Bundesministerium des Innern Berlin, den 22. August 2007

Fragenkatalog der SPD-Bundestagsfraktion
AG Kultur und Medien
AG Neue Medien

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.

1. ***Bei der Wohnungsdurchsuchung muss ein Dritter Zeuge hinzugezogen werden, wenn der Inhaber nicht anwesend ist. Außerdem ist eine Wohnraumdurchsuchung zeitlich limitiert und physisch sichtbar. Die Online-Durchsuchung ist durch Dritte nicht zu kontrollieren und damit für den Betroffenen nicht nachvollziehbar. Welche rechtlichen Schlussfolgerungen ziehen Sie daraus?***

   Zunächst folgt aus dem verdeckten Charakter der Maßnahme und dem gegenüber einer Wohnungsdurchsuchung vollständig unterschiedlichen Charakter der Maßnahme, dass es sich bei einer Online-Durchsuchung wesensmäßig nicht um eine Wohnraumdurchsuchung im Sinne des Art. 13 GG handeln kann. Nicht zuletzt durch die Entscheidung des Bundesgerichtshofs vom 31. Januar 2007

wird festgestellt, dass eine Online-Durchsuchung im hier verstandenen Sinne somit nicht von den Vorschriften einer physischen Durchsuchung (im Fall der Strafverfolgung: §§ 102 ff. StPO) gedeckt ist, da den konventionellen Durchsuchungsregelungen ein offener Charakter der Maßnahme zugrunde liegt.

Art. 13 GG schützt nur gegen bestimmte Beeinträchtigungen der räumlichen Sphäre, in der sich das Privatleben entfaltet. Bei einer Datenerhebung, die ohne Eindringen in die Wohnung vorgenommen wird, ist daher fraglich, ob Art. 13 GG betroffen ist oder nicht von einem Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG auszugehen ist. Diese Frage ist in der Literatur umstritten.

Aufgrund der Eingriffsintensität und der Art der möglicherweise betroffenen Daten sind bei der Schaffung einer Rechtsgrundlage unabhängig von dem betroffenen Grundrecht besondere Verhältnismäßigkeits- und Verfahrensanforderungen zu beachten. Insofern bedarf es einer jeweils bereichsspezifischen und dem Bestimmtheitsgrundsatz entsprechenden Normierung für eine „verdeckte“ Online-Durchsuchung. Diese muss den Schutz des Kernbereichs privater Lebensgestaltung gewährleisten, einen Richtervorbehalt und Benachrichtigungspflichten für die Betroffenen vorsehen.

2. ***Die Online-Durchsuchung hat eine weitaus größere Eingriffstiefe als die Wohnungsdurchsuchung und umfasst - da es sich um einen Datenspeicher handelt - auch Informationen, die vom Tagebuch, über Briefe, E-Mails, Zeitunglesen, Onlinebanking, Webserven eine Vielzahl an sozialen Tätigkeiten eines Bürgers. Sie ist nicht punktuell wie die Wohnungsdurchsuchung, sondern sie wirkt über Zeitabschnitte und ist damit erheblich intensiver. Wie bewerten Sie die Eingriffstiefe der heimlichen Online-Durchsuchung gegenüber der offen durchzuführenden Wohungsdurchsuchung und welche rechtlichen Schlussfolgerungen ziehen Sie daraus?***

Auf die Antwort zu Frage 1 wird Bezug genommen. Die Maßnahme der Online-Durchsuchung ist im Gegensatz zur (konventionellen) Wohnungsdurchsuchung zwar nicht offen, sondern verdeckt.

Das Bundeskriminalamt hat beim (verdeckten) Zugriff auf das informationstechnische System kein Interesse an der Kenntnisnahme etwa von Krankheitsberichten, Tagebüchern oder Liebesbriefen. Von Interesse sind vielmehr allein ermittlungsrelevante Informationen zu Terroristen und Extremisten, die jedoch, wie das Bundesverfassungsgericht in seinem Urteil vom 3. März 2004 zum „Großen Lauschangriff“ hinsichtlich strafrechtlich relevanter Inhalte festgestellt hat (Abschn. 136 f. des Urteils), nach typisierender Wertung gerade nicht dem Kernbereich persönlicher Lebensgestaltung zuzuordnen sind. Das Bundeskriminalamt wird zudem durch technische Maßnahmen weitestgehend ausschließen, dass durch eine Online-Durchsuchung ein Eingriff in den durch Art. 1 GG geschützten Kernbereich der persönlichen Lebensgestaltung stattfindet. Bei einem Zugriff mittels einer RFS wird nicht die gesamte Festplatte der Zielperson kopiert, sondern es werden vielmehr zunächst in einem ersten Verfahrensschritt anhand von vorher festgelegten Suchkriterien die mutmaßlich relevanten Daten ermittelt. Erst danach werden diese selektiert und in einem weiteren Schritt gezielt angefordert. Sollten trotz dieses mehrstufigen Verfahrens ausnahmsweise und zufällig Daten auf dem Rechner einer Zielperson gesichert werden, die dem Kernbereich persönlicher Lebensgestaltung zuzuordnen sind, wären diese unverzüglich zu löschen.

Sofern in der Frage als Beispiel das Tagebuch angeführt wird, ist es für die Grundrechtsposition des Betroffenen im Übrigen irrelevant, ob das Tagebuch im Rahmen einer offenen Durchsuchung/Sicherstellung/Beschlagnahme, unter Umständen an einem verstecktem Ort, aufgefunden und gesichtet oder in elektronischer Form qua Online-Durchsuchung durch die Polizei festgestellt wird.

3. ***Frage zur Beweissicherheit: In der Computerforensik werden heute Festplatten nach der Beschlagnahme "eingefroren", damit sie nicht später verändert werden können (sonst wäre der Beweiswert gleich Null). Die Online-Durchsuchung lässt diese Möglichkeit nicht zu: Sie ist eine Online-Beobachtung des Clients. Die Erkenntnisse lassen sich nicht beweissicher speichern. Welchen Beweiswert soll eine solche Online-Durchsuchung haben und wie soll die Beweissicherheit hergestellt werden?***

Zur Durchführung einer herkömmlichen Datenträgeruntersuchung (DTU) wird eine physikalische Kopie der Daten angefertigt. Danach erfolgen die Verifizierung der physikalischen Kopie sowie das Erstellen einer Sicherheitskopie. Das gesamte Verfahren wird dokumentiert und ist damit nachvollziehbar. Die Untersuchung/Auswertung der beweisgesicherten Daten erfolgt an Hand der gefertigten physikalischen Kopie und kann jederzeit anhand der Dokumentation nachvollzogen werden.

Die Durchführung einer Online-Durchsuchung soll ebenfalls lückenlos dokumentiert werdem. So werden die Einbringung der RFS auf den Zielrechner, jeder Remote-Zugriff auf den Zielrechner, alle Befehle für den Zielrechner und die Übertragung der Daten vom Zielrechner protokolliert. Damit ist die gesamte Maßnahme einer späteren gerichtlichen Überprüfung zugänglich. Das Problem der Nachvollziehbarkeit und „Wiederholbarkeit“ bei der Online-Durchsuchung ist durch die Tatsache gegeben, dass eine erneute Untersuchung wegen des dynamischen Charakters nicht unter den gleichen Bedingungen wiederholt werden kann. Insofern ist eine äußerst exakte und detaillierte Dokumentation während der Durchführung der Maßnahme notwendig. Technisch kann durch verschiedene Funktionalitäten, wie etwa dem Einsatz von Hash- und/oder Verschlüsse-

lungsverfahren oder digitaler Signatur die Integrität der übertragenen Daten überprüfbar gemacht werden.

4. ***Wenn die Beweissicherheit nicht als notwendig angesehen wird, dann ist die Online-Durchsuchung ein weiterer Schritt zur „Vernachrichtendienstlichung" der Polizei. Wie bewerten Sie die immer schwierigere Abgrenzung zwischen Nachrichtendienst und Polizei?***

Entscheidend ist nicht die Heimlichkeit einer einzelnen Befugnis, die der Polizei verliehen wird, sondern vielmehr der konkrete gesetzliche Zweck, zu dem diese genutzt werden. Dieser ist aufgrund der gesetzlichen Aufgabenzuweisungen eindeutig zwischen den Polizeien als Strafverfolgungsbehörden, den Polizeien als Gefahrabwehrbehörden und den Verfassungsschutzbehörden als nachrichtendienstliches Frühwarnsystem und Gefahrabwehrbehörde im Vorfeld festgelegt. Bei einer Nutzung der Online-Durchsuchung als Maßnahme im Bereich der Strafverfolgung ist die (forensische) Beweiserhebung einziger Zweck, bei einer Nutzung als Maßnahme zur Abwehr einer konkreten Gefahr ist die Erkenntnisgewinnung und Abwehr der Gefahr einziger Zweck.

Die Abgrenzung zwischen Polizei und Nachrichtendienst ergibt sich abschließend aus der jeweiligen gesetzlichen Aufgabenstellung. Die Online-Durchsuchung ist nicht geeignet, diese Systematik zu durchbrechen, auch wenn sie perspektivisch sowohl durch die Polizei als auch die Nachrichtendienste genutzt werden könnte. Verdeckte Maßnahmen, wie etwa eine Observation, werden bereits nach geltender Rechtslage im Aufgabenbereich der Nachrichtendienste wie auch innerhalb der Polizeien sowohl zur Gefahrenabwehr und als auch zur Strafverfolgung vorgenommen. Von einer „Vernachrichtendienstlichung" oder „Verpolizeilichung" kann nicht die Rede sein, da eine solche Maßnahme jeweils im zuständigen Aufgabenbereich je nach Einzelfall auf ihre Geeignetheit und Zulässigkeit anhand gesetzlicher Vorgaben geprüft wird.

5. ***Wie kann der Kernbereich der privaten Lebensgestaltung der Beschuldigten bzw. anderer betroffener Benutzer des gleichen Systems (bei Multi-User-Systemen) sichergestellt werden***?

Aufgrund der vor der eigentlichen Online-Durchsuchung erforderlichen Aufklärung (Lebensgewohnheiten, Internetverhalten, Kontaktpersonen u.ä.) wird in der Regel eine nähere Auffindevermutung bestehen, so dass sich das Tool auf bestimmte Dateinamen oder Dateiformate, sogenannte Suchkriterien, beschränken kann. Kernbereichsrelevante Erkenntnisse sind für die sicherheitsbehördlichen Belange stets irrelevant.

Der Schutz des Kernbereichs anderer Benutzer wie auch des Beschuldigten kann allein mit technischen Mitteln nicht abschließend garantiert werden. Ebenso wie bei der Datenträgeruntersuchung, etwa die Beschlagnahme einer Festplatte eines sog. Multi-User-Systems, oder anderen klassischen Ermittlungsmaßnahmen, etwa einer Wohnungsdurchsuchung, muss der Schutz des Kernbereichs letztlich auch im Rahmen der Auswertung im Anschluss an die Erhebung der Daten gewährleistet werden. Hierzu sind geeignete Regelungen über eine gerichtliche Kontrolle und Löschungspflichten zu treffen.

6. ***Welche Gefahren für den Kernbereich der privaten Lebensgestaltung eröffnen sich und wie kann ein Missbrauch der Spionagesoftware technisch unterbunden werden? In welcher Weise ist der vom Bundesverfassungsgericht geforderte Schutz des Kernbereichs privater Lebensgestaltung beim Einsatz von Spionagesoftware technisch machbar?***

Bei der hier in Rede stehenden RFS handelt es sich nicht um eine „Spionagesoftware“, sondern um ein technisches Mittel zur Datenerhebung.

Im Rahmen der Designkriterien für die RFS ist unter anderem festgelegt, dass die Software keine eigenen Verbreitungsroutinen und auch einen wirksamen Schutz gegen Missbrauch durch Dritte beinhaltet. Speziell wird sichergestellt, dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen Server als den von den Sicherheitsbehörden benutzten

Server zurückzumelden, und dass die Software weder von außen erkannt noch angesprochen werden kann.

Das Risiko einer Entdeckung kann durch technische Maßnahmen reduziert werden. Abgesehen davon, dass das Entdeckungsrisiko als solches als gering einzustufen ist, wäre eine anschließende Manipulation im Vergleich zu anderen Möglichkeiten der Nutzung von frei verfügbarer Schadsoftware extrem aufwendig. Niemand ist ernsthaft darauf angewiesen, eine RFS zu analysieren und für eigene Zwecke zu verändern, da entsprechende Produkte mit sehr großem Missbrauchspotenzial im Internet frei erhältlich sind (z.B. Optix Pro oder Back Orifice). Im übrigen siehe Antwort zu Frage 31.

Sollten ungewollt Daten aus dem Kernbereich erhoben worden sein, sind diese unverzüglich zu löschen.

7. ***Was genau ist mit den "Suchbegriffen" (BKA-Gesetz Art. 20k) gemeint? Woher weiß ein Ermittler, unter welchen Begriffen Terroristen ihre Pläne auf ihrer Festplatte speichern?***

Zur Auswahl relevanter Daten sind anhand der bestehenden Erkenntnislage Suchkriterien festzulegen. Dadurch wird eine zielgerichtete und von vorneherein begrenzte Suche sichergestellt. Diese Suchkriterien können u. a. sein:
- Dateinamen
- bestimmte Dateiendungen
- Eigenschaften/Attribute (Zugriffdaten etc.)
- Schlüsselwörter
- bestimmte Verzeichnisse
- Dateien eines bestimmten Dateityps

Durch entsprechende Vorfeldermittlungen sind oftmals (Such-)Begriffe bekannt, anhand derer auf dem Zielsystem gesucht werden kann, um die zu sichernden Daten zu bestimmen.

Das Verbot der Verwendung bestimmter Suchkriterien dient der Gewährleistung des grundrechtlich gebotenen Kernbereichsschutzes, indem nach derartigen Inhalten nicht gezielt gesucht werden darf. Oftmals sind aufgrund anderer im Vorfeld gewonnener Erkenntnisse bereits Suchkriterien bekannt, mit Hilfe derer auf dem Zielsystem selektiert werden kann, um die zu sichernden Daten zu bestimmen. Jedoch sollte die Datenerhebung nicht ausschließlich mittels vorher festgelegter Suchkriterien erfolgen, sondern sich flexibel der aktuellen Erkenntnislage anpassen können.

8. ***Sollen Teile der entwickelten Spionagesoftware später wiederbenutzt werden? Wie soll in diesem Fall sichergestellt werden, dass dies nicht zum Aufspüren der Software durch Anti-Viren-Hersteller oder Wirtschaftsspionierende führen wird?***

Die entwickelte Software soll grundsätzlich nur einmal zum Einsatz kommen. Dadurch ist das Entdeckungsrisiko aufgrund der insgesamt geringen Einsatzhäufigkeit sehr gering. Die RFS wird darüber hinaus vor dem Einsatz mit aktueller Anti-Viren-Software geprüft. Wird die RFS durch die Anti-Viren-Software erkannt, kommt sie nicht zum Einsatz und wird überarbeitet. Im Weiteren siehe Frage 6.

9. ***Die Online-Durchsuchung setzt ein mehr oder minder „unsicheres“ Netz voraus. Damit einher geht eine Umwertung der bisherigen Sicherheitspolitik. Die Sicherheitsbehörden und das BSI machen das Netz nicht sicherer, sondern im Gegenteil: Es gibt ein staatliches Interesse, „Hintertüren“ in Betriebs- und Anwendungssysteme zu nutzen oder sogar „einzubauen“. Hinzu kommt, dass wenn die deutschen Sicherheitsbehörden heimlich auf Rechner zugreifen können, dass dies dann auch Dienste anderer Staaten können. Wie bewerten Sie diese Tatsache vor dem Hintergrund der weltweiten Wirtschaftsspionage und welche Folgen könnte dies für den Wirtschafts- und Forschungsstandort Deutschland haben? Wer schützt die Zugänge (Ports), die für die Online-Durchsuchung genutzt werden sollen, gegen den Zugriff beispielsweise zu Zwecken der Wirtschaftsspionage oder durch Sicherheitsbehörden und Dienste anderer Staaten?***

Es besteht Einigkeit darüber, dass kein Interesse daran besteht, „Hintertüren“ in Betriebs- und Anwendungssysteme einzubauen. Solche „Hintertüren“ beziehungsweise absichtlich eingebaute Schwachstellen in Soft- und Hardware hätten nicht nur für die IT-Sicherheit, sondern auch für die deutsche IT-Wirtschaft fatale Konsequenzen. Die obige Annahme, es bestehe ein Interesse an einem „unsicheren“ Netz ist daher unzutreffend. Hinzu kommt: Der Einbau von „Hintertüren“ in deutsche Produkte wäre schon allein aufgrund der einfachen Ausweichmöglichkeit auf ausländische Produkte, die nicht dem Einflussbereich der deutschen Gesetzgebung unterliegen, unsinnig. Das Nutzen nur einer Sicherheitslücke für alle Maßnahmen wäre zudem ein stark risikobehaftetes Vorgehen, da alle Maßnahmen entdeckt würden, wenn diese Sicherheitslücke identifiziert würde.

10. ***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 Vertrauenskrise der e-Society sein: Bürgerinnen und Bürger und möglicherweise auch Unternehmen werden beispielsweise auf Updates verzichten, weil sie ihren Systemen nicht mehr vertrauen. Sie werden möglicherweise auch auf Anwendungen wie Online-Banking***

verzichten. Welche Konsequenzen erwarten Sie aus der heimlichen Online-Durchsuchung für die Akzeptanz der Nutzerinnen und Nutzer und das Vertrauen in die IT-Sicherheitsinfrastruktur?

Eine „Vertrauenskrise der e-Society“ wird nicht gesehen. Bereits heute existieren erhebliche Schwachstellen, die durch Kriminelle genutzt werden, ohne dass dies zu einer Vertrauenskrise geführt hätte. Die Online-Durchsuchungen sollen an hohe Voraussetzungen geknüpft werden und, nicht zuletzt aufgrund dieser Voraussetzungen, aber auch aufgrund des Aufwandes, nur in geringer Anzahl zur Anwendung kommen. Zu einer maßgeblichen Änderung der Situation der IT-Sicherheit wird dies nicht führen.

11. ***Wie möchte das BSI der abzusehenden Vertrauenskrise, der sich auch eine erneute BSI-Debatte anschließen wird, begegnen?***

Bundesinnenminister Dr. Schäuble hat in seiner Rede beim BSI-Kongress am 22. Mai 2007 den Charakter des Bundesamtes für Sicherheit in der Informationstechnik als präventive Behörde hervorgehoben. Das Bundesamt für Sicherheit in der Informationstechnik hat die ausdrückliche Weisung, sich nicht aktiv an der Entwicklung der für die Online-Durchsuchung einzusetzenden Software zu beteiligen.

12. ***Wer berät sachverständig die Sicherheitsbehörden und das BMI bei der Konfiguration von Online-Durchsuchungen?***

Die Sicherheitsbehörden und das Bundesministerium des Innern verfügen grundsätzlich über genügenden Sachverstand.

13. ***Welche staatlichen Stellen beraten Bürgerinnen und Bürger, Forschungseinrichtungen und Unternehmen oder Verwaltung, um Schutzlücken ihrer technischen Systeme aufzudecken und sich vor unberechtigten Zugriff zu schützen?***

Nach dem BSI-Gesetz hat das Bundesamt für Sicherheit in der Informationstechnik die Aufgabe, Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen zu beraten, § 3 Abs. 7 BSI-Errichtungsgesetz. Das Bundesamt für Sicherheit in der Informationstechnik stellt dazu ein umfassendes Spektrum an Sicherheitsempfehlungen und Produkten bereit. Für Bürger gibt es die Internet-Angebote www.bsi-fuer-buerger.de und das Bürger-CERT unter www.buerger-cert.de. An Behörden und Unternehmen richten sich zahlreiche Studien sowie IT-Grundschutz und verschiedene Sicherheitszertifizierungen.

14. ***Wenn keine Softwareteile wiederbenutzt werden, wie hoch schätzen Sie den Mehraufwand für die jeweilige komplette Neuentwicklung?***

Die Kosten sind von der jeweiligen Fallkonstellation abhängig und können daher nicht näher beziffert werden.

15. ***Mit welchen Kosten rechnet das BMI / das BKA pro ausgespähter Person, bei Wiederverwendung von Teilen der Software für die Durchführung von Online-Durchsuchungen bzw. bei kompletter Neuentwicklung?***

Mit der Online-Durchsuchung werden keine Personen ausgespäht, sondern relevante Erkenntnisse auf informationstechnischen Systemen erhoben. Im übrigen wird auf die Antwort zu Frage 14 verwiesen.

16. ***Wie hoch ist nach Einschätzung des BMI / BKA die Entdeckungsgefahr beim Einsatz des bzw. der Tools der Online-Durchsuchung? Wie soll sichergestellt werden, dass Kriminelle oder Wirtschaftsspionierende keinen Zugriff auf den mit der Spionagesoftware infizierten Rechner bekommen und darüber in andere mit dem Rechner verbundene Netzwerke (VPN-Netzwerke etwa in Firmen und Behörden o. ä.) gelangen?***

Siehe Antwort zu Frage 6.

17. ***Eine Schwachstelle in einem Computersystem, die ausgenutzt wird, lässt ein Tor offen für andere Spionageprogramme - sehen Sie eine Gefahr möglicher Schadensersatzforderungen betroffener Unternehmen?***

    Mit der RFS werden keine zusätzlichen „Tore“ geöffnet. Die RFS wird so entwickelt, dass von ihr nach dem aktuellen Stand der Technik keine Schadfunktionen ausgehen. Insofern sind diesbezügliche Schadensersatzforderungen nicht zu erwarten.

18. ***Was ist vorgesehen, um die Software zu steuern oder abzuschalten, wenn der Port für die Kommunikation beispielsweise mittels einer Firewall gesperrt ist?***

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

19. ***Wie soll sichergestellt werden, dass die Online-Durchsuchungssoftware unbemerkt bleibt, vor allem beim Einsatz von Firewalls und Systemüberwachungssoftware? Sollen diese evtl. durch die Online- Durchsuchungssoftware ausgeschaltet werden? Wenn ja, wie sehen Sie die dann erhöhte Anfälligkeit des Systems gegenüber anderen Angreifern?***

    Vor einem Einsatz wird die Systemumgebung des Zielsystems erkundet, insbesondere die darauf installierten Sicherheitsvorkehrungen. Die RFS wird hinsichtlich ihrer Tauglichkeit zu deren Überwindung getestet und gegebenenfalls modifiziert. Es ist nicht vorgesehen, die auf dem System befindlichen Sicherheitssysteme auszuschalten.

20. ***Wie soll verfahren werden, wenn gängige Anti-Viren-Programme oder Firewalls die Tools bzw. die Online-Durchsuchungssoftware entdeckt haben?***

Es ist nicht zu erwarten, dass die RFS entdeckt wird. Sollte dies dennoch der Fall sein, wird das verwendete Tool vom Zielsystem entfernt. In dem Fall, dass die RFS durch eine Firewall oder eine Anti-Virus-Software erkannt wird, ist der Rückschluss auf die Sicherheitsbehörden nicht gegeben.

21. ***Wie sollen Instabilitäten bei sich oft ändernden Bedingungen auf dem Zielrechner (Neuinstallation oder Updates von Software oder Betriebssystem) verhindert werden?***

Durch den Nutzer selbst vorgenommene Änderungen an der Systemkonfiguration, die zu Systeminstabilitäten führen, können nicht verhindert werden. Durch die RFS selbst werden keine Instabilitäten auf dem Zielsystem verursacht.

22. ***Wie soll die automatische Löschung der Software nach dem vorgeschriebenen Zeitrahmen realisiert werden? Auf welchen Zeitgeber stützt sich die Löschung und was geschieht, wenn dieser nicht verfügbar ist bzw. verändert wird?***

Die Löschung kann sowohl manuell als auch automatisch erfolgen. Als Zeitgeber werden außer der Systemzeit weitere Zeitberechungsmodule parallel eingesetzt.

23. ***Sollen die technischen Möglichkeiten der Onlinedurchsuchung auch zu einer dauerhaften akustischen und visuellen Raumüberwachung verwendet werden?***

Eine akustische wie auch visuelle Wohnraumüberwachung ist nicht das Ziel der Online-Durchsuchung. 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.

24. ***Trojaner können Daten eines ausspionierten Rechners manipulieren sowie Daten platzieren. Können die mittels Online-Durchsuchung gewonnenen Informationen vor Gericht zweifelsfrei als echt angesehen werden? Welchen Beweiswert und Aussagegehalt haben die mit der Online-Durchsuchung erlangten Daten und Informationen?***

Siehe Antworten zu Frage 3 und 25. Die Beurteilung des Aussagehaltes (der Beweiswert spielt im Rahmen der Gefahrenabwehr zunächst keine Rolle) dürfte sich generell an anderen Maßnahmen der IuK-Forensik orientieren. Es ist nicht erkennbar, dass die Maßnahme aufgrund ihres Charakters in Frage gestellt werden wird.

25. ***Informatiker und IT-Sicherheitsfachleute sind übereinstimmend der Meinung, dass es technisch nicht möglich ist, während der Durchführung der Online-Durchsuchung zu verhindern a) privateste Daten des durchsuchten PCs einzusehen und b) Daten auf dem PC zu manipulieren oder hochzuladen, bspw. um Beweise für eine Straftat zu fälschen. Ein "digitales Richterband" in Form eines Logs lässt sich so manipulieren, dass dieser Missbrauch für einen überprüfenden Richter nicht nachweisbar ist. Wie wollen Sie einen solchen Missbrauch verhindern?***

Siehe Antworten zu Frage 3 und 6.Im Gegensatz zur in dieser Praxis anerkannten „herkömmlichen“ Datenträgeruntersuchung werden allerdings bei der Online-Durchsuchung nicht alle auf dem System befindlichen Daten, die dem Schutzbereich unterliegen, sichergestellt und ausgewertet, sondern allenfalls ein kleiner Teil. Durch die Hinterlegung des Quellcodes der RFS bei Gericht könnte zudem etwa belegt werden, dass die Software keine Daten frei im Zielsystem platzieren kann. Damit lässt sich der Vorwurf der Manipulation von Daten auf dem Zielsystem widerlegen.

26. ***Das BKA argumentiert, dass man den Quellcode der Durchsuchungs-Software bei Gericht vorlegen werde, wenn die Maßnahme beantragt wird. Sind sie der Meinung, dass Gerichte in Deutschland tatsächlich in der La-***

ge sind, anhand des Quellcodes einer Software deren korrekte Funktion zu beurteilen?

Die Justiz könnte sich gegebenenfalls unabhängigen Sachverstandes bedienen.

27. ***Was ist unter einem informationstechnischem System in abschließender Definition zu verstehen? Sind unter "informationstechnischen Systemen" auch Mobilgeräte wie Handys, Smartphones, Blackberries etc. zu verstehen? Sind unter "informationstechnischen Systemen" auch Infrastrukturkomponenten untergeordneter Netzebenen zu verstehen (Router, Switches, aber auch DE-CIX-Einrichtungen ...)?***

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

Es wird jedoch darauf hingewiesen, dass die bisher in der Diskussion genutzte Definition der Online-Durchsuchung gerade die Aufzeichnung von Telekommunikationsinhalten nicht mit umfasst.

28. ***Wie wird die Zugriffsmöglichkeit für Ermittler technisch installiert und realisiert? Wie wird die Datenübertragung realisiert? Wie wird die Revisionsfähigkeit der Online-Durchsicht technisch sichergestellt, so dass die Methode und die Authentizität der gewonnenen Informationen der Prüfung durch einen unabhängigen Gutachter standhält?***

Die Zugriffsmöglichkeit auf das Zielsystem wird durch das Aufspielen der RFS eröffnet. Die Datenübertragung erfolgt auf verschlüsseltem Wege. Zur Revisionsfähigkeit siehe Antworten zu Frage 3, 25 und 26.

29. ***Wie wird technisch sicher ausgeschlossen, dass der für eine Online-Durchsicht verwendete Zugang nicht von Dritten missbraucht wird?***

Siehe Antwort zu Frage 17.

30. ***Wie wird bei Beendigung der Maßnahme technisch sichergestellt, dass das untersuchte informationstechnische System wieder in den ursprünglichen Zustand versetzt wird? Wie wird technisch sichergestellt, dass nicht z.B. durch ein während der Maßnahme erzeugtes Backup der kompromittierte Zustand wieder hergestellt wird***?

Ein in Betrieb befindliches Computersystem verändert sich dynamisch, sodass ein „statischer" Ursprungszustand technisch nicht mehr wiederherstellbar ist. Bei Beendigung der Maßnahme werden alle Bestandteile der RFS restlos von dem System entfernt. Durch die RFS selbst werden keine weitergehenden Systembeeinträchtigungen vorgenommen. Durch Einprogrammieren eines Verfalldatums und eines Zeitzählmechanismus kann die Selbstdeinstallation der RFS auch nach einem evt. Wiederaufsetzen des Systems mittels Back-Up initiiert werden. Diese Selbstzerstörungsmechanismen dienen auch der Unterbindung der Weiterverbreitung.

31. ***Wie wird während der einzelnen Phasen von Infiltration, Überwachung/Kommunikation und Beendigung der Maßnahme technisch sichergestellt, dass die Maßnahme nicht aufgedeckt und mit Gegenmaßnahmen beantwortet wird?***

Durch verschiedene Maßnahmen wird sichergestellt, dass eine Rückverfolgbarkeit nahezu unmöglich ist. Die Zielperson könnte nur feststellen, dass sich auf dem System eine für ihn unerwünschte Software installiert hat. Bevor Gegenmaßnahmen durch den Betroffenen getätigt werden könnten, müsste dieser zunächst das entdeckte Programm analysieren. Diese Analyse der RFS (Disassembling) wird jedoch durch die Verwendung kryptographischer Methoden nahezu unmöglich gemacht.

32. ***Mit welchen Gegenmaßnahmen gegen Online-Durchsicht und -Überwachung wird gerechnet und wie soll diesen technisch wie organisatorisch begegnet werden?***

Im Rahmen der vorbereitenden Maßnahmen werden Erkenntnisse über das Nutzer- bzw. Schutzverhalten der Zielperson erhoben und daraus die Vorgehensmethodik entwickelt. Bei laufenden Maßnahmen wird das Nutzerverhalten weiterhin beobachtet. Wenn sich bei dieser Beobachtung Hinweise ergeben, die eine Modifizierung der Vorgehensweise oder des eingesetzten Programms notwendig machen oder sogar die Beendigung der Maßnahme wegen eines zu hohen Entdeckungsrisikos angezeigt erscheinen lassen, erfolgt die Anweisung an das Programm sich selbst zu deinstallieren.

33. ***Wie soll verschlüsselte Internettelefonie überwacht werden, wenn die Nutzer die Verschlüsselung nicht durch einen PC durchführen lassen, sondern durch ein Hardware-VoIP-Telefon, das sichere Verschlüsselung unterstützt?***

Eine Online-Durchsuchung im Sinne der hier gebrauchten Definition dient nicht der Überwachung von Telekommunikation.

34. ***Warum ist diese Methode nicht auch für das Abfangen PC-verschlüsselter VoIP-Kommunikation geeignet?***

Ob und in welcher Weise die bei der Online-Durchsuchung eingesetzte Technik auch für die Überwachung verschlüsselter VoIP-Kommunikation verwendet werden könnte, bedarf noch weiterer Klärung. Insofern sind hierzu keine abschließenden Aussagen möglich.

35. ***Welche Stellen sind aus Gründen der Einleitung der Maßnahme ggf. zu kontaktieren (z.B. Provider)?***

Grundsätzlich ist es nicht notwendig, weitere Stellen bei der Einleitung zu kontaktieren.

36. ***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 auf Tauglichkeit für den jeweiligen Einsatz überprüft, ausgewählt und eventuell angepasst werden müssen. 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 Identifizierung (Dateien) und Erfassung (Tastatureingaben etc.) von Inhalten unter Sicherstellung des Schutzes des Kernbereichs privater Lebensgestaltung*,**

Zur Selektion der relevanten Daten werden die bereits beschriebenen Suchkriterien verwendet. Tastatureingaben können durch Key-Logger erfasst werden. Zur Frage des Kernbereichschutzes siehe Antwort zu Frage 6.

c) der Ausleitung von Inhalten aus dem informationstechnischen System,
Die gewonnenen Ergebnisse werden so lange verschlüsselt auf dem Zielrechner zwischengelagert, bis eine Internetverbindung durch den Betroffenen hergestellt wird. Bei aktiver Internetverbindung werden die verschlüsselten Daten über das Netzwerk auf einen von den Sicherheitsbehörden genutzten Server übertragen. Nach erfolgreicher Übertragung dieser zwischengelagerten Daten an den Server, werden diese verschlüsselten Daten auf dem Zielrechner gelöscht. Die dann in die Sicherheitsbehörde übertragenen Daten werden entschlüsselt und für die Auswertung entsprechend aufbereitet.

d) der jederzeitigen Beendigung der Maßnahme unter Sicherstellung, dass keine Beeinträchtigung der Systemsicherheit resultiert.

Die Deinstallationsroutine wirkt sich nur auf die RFS selbst aus, so dass keine Beeinträchtigungen zu erwarten sind.

37. ***Wie wird technisch sicher ausgeschlossen, dass vom Aufbringen der Überwachungssoftware versehentlich Unbeteiligte betroffen werden?***

Durch die Rückmeldung einer eindeutigen Identifikation des Zielsystems und den in der Regel erfolgenden Abgleich der Aktivitäten des Zielsystems durch eine flankierende Telekommunikationsüberwachung wird der Einsatz auf dem „richtigen“ Zielsystem gewährleistet.

38. ***Ist auch geplant, zur Installation eines Trojanischen Pferdes E-Mail-Kommunikation zwischen Verdächtigen zu manipulieren (z.B. durch Infizierung eines erwarteten Dateianhangs) oder vorzutäuschen? Falls ja: Wie soll dies technisch realisiert werden? Wie wird technisch sicher ausgeschlossen, dass sich Dritte dieser Möglichkeit bemächtigen?***

Die Einbringung der RFS im Wege der E-Mail-Kommunikation kann je nach Einzelfall ein geeignetes Mittel darstellen. Dazu wird ein Bestandteil der RFS einer weiteren Datei beigefügt. Bei Öffnen dieser Datei wird die RFS auf dem Zielsystem installiert.

39. ***Ist geplant, dass eine Softwarekomponente auf dem Zielsystem auch bei Nichtbestehen einer Online-Verbindung Informationen sammelt (Tastatureingaben, etc.), diese auf dem Rechner zwischenspeichert und dann zeitversetzt übermittelt?***

Die Möglichkeit der verschlüsselten Zwischenspeicherung und des zeitversetzten Übermittelns von gesammelten Daten ist geplant. Dadurch können Auffälligkeiten im Systemverhalten vermieden und das Entdeckungsrisiko minimiert werden. Siehe auch Antwort zu Frage 36 Buchstabe c).

40. ***Soll eine Installation eines Trojanischen Pferdes Änderungen an der Systemkonfiguration vornehmen? Falls ja: Zu welchem Zweck? Wie wird sichergestellt, dass nach Beendigung der Maßnahme die Systemkonfiguration bereinigt wird?***

Jedes Programm, das in eine Systemumgebung eingebracht wird, nimmt Änderungen an der Systemkonfiguration vor. Diese Änderungen werden durch die Deinstallationsroutinen beim Löschvorgang rückgängig gemacht.

41. ***Soll eine Identifizierung relevanter Inhalte vor der Übertragung auf dem Zielsystem oder erst nach einer Übertragung auf einem Ermittlersystem erfolgen?***

Wenn mit dem Begriff „Identifizierung relevanter Inhalte“ die Auswertung eines Dateiinhalts auf Relevanz gemeint ist, dann erfolgt diese Auswertung in der Regel nicht auf dem Zielsystem selbst, sondern erst nach Übertragung auf ein Ermittlungssystem der Behörde.

42. ***Wie wird im Falle fremdsprachlicher Datenbestände die Analyse von Daten realisiert?***

Wie bei anderen polizeilichen/nachrichtendienstlichen Maßnahmen mit der gleichen Problematik werden fremdsprachliche Datenbestände unter Beteiligung von sicherheitsüberprüften Übersetzern analysiert.

43. ***Ist geplant, für die Infiltration von Zielsystem Informationen über Sicherheitslücken in Software, die den jeweiligen Herstellern noch nicht bekannt sind (sog. Zero-Day-Exploits) auf entsprechend von Kriminellen angebotenen Märkten zu erwerben? Falls nein: Wie sollen diese Informationen dann beschafft werden?***

Ein derartiger Erwerb ist nicht geplant. Diese sogenannten Zero-Day-Exploits haben in der Regel nur eine gewisse Zeitspanne, in denen sie eingesetzt wer-

den könnten. Informationen, die die Sicherheit von Betriebssystemen und Programmen betreffen, sind im Internet in der Regel offen zugänglich.

44. ***Wie wird bei einem Zielsystem, dass keine Internet-Verbindung mit dem Ermittlungssystem mehr aufbauen kann, sichergestellt, dass das Trojanische Pferd nach Ablauf einer befristeten Anordnung deaktiviert und vom System ohne Zurücklassen von Sicherheitslücken deaktiviert wird?***

Durch eine für den Fall der erfolglosen Kontaktaufnahme mit dem Steuerungssystem eingebaute Selbstdeinstallationsroutine entfernt sich die RFS rückstandsfrei vom System.

45. ***Welche Software wurde bei den bereits ohne Rechtsgrundlage durchgeführten Online-Durchsuchungen verwendet, wer hat sie hergestellt, wer unabhängig die Funktionsweise geprüft?***

Beim Bundeskriminalamt wurden bislang keine Online-Durchsuchungen durchgeführt.