IP-Feststellung.

- ***Falls ja, von welchem technischen Voraussetzungen wird in diesen Ländern ausgegangen? Gibt es unterschiedliche technische Lösungen?***

Die technischen Lösungen der einzelnen Länder sind dem Bundeskriminalamt nicht bekannt. Das Bundeskriminalamt beabsichtigt aber zukünftig den Informationsaustausch hierüber zu intensivieren.