DuD
Datenschutz und Datensicherheit

Realisierung, Grenzen und Risiken der „Online-Durchsuchung“

Dirk Fox

Als ein Mittel zur Erweiterung der Möglichkeiten von Nachrichtendienten und Strafverfolgungsbehörden sind so genannte „Online-Durchsuchungen“ in der Diskussion. Gegen eine entsprechende Befugnis im Nordrhein-Westfälischen Verfassungsschutzgesetz sind derzeit zwei Klagen beim Bundesverfassungsgericht anhängig. Zur Frage der Ermächtigungsgrundlage bezog Gerrit Hornung in DuD 8/2007 Position;[1] zu den technischen Hintergründen eines vom BND verfolgten Ansatzes äußerte sich Hartmut Pohl in DuD 9/2007.[2] Der vorliegende Beitrag systematisiert die technischen Möglichkeiten und Grenzen einer Online-Durchsuchung. Er basiert auf einer Stellungnahme des Autors anlässlich der Anhörung des Bundesverfassungsgerichts am 10. Oktober 2007.

Dirk Fox

Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.

E-Mail: dirk.fox@secorvo.de

1 Begriffliche Abgrenzung

Zielsetzung der so genannten „Online-Durchsuchung“ ist ein unbemerkter Zugriff von Strafverfolgungsbehörden und Nachrichtendienste auf informationstechnische Systeme Verdächtiger. Eine „Online-Durchsuchung“ soll Ermittlern den Zugriff auf Dokumente ermöglichen, der auf andere Weise nur sehr aufwändig oder überhaupt nicht realisierbar wäre.

Der Zugriff auf die Inhalte elektronischer Kommunikation (wie bspw. E-Mail oder digitale Telefonie, so genannte VoIP-Dienste), die einer herkömmlichen Telekommunikationsüberwachungsmaßnahme möglicherweise nicht zugänglich sind, weil die Zielperson Verschlüsselungsverfahren einsetzt, soll hingegen nach Auskunft des BMI nicht Gegenstand einer Online-Durchsuchung sein [BMI2_07]. Das BMI unterscheidet hier begrifflich und spricht in diesem Zusammenhang von „Quellen-Telekommunikationsüberwachung“.

Wie Buermeyer zutreffend anmerkt, ist „Online-Durchsuchung“ eine irreführende Bezeichnung, da im Unterschied zu einer Beschlagnahme das Zielsystem nicht zu einem bestimmten Zeitpunkt untersucht, sondern während eines definierten Zeitraums Benutzeraktivitäten an dem System überwacht und protokolliert werden sollen. Daher sei die Bezeichnung „Online-Überwachung“ zutreffender [Buer_07]. Das BMI verwendet hingegen die „Online-Durchsuchung“ als Oberbegriff, der eine „Online-Durchsicht“ (als verdeckten Akt der elektronischen Durchsuchung eines informationstechnischen Systems) und eine nachfolgende „Online-Überwachung“ über einen festgelegten Zeitraum umfasst [BMI2_07].

Dabei sind unter „informationstechnischen Systemen“ nicht nur Computer, sondern auch kleine, leistungsfähige mobile Endgeräte wie Personal Digital Assistants (PDAs) und Smartphones (Handys mit Zusatzfunktionen wie Adressdatenbank, Kalender, Dokumenten-Viewer und E-Mail-Programm) zu verstehen. Im Kontext von „Online-Durchsuchungen“ erscheint es – auch mit Blick auf die technische Entwicklung und zunehmende Konvergenz unterschiedlicher Technologien – sinnvoll, alle informationstechnischen Endsysteme, die über einen Internet-Zugang verfügen, in die Betrachtungen einzubeziehen.[3] Auch einige MP3-Player verfügen heute über leistungsfähige Kommunikationsmodule.

Die „Online-Durchsuchung“ selbst kann nicht nur den Zugriff auf (ausgewählte) Dokumente oder gespeicherte elektronische Nachrichten, sondern auch eine Protokollierung aller an einem informationstechnischen Endsystem vorgenommenen Aktivitäten umfassen, einschließlich aller Tastatureingaben (also auch PINs, Passwörter etc.). Schließlich können Schnittstellen des Zielsystems der Online-Durchsuchung genutzt werden, um weitere Systeme (z. B. über einen Netzwerkanschluss verbundene Rechner) zu untersuchen. Daher können auch über das Zielsystem erreichbare Server oder Server-Verzeichnisse von einer „Online-Durchsuchung“ betroffen sein [BMI2_07]. Eine Analyse der Betriebsumgebung z. B. durch Nutzung eines im Zielsystem eingebauten Mikrofons oder einer angeschlossenen Webcam zur Raumüberwachung ist technisch möglich, wird vom BMI jedoch ausgeschlossen.

Bei der zur „Online-Durchsuchung“ verwendeten Software spricht das BMI gemäß der internen Bezeichnung von „Remote Forensic Software“ (RFS). Dieser Begriff ist jedoch irreführend, da er suggerieren kann, dass die im Rahmen einer

[1] Hornung, Gerrit: *Ermächtigungsgrundlage für die „Online-Durchsuchung“?* DuD 8/2007, S. 575 ff.

[2] Pohl, Hartmut: *Zur Technik der heimlichen Online-Durchsuchung*. DuD 9/2007, S. 684 ff.

[3] Zwar könnten grundsätzlich auch andere Kommunikationstechnologien wie Fax-Verbindungen, Bluetooth- oder Infrarot-Übertragung genutzt werden. Deren Eignung ist jedoch wegen der geringen Übertragungsbandbreite und leichten Erkennbarkeit (Fax), der geringen Reichweite (Bluetooth) oder der Erforderlichkeit einer Sichtverbindung (Infrarot) stark begrenzt.

„Online-Durchsuchung“ gewonnenen Erkenntnisse den Beweiswert einer forensischen Analyse besitzen. Dies ist aus mehreren Gründen unzutreffend; daher wird hier von „Durchsuchungssoftware“ gesprochen.

2 Perspektive der Strafverfolgungsbehörden

Grundsätzlich lässt sich der Zugriff auf ein informationstechnisches System auch im Rahmen einer Beschlagnahme realisieren. Allerdings stößt die Beweiserhebung durch eine Beschlagnahme an Grenzen:

- Flüchtige Inhalte wie z. B. anonyme Eintragungen in einem Online-Forum oder Chat-Beiträge, aber auch ohne Ausgangskopie versandte (und vom Empfänger gelöschte) E-Mail-Nachrichten hinterlassen auf den für die Übermittlung genutzten Systemen wenige oder keine Spuren; die Inhalte sind daher in der Regel nicht rekonstruierbar, wenn keine Kopien auf dem System gespeichert wurden.
- Daten, die nur kurzzeitig auf dem Zielsystem gespeichert und wieder gelöscht wurden, sind bei einer Beschlagnahme nur dann rekonstruierbar, wenn die Löschung „oberflächlich“, beispielsweise mit den Löschfunktionen des Windows-Betriebssystems erfolgte. Hilfsprogramme ermöglichen jedoch eine vollständige und nicht-revidierbare Datenlöschung.
- Werden Daten vom Zielsystem aus auf externe Server übertragen und dort gespeichert, ist ein Zugriff darauf nur bei Kenntnis des externen Systems und der Zugangsdaten möglich. Sofern die Daten über verschlüsselte Verbindungen übertragen werden, ist mit herkömmlichen Ermittlungsmethoden ein Abhören der Zugangsdaten nicht möglich.
- Verschlüsselte Daten auf einem untersuchten System sind ohne Kenntnis des Entschlüsselungsschlüssels auch mit forensischen Methoden i.d.R. nicht rekonstruierbar. Ist sogar das gesamte System oder eine Festplatte vollständig verschlüsselt, sind die Daten nur nach Eingabe eines Entschlüsselungspassworts lesbar.
- Die auf mobilen Systemen gespeicherten Daten können einer Beschlagnahme durch spontane Vernichtung (z. B. mit Wasser, Feuer) oder, bei ausgewählten Geräten wie einigen Smartphones oder PDAs, der Auslösung einer Sofortlöschung entzogen werden.
- Bei geeigneter Gestaltung (z. B. Missbrauch eines fremden DSL-Anschlusses oder eines ungeschützten kabellosen Internet-Zugangs eines Dritten) ist der Nutzer des Zielsystems möglicherweise nicht identifizierbar, sodass keine Beschlagnahme veranlasst werden kann.
- Werden vom Zielsystem verschlüsselte Telefonie-Anwendungen genutzt (wie z. B. der Dienst Skype), dann sind diese Kommunikationsverbindungen einer herkömmlichen Telekommunikations-Überwachungsmaßnahme nicht zugänglich.

In allen genannten Fällen kann eine geeignete Online-Durchsuchungssoftware den Zugriff auf die jeweils genutzten Daten und Zugangspasswörter ermöglichen.

3 Technische Realisierung

Zur technischen Realisierung von Online-Durchsuchungen liegen – abgesehen von Veröffentlichungen in der Presse, die auf Mutmaßungen beruhen – sehr unkonkrete öffentliche Äußerungen des BKA, zwei ausführliche Stellungnahmen des BMI (zu Fragen des BMJ und der SPD-Bundestagsfraktion; [BMI1_07, BMI2_07]) und eine Veröffentlichung über durchgeführte Online-Durchsuchungen des Bundesnachrichtendienstes vor [Pohl_07]. Die folgende Darstellung basiert auf diesen Veröffentlichungen und wurde um weitergehende Überlegungen zu den grundsätzlichen technischen Realisierungsmöglichkeiten ergänzt.

3.1 Analyse des Zielsystems

Sowohl für die erfolgreiche Installation als auch für die Ausgestaltung der Durchsuchungssoftware sind Detailkenntnisse über die technischen Voraussetzungen auf dem Zielsystem erforderlich. Dazu zählen insbesondere

- das verwendete Betriebssystem (Hersteller, Version, Patch-Stand),
- der genutzte technische Internet-Zugang (Einwahl oder DSL, Provider),
- die genutzte Schutzsoftware (Virenschutz, Personal Firewall, Verschlüsselungssoftware etc.; ebenfalls mit Versionsstand),
- die vorgenommene Sicherheitskonfiguration (Rechte des Nutzers auf dem System, Konfiguration der Schutzsoftware) und
- die vom Benutzer des Zielsystems genutzten Kommunikationsdienste sowie die dafür verwendete Software mit Versionsangabe (z. B. VoIP, E-Mail, Browser).

Auch das Benutzerverhalten (Art, Zeitpunkt und Häufigkeit der Nutzung des Online-Zugangs) ist hilfreich für die konkrete Gestaltung der Durchsuchungssoftware. Die Erhebung dieser Daten im Rahmen von Vorermittlungen wird vom BMI im Wesentlichen bestätigt [BMI1_07].

Die Analyse kann (und soll) teilweise online durchgeführt werden; z. B. mit einem Portscanner, der offene Zugänge des Zielsystems identifiziert. Eine solche Analyse kann dem Betreiber des Zielsystems jedoch auffallen, da zahlreiche Antiviren-Programme und Personal Firewalls gezielte Portscans als Angriffsversuch registrieren und mit einer Warnmeldung reagieren.

Einzelne Angaben (wie Provider, technischer Zugang, Nutzungsverhalten) können durch Observation und herkömmliche Ermittlungsmethoden gewonnen werden. Die Mitwirkung Dritter (Provider, andere Behörden etc.) ist dazu nicht erforderlich, wiewohl möglicherweise hilfreich.

Gesicherte Erkenntnisse über das Betriebssystem, die eingesetzte Sicherheitssoftware und deren Konfiguration setzen allerdings eine genaue Kenntnis des Zielsystems voraus, die nur mit einem Zugriff auf das Zielsystem gewonnen werden kann, da die Angaben in Online-Verbindungen[4] vom Betreiber des Zielsystems modifiziert bzw. von eingesetzten Sicherheitsmechanismen unterdrückt werden können. Zahlreiche Informationen können über eine Online-Verbindung gar nicht in Erfahrung gebracht werden.

Die Auswertung der Ergebnisse dieser Analyse kann auch ergeben, dass eine Online-Durchsuchung im vorliegenden Fall mit den verfügbaren technischen Mitteln nicht möglich ist [BMI2_07].

[4] So meldet beispielsweise jeder Browser beim Zugriff auf eine Webseite u. a. Name und Version des verwendeten Betriebssystems, den eingesetzten Browser und die Version. Diese Angaben können jedoch manipuliert werden.

3.2 Installation der Durchsuchungssoftware

Der wesentliche und zugleich schwierigste technische Teil einer Online-Durchsuchung ist der Mechanismus, mit dem eine Durchsuchungssoftware auf einem Zielsystem installiert wird. Dies kann grundsätzlich durch drei unterschiedliche Methoden geschehen:

- Entfernte manuelle Installation: Durch die Ausnutzung einer unsicheren Konfiguration des Zielsystems oder eines (möglicherweise sogar nicht allgemein bekannten) Fehlers im Betriebssystem oder einer Online-Anwendung (z. B. dem Browser) wird die Durchsuchungssoftware über das Internet auf das Zielsystem übertragen und dort fest installiert. Dabei ist keine Mitwirkung des Benutzers des Zielsystems erforderlich.
- Automatische Hintergrund-Installation: Die Installation wird in einem anderen Prozess versteckt und im Hintergrund durchgeführt. Dabei kann die Installation verschiedene Mechanismen nutzen, die auch bei Viren und Trojanern Anwendung finden. Hierbei ist eine Mitwirkung des Benutzers erforderlich:
  - Installation über eine infizierte Webseite: Auf einer Webseite, die vom Benutzer des Zielsystems regelmäßig besucht wird, wird ein Script-Programm verborgen, dass bei Aufruf der Webseite durch das Zielsystem ein Installationsprogramm startet und die Durchsuchungssoftware nachlädt und installiert.
  - Installation über eine CD/DVD: Nach Einlegen einer dem Benutzer des Zielsystems zugestellten CD/DVD installiert eine Autostart-Funktion das Durchsuchungsprogramm im Hintergrund.
  - Installation über einen USB-Stick: Neue Generationen von USB-Sticks gaukeln dem System-BIOS des Zielrechners ein CD-Laufwerk vor und können somit ebenfalls eine Installation über die Autostart-Funktion im Hintergrund aktivieren.
  - Installation über ein Update: Dem Betreiber des Zielsystems wird ein manipuliertes Software-Update zugestellt, das die Durchsuchungssoftware mitinstalliert. Vorteil: Der Benutzer kann so möglicherweise veranlasst werden, die Installation mit Administratorrechten durchzuführen.
  - Installation über einen E-Mail-Anhang: E-Mail-Anhänge können (als Dokumenten-Anhang getarnt oder unter Ausnutzung einer Sicherheitslücke der Darstellungssoftware) ausführbaren Programmcode enthalten. Öffnet der Empfänger den Anhang, wird dieser gestartet und kann die Installation im Hintergrund vornehmen.
- Manuelle Installation: Sofern ein direkter physischer Zugriff auf das Zielsystem besteht, kann die Durchsuchungssoftware auch direkt auf diesem System installiert werden. Das geht vergleichsweise einfach, wenn auf dem System keine wirksamen Sicherheitsmechanismen eingerichtet sind (wie beispielsweise eine Vollverschlüsselung des Systems). Mit Hilfsmitteln können ggf. aber auch diese Schutzmechanismen umgangen werden, z. B. durch den Einsatz eines „Key-Loggers“, um die zum Starten des Systems benötigten Passworte mitzuschneiden. Ein solcher Zugriff erfordert in der Regel ein ein- oder sogar mehrmaliges verdecktes Eindringen in die Räume der Zielpersonen.[5]

In allen drei Fällen wird die Durchsuchungssoftware so im System verankert, dass sie bei jedem Neustart des Zielsystems ebenfalls gestartet wird und als (versteckter) Hintergrundprozess läuft.

Sowohl bei der entfernten manuellen Installation als auch bei der automatischen Hintergrund-Installation spielt die Ausnutzung von Schwachstellen der auf dem Zielsystem eingesetzten Betriebssystem- und Anwendungssoftware eine zentrale Rolle. Werden dabei veröffentlichte Schwachstellen genutzt, kann der Betreiber des Zielsystems sich in der Regel (sofern bereits verfügbar) durch einen Hersteller-Patch davor schützen. Nach [Pohl_07] werden daher bereits seit 2005 vom Bundesnachrichtendienst (BND) „Less Than Zero Day Exploits“, d.h. noch nicht öffentlich bekannte kritische Schwachstellen, zur Installation von Durchsuchungssoftware eingesetzt. Die Existenz und die technischen Details solcher kritischen Schwachstellen müssen sehr aufwändig recherchiert, teuer erworben oder ersteigert werden.[6]

Eine vierte Möglichkeit, Online-Durchsuchungssoftware zu installieren, wird derzeit vom BMI ausgeschlossen, wäre aber ebenfalls möglich (allerdings mittelfristig kaum zu verbergen):

- Einbau einer „Hintertür“: Verbreitete Soft- oder Hardware könnte mit einer „Hintertür“ ausgestattet werden, die den Strafverfolgungsbehörden jederzeit einen Zugriff auf die Systeme ermöglicht.[7]

Zentrale Schwierigkeit bei der Installation der Durchsuchungssoftware ist die genaue Identifikation des Zielsystems, um sicher zu stellen, dass kein unbeteiligtes System erreicht wird. Dafür müssen eindeutige Merkmale des Systems bekannt sein. Die IP-Adresse des Systems kann dabei nicht als Identifikationsmerkmal dienen, da sie in der Regel von einem Online-Provider dynamisch vergeben wird. Auch die Installation über ein Web-Angebot ist nur dann einigermaßen zielscharf, wenn eine Identifikation des Benutzers (z. B. Eingabe von Login-Daten) erfolgt ist; selbst dann ist aber nicht gewährleistet, dass das Login tatsächlich vom Zielsystem erfolgte.[8] Auch die – im Auslieferungszustand weltweit eindeutige – MAC-Adresse der Kommunikationshardware (Netzwerkkarte) ist als Merkmal nur eingeschränkt geeignet, da die Angabe nach Start des Systems manuell verändert werden kann. Eindeutig wird das Zielsystem nur erreicht, wenn die Installation der Durchsuchungssoftware manuell erfolgt.

3.3 Ausgestaltung der Durchsuchungssoftware

Die Durchsuchungssoftware muss an das Zielsystem angepasst werden. So ist mindestens erforderlich, dass die Software sich mit dem auf dem Zielsystem verwendeten

[5] “Key-Logger“ im PC-Tastaturkabel, zumindest handelsübliche Versionen, sind möglicherweise für einen Observierten leicht erkennbar. Sie helfen nicht bei mobilen Systemen wie Laptops, Smartphones oder PDAs.

[6] In der „Szene“ spricht man von z. T. sechsstelligen Summen, die für „Less Than Zero Day Exploits“ gezahlt wurden.

[7] Das BMI hält dies für derzeit „politisch nicht gewollt“ [BMI2_07]. Zudem könnten nur deutsche Hersteller zum Einbau von Hintertüren verpflichtet werden; Täter könnten auf ausländische Software oder Open-Source-Produkte ohne Hintertüren ausweichen. Hintertüren sind grundsätzlich problematisch im Hinblick auf die Missbrauchsmöglichkeit durch Dritte und das Vertrauen der Bürger in die Sicherheit informationstechnischer Systeme und Dienste.

[8] Die Verbindung könnte auch aus einem Internet-Café oder einem anderen Internet-fähigen Gerät wie einem Smartphone, oder aber von dem System eines Dritten stammen.

Betriebssystem (Microsoft Windows 2000/XP/Vista/Mobile, Palm OS, Symbian OS, Apple OS/X, ...) verträgt. Gegebenenfalls sind Besonderheiten des Geräts zu berücksichtigen, wie z. B. die Art des Internet-Zugangs (WLAN-Login, ISDN-Einwahl, DSL-Leitung, UMTS-Verbindung o.ä.).

Der Leistungsumfang einer Durchsuchungssoftware kann erheblich sein. Das BMI nennt die folgenden Funktionen [BMI1_07, BMI2_07]:

- Systemanalyse (Betriebssystem, Patch-Level, Leistungsmerkmale, installierte Programme, Benutzeraccounts, ...), Zugriff auf Systemeinstellungen
- Erstellung von Verzeichnisübersichten, Durchsuchen von Verzeichnissen nach bestimmten Dateinamen, Volltextsuche nach Stichworten
- Durchsuchen angeschlossener Datenspeicher (USB-Sticks, CDs/DVDs, Flash-Memory, externe Festplatten, zugängliche Netzwerk-Laufwerke/Server-Laufwerke)
- Herunterladen von ausgewählten Dokumenten (Texte, Bilder, ...)
- Tastatur-Logger (Protokollierung aller Tastaturanschläge)
- Remote-Deaktivierung (unbemerkte Entfernung der Durchsuchungssoftware vom System, Spurenlöschung)
- Automatische Deaktivierung (nach Zeitablauf)

Verbreitete (bösartige) so genannte „Trojaner“ bieten darüber hinaus die folgenden Dienste:

- Protokollierung von Internetzugriffen (URL, Datentransfers, Verweildauer, ...)
- Passwort-Protokollierung (Web-Dienste, Entschlüsselung von Daten etc.)
- Einblenden von Meldungen auf dem Zielsystem (um den Nutzer zu bestimmten Reaktionen zu veranlassen)
- Netzwerk-Scan (Analyse weiterer über ein Netzwerk oder ein Kommunikationsprotokoll angeschlossene Geräte wie z. B. PDAs zur Synchronisation)
- Übermittlung des vollständigen Bildschirminhalts („Screen-Shots“)
- Abfangen von gesendeten und empfangenen elektronischen Nachrichten (nach Angaben des BMI Teil einer „Quellen-Telekommunikationsüberwachung“)
- Raumüberwachung (Aktivierung des Rechnermikrofons, Aktivierung einer angeschlossenen Web-Kamera; nach Angaben des BMI nicht geplant)

Auch weitere Funktionen sind möglich, wie z. B. das Nachladen weiterer Software, die Speicherung einer auf das Zielsystem „hochgeladenen“ Datei, die gezielte Modifikation von Daten oder die Destabilisierung bzw. Zerstörung des Zielsystems, bis hin zur vollständigen Datenlöschung. Auch könnte die Software versuchen, über Infrarot- oder Bluetooth-Schnittstellen Verbindung zu anderen Geräten in der unmittelbaren Umgebung (Handy, Smartphone, PDA, PC etc.) herzustellen und dort nach abrufbaren Daten zu suchen.[9]

Zum Verbergen der Aktivitäten während einer Online-Durchsuchung sollten ressourcenintensive Funktionen so genutzt werden können, dass sie nur einen begrenzten Teil der Rechenleistung und der Kommunikationsbandbreite des Zielsystems belegen.

Da die verschiedenen technisch möglichen Dienste und Leistungsmerkmale unterschiedlich stark in die Persönlichkeitsrechte der Zielpersonen eingreifen, ist möglicherweise eine gesetzliche Abgrenzung des Leistungsumfangs einer Online-Durchsuchung sinnvoll.

3.4 Durchführung der Online-Durchsuchung

Die Online-Durchsuchung selbst wird nach Installation der Durchsuchungssoftware zu einem geeigneten Zeitpunkt durch Fernzugriff auf das Zielsystem oder zu einem zuvor festgelegten Zeitpunkt gestartet und durchgeführt. Um keine Missbrauchsmöglichkeit von außen zu bieten, wird die Durchsuchungssoftware als „inside out“-Attacke realisiert, d. h. die Verbindung zu einem Server der Strafverfolgungsbehörden wird von der Durchsuchungssoftware von „innen“ (dem Zielsystem) nach „außen“ (dem Server) aufgebaut.

Die Online-Durchsuchung kann entweder während einer Online-Verbindung und bei eingeschaltetem Zielsystem erfolgen, oder anhand vorgegebener Such-Kommandos („Script“, „Batch“) auch ohne Online-Verbindung automatisiert durchgeführt werden. In letzterem Fall werden die Ergebnisse (gefundene Dokumente, Übersichten, protokollierte Aktivitäten etc.) bis zur nächsten Online-Verbindung zwischengespeichert und erst dann an ein externes, von den Strafverfolgungsbehörden kontrolliertes System übertragen.

Nach Auskunft des BMI soll diese Zwischenspeicherung verschlüsselt erfolgen [BMI1_07]. Wegen der begrenzten „upload“-Bandbreite der meisten Online-Zugänge, aber auch um die Aktivität der Durchsuchungssoftware zu verbergen, sollen die übermittelten Daten geeignet auf wesentliche Informationen beschränkt werden.

4 Gegenmaßnahmen

Tatsächlich sind keine Möglichkeiten bekannt, eine Online-Durchsuchung so zu gestalten, dass ein Zielsystem nicht wirksam davor geschützt werden kann. Der Betreiber des Zielsystems kann durch geeignete Maßnahmen entweder

- die Installation („Einnistung“) der Durchsuchungssoftware auf seinem System verhindern

oder

- durch Sicherheitssoftware die Arbeit der Durchsuchungssoftware aufdecken oder zumindest erheblich behindern.

Im Vorfeld kann zudem die Informationserhebung über das Zielsystem erschwert werden.

Das bedeutet nicht, dass eine Online-Durchsuchung damit von vorneherein erfolglos wäre. Tatsächlich muss zumindest zur Zeit davon ausgegangen werden, dass hinreichend viele Zielsysteme nicht besonders wirkungsvoll vor einer Online-Durchsuchung geschützt sind. Allerdings kann sich dies schnell ändern, sollten Online-Durchsuchungen gesetzlich verankert werden.

Im Rahmen der Voranalyse des Zielsystems können zumindest einige der möglichen Schutzmechanismen identifiziert und damit die Wahrscheinlichkeit einer wirkungslosen Investition in eine Online-Durchsuchung zumindest verringert werden.

4.1 Behinderung der Informationsbeschaffung

Wird das Zielsystem durch geeignet konfigurierte Sicherheitssoftware, ein (gut gewähltes) Zugangspasswort und eine vollständige Festplattenverschlüsselung geschützt, ist ohne Kenntnis der entsprechenden Passwörter eine Analyse des Systems auch bei direktem Zugriff (Beschlagnahme oder Vor-Ort-Analyse) zunächst einmal

[9] Diese Funktion setzt eine entsprechend „offene“ Konfiguration der betroffenen Geräte voraus. Auch kann ein solcher Verbindungsaufbauversuch durch eine Meldung des Geräts auffallen.

praktisch unmöglich. Ist das Zielsystem ein PC, kann gegebenenfalls die Nutzung eines „Key-Loggers“, der im Tastaturkabel eingesetzt wird, helfen, um die erforderlichen Zugangs-Passwörter zu ermitteln; dazu ist allerdings ein mehrmaliger physischer Zugriff auf das Zielsystem erforderlich. Ist das Zielsystem hingegen ein mobiles Gerät (PDA, Laptop, Smartphone), kann durch eine Vollverschlüsselung ein direkter Zugriff auf das System verhindert werden.

Durch die Nutzung unterschiedlicher Internet-Provider und verschiedener (wechselnder) Zugangsprotokolle (z. B. UMTS, DSL, ISDN) oder diverser Anonymisierungsdienste kann der Nutzer zudem die Identifikation des Zielsystems erschweren. Auch könnte eine Zielperson alle relevanten Daten auf einer Flash-Speicherkarte (im Handel für unter 50 € erhältlich) ablegen und diese in wechselnden Zielsystemen nutzen (Smartphone, PDA, PC).

4.2 Verhinderung der Installation

Um die „Einnistung“ der Durchsuchungssoftware auf einem Zielsystem zu verhindern, kann der Betreiber des Zielsystems zahlreiche Maßnahmen ergreifen:

- Patchen des Betriebssystems: Durch regelmäßiges Einspielen von Software-Updates des Betriebssystems auf dem Zielsystem werden die Möglichkeiten, eine Durchsuchungssoftware über eine veröffentlichte Betriebssystem-Lücke remote zu installieren, erheblich eingeschränkt. Werden die System-Patches dabei ausschließlich über eine vertrauenswürdige Quelle bezogen oder deren Integrität überprüft (Hashwerte, Signaturen), ist es zudem schwierig, dem Betreiber des Zielsystems ein manipuliertes Update unterzuschieben.
- Restriktive Konfiguration des Systems: Wird das Zielsystem ausschließlich mit eingeschränkten Benutzerrechten betrieben, kann z. B. unter dem Betriebssystem Windows keine Durchsuchungssoftware installiert werden, die automatisch beim Boot-Vorgang gestartet wird. Eine verborgene automatische Installation von einem Boot-fähigen Medium wie einem USB-Stick, einer CD oder DVD kann verhindert werden, indem Bootvorgänge durch entsprechende BIOS-Einstellungen nur von der Boot-Partition der Festplatte zugelassen werden.
- Restriktive Konfiguration des Browsers: Erlaubt der verwendete Internet-Browser keine Script-Sprachen oder die Ausführung aktiver Webseiten-Inhalte, wird eine Installation einer Durchsuchungssoftware über eine entsprechend manipulierte Web-Seite wirksam verhindert (sofern die Browser-Version keine Schwachstelle enthält).
- Nutzung eines Virenscanners: E-Mails mit kritischen Anhängen können heute von guten Virenscannern erkannt werden; mit Hilfe heuristischer Verfahren entdecken sie auch alle Versuche, beispielsweise Tastatureingaben mitzuschneiden oder ein Programm im Betriebssystem zu verankern und schlagen mit einer entsprechenden Meldung Alarm. Ohne explizite Freigabe durch den Nutzer werden solche Programmaufrufe blockiert.
- Ständige Wechsel des Online-Zugangs: Wechselt das System für jede Online-Verbindung den Zugangsweg, z. B. indem es offene WLANs nutzt oder schlecht geschützte WLAN-Verbindungen[10] hackt und missbraucht, ist es für eine zielgerichtete Installation der Durchsuchungs-Software möglicherweise nur per E-Mail erreichbar. Auch durch die Nutzung von Anonymisierungsdiensten kann das System verborgen werden.
- Sicherheitssensibler Umgang mit E-Mails: Werden E-Mail-Anhänge vom Benutzer grundsätzlich nicht aufgerufen oder gestartet sondern gleich gelöscht, ist eine Aktivierung des Installationsprozesses auf diesem Weg ausgeschlossen.
- Nutzung einer Personal Firewall: Über eine (restriktiv konfigurierte) Personal Firewall kann verhindert werden, dass ein gestartetes Installationsprogramm weiteren Code über eine Online-Verbindung des Systems nachlädt.
- Einsatz „Virtueller Maschinen“: Wird das Zielsystem als „Virtuelle Maschine“, gewissermaßen auf einem „simulierten Rechner im Rechner“ betrieben, und wird die ursprüngliche virtuelle Maschine täglich neu gestartet, ist damit auch eine erfolgreich installierte Durchsuchungssoftware spätestens beim nächsten Neustart entfernt.
- Booten von CD: Wird der PC von einem schreibgeschützten Medium (z. B. einer CD) mit einem „sauberen“ und konservativ konfigurierten Betriebssystem gebootet, ist auf diesem System eine Installation der Durchsuchungssoftware nicht möglich.

Werden für die Installation „Less Than Zero Day“-Exploits verwendet, d. h. unveröffentlichten Sicherheitslücken, die von Mitgliedern einschlägiger Hacker-Kreise identifiziert, aber dem betroffenen Softwarehersteller nicht mitgeteilt oder veröffentlicht wurden, kann damit möglicherweise auch die eine oder andere der vorgeschlagenen Schutzmaßnahmen umgangen werden. Werden alle oben genannten Maßnahmen am Zielsystem ergriffen, sollte jedoch auch keine Installation unter Verwendung unveröffentlichter Schwachstellen (die naturgemäß nicht durch einen Patch des Herstellers beseitigt werden können) möglich sein.

4.3 Behinderung der Online-Durchsuchung

Auch wenn es gelungen ist, eine Durchsuchungssoftware auf einem Zielsystem zu installieren, kann deren erfolgreiche Nutzung verhindert werden. Die wichtigsten Schutzmechanismen sind die folgenden:

- Nutzung einer Personal Firewall: Eine Personal Firewall erlaubt eine sehr restriktive Behandlung ein- und ausgehender Kommunikationsverbindungen. Bei strikter Konfiguration werden alle ausgehenden Verbindungen blockiert, die nicht von ausdrücklich freigegebenen Anwendungen kommen. Die Übermittlung von Daten durch eine Durchsuchungssoftware ließe sich so mit sehr hoher Wahrscheinlichkeit verhindern und würde durch eine entsprechende Meldung der Firewall auffallen, sofern die Software nicht versteckte Kommunikationskanäle über eine laufende Anwendung aufbaut.
- Schutz vor (Software-)Key-Loggern: Einige Virenscanner und Personal Firewalls installieren einen Key-Logger-Schutz, der erkennt, wenn ein Prozess gestartet wird, mit dem Tastatureingaben „abgefangen“ werden können.[11]
- Neuinstallation des Systems: Wird das System von Zeit zu Zeit von einem „sauberen“, gleich nach der Erstinstallation und vor jedem Internet-Kontakt ers-

[10] Beispielsweise lässt sich das verbreitete WEP-Protokoll zum Schutz von WLAN-Verbindungen innerhalb weniger Minuten kompromittieren.

[11] Dieser „Key-Logger“-Schutz erkennt keine „Hardware-Key-Logger“, die üblicherweise als vermeintliche Verlängerung des Tastaturkabels in PCs eingesetzt werden.

tellten Boot-Image neu installiert (Aufwand ca. eine Stunde), werden alle seitdem möglicherweise installierten Durchsuchungsprogramme beseitigt. Eine Alternative ist die im vorangegangenen Abschnitt genannte Nutzung einer „Virtuellen Maschine“, die regelmäßig neu gestartet wird, oder einer Boot-CD.

- Integritäts-Checks: Es existieren Schutzprogramme, die alle Systemdienste und eine Liste der manuell vom Benutzer zugelassenen Anwendungsprogramme mit Integritäts-Checksummen oder sogar einer digitalen Signatur versehen. Wird ein Programm gestartet oder ausgeführt, das über keine vom Nutzer freigegebene Checksumme oder von ihm erzeugte digitale Signatur verfügt, alarmiert das Schutzprogramm und verhindert die Ausführung.
- Protokollierung/Filterung: Die Inhalte aller über die Kommunikationsverbindung des Zielsystems übertragenen Daten lassen sich mit (frei verfügbaren) Programmen protokollieren. Bei einer gründlichen Auswertung der Protokolle können unerwünschte und keiner bekannten Anwendung zuzuordnende Übertragungen auch bei verschlüsselter Übermittlung auffallen. Ein Filter, der Verbindungen nur zu ausgewählten Systemen (E-Mail-Server, Bank etc.) zulässt, würde Übermittlungsversuche einer Durchsuchungssoftware blockieren (und entdecken).

Auch nach erfolgreicher Durchführung und dem Abschluss einer Online-Durchsuchung inklusive Beseitigung der Durchsuchungssoftware kann die Durchsuchung möglicherweise nachträglich entdeckt werden, z. B. wenn im Durchsuchungszeitraum Backups vom Zielsystem erstellt wurden und diese zurückgespielt und analysiert werden.

Einige der vorgenannten Schutzmechanismen könnte die Durchsuchungssoftware deaktivieren oder umkonfigurieren. Dann würde allerdings die Sicherheit des betroffenen Systems insgesamt beeinträchtigt. Nach Auskunft des BMI ist eine solche Veränderung der Systemkonfiguration des Zielsystems nicht vorgesehen [BMI1_07].

4.4 Manipulation einer Online-Durchsuchung

Bemerken Verdächtige die Durchführung einer Online-Durchsuchung, können sie auch gezielt falsche Spuren legen oder mit manipulierten Dokumenten Fehlbewertungen verursachen. Zugleich wäre es leicht möglich, die Kommunikation auf ein anderes, bislang unverdächtiges Zielsystem zu verlagern und dieses geeignet vor einer Online-Durchsuchungssoftware zu schützen.

5 Grenzen der Online-Durchsuchung

Die Annahme, die Online-Durchsuchung eines Zielsystems führe zu den gewünschten Fahndungsergebnissen, basiert auf verschiedenen Voraussetzungen und ist nur innerhalb einiger grundsätzlicher Grenzen zutreffend:

- So können Online-Durchsuchungen (wie der Name sagt) nur auf Zielsystemen durchgeführt werden, die über eine aktive Online-Verbindung verfügen. Besteht nur temporär eine Online-Verbindung, können nur während dieser Verbindungen eine Durchsuchung gestartet, gesteuert bzw. die Ergebnisse abgerufen werden.
- Die Ergebnisse einer Online-Durchsuchung sind in der Regel auf die auf dem Zielsystem gespeicherten Daten beschränkt.[12] Wird das Zielsystem ausschließlich für Kommunikationszwecke genutzt, während die sonstige Datenverarbeitung auf einem Stand-Alone-System ohne Netzzugang erfolgt, sind der Durchsuchungssoftware nur ausgewählte Kommunikationsdaten zugänglich und fällt das Ermittlungsergebnis dürftig aus.
- Der Beweiswert der Ergebnisse einer Online-Durchsuchung könnte – selbst bei einer lückenlosen Dokumentation, wie sie vom BMI angekündigt wurde [BMI2_07] – aus mehreren Gründen in Frage stehen:
  - Grundsätzlich könnte, wenn ein Online-Zugriff auf ein Zielsystem besteht, auch ein belastendes Dokument zunächst auf das System überspielt werden, bevor es anschließend im Rahmen der Durchsuchung „gefunden“ wird. Auch die vom BMI angegebene Quellcode-Hinterlegung bei Gericht schließt eine solche Manipulation der Beweismittel nicht aus: Schließlich könnte dafür eine andere als die hinterlegte Software-Version eingesetzt oder das Dokument manuell auf dem Zielsystem abgelegt worden sein.
  - Die Zuordnung des Zielsystems zu einer verdächtigen Person kann mit technischen Mitteln nicht belegt werden. Mittels Online-Durchsuchung kann auch der Standort des Zielsystems nicht bestimmt werden. Selbst bei Mitwirkung des Online-Providers ist der Standort in einigen Fällen nicht hinreichend eingrenzbar, beispielsweise wenn der Zugang über UMTS erfolgt oder eine DSL-Verbindung über WLAN genutzt wurde. Da ein Missbrauch fremder DSL-Zugänge über offene oder gehackte WLAN-Verbindungen sehr leicht und sogar mit ständig wechselnden Zugängen möglich ist, kann das Zielsystem leicht seine Spuren verwischen.
  - Entscheidend bei forensischen Untersuchungen ist die persönliche Bezeugung von wichtigen Schritten durch einen Dritten, die schriftlich festgehalten wird. Eine Bezeugung der Vorgänge auf dem Zielsystem ist bei einem Fernzugriff prinzipiell unmöglich; dies kann auch eine Protokollierung (Log-File) nicht ausgleichen.
  - Entdeckt der Benutzer oder Betreiber des Zielsystems die Online-Durchsuchung, kann er die Untersuchungsergebnisse manipulieren. Damit können Originalität und Integrität der gefundenen Dokumente in Frage stehen.
- Vorbereitung und Durchführung einer Online-Durchsuchung erfordern (ggf. sogar sehr viel) Zeit und sind daher ungeeignet bei „Gefahr im Verzug“.

6 Kosten der Online-Durchsuchung

Die Kosten einer Online-Durchsuchung können erheblich sein. Dies wird weniger durch die eigentliche Durchführung der Durchsuchung verursacht, die in der Regel in wenigen Stunden oder automatisiert über einen längeren Überwachungszeitraum durchgeführt werden kann. Vielmehr entfällt auf die Vorbereitung der größte Teil der Kosten. Diese Vorbereitungskosten lassen sich wie folgt unterteilen:

- Vor-Analyse des Zielsystems: Identifikation der Systemkonfiguration und Suche nach möglichen Systemschwächen, die

[12] Ausnahme: Sofern das Zielsystem mit weiteren Systemen z. B. über eine Netzwerkverbindung gekoppelt ist, können auch diese Systeme Ziel der Untersuchung sein.

für die Installation der Durchsuchungssoftware ausgenutzt werden können.

Der Aufwand hängt dabei ab von der Leistungsfähigkeit der für die Analyse zur Verfügung stehenden Hilfsprogrammen (je „exotischer" das Betriebssystem, desto weniger freie oder käufliche Analyseprogramme existieren) und der Qualität der Konfiguration des Zielsystems (z. B. durch Deaktivierung „geschwätziger" Systemprogramme oder Vortäuschung falscher Systemeigenschaften). Bei durchschnittlich geschützten Systemen mit verbreitetem Betriebssystem ist mit einem Aufwand von wenigen Stunden bis Tagen zu rechen. Exotische oder besonders gut geschützte Systeme können einen mehrwöchigen Aufwand erfordern, möglicherweise auch den Einsatz von (klassischen) Ermittlern.

- Entwicklung resp. Anpassung der „Installationssoftware": Der Installationsmechanismus für die Durchsuchungssoftware muss auf die gefundenen Schwachstellen des Zielsystems und dessen Betriebssystem zugeschnitten werden.

Der Aufwand für die Entwicklung des Installationsmechanismus hängt davon ab, ob eine verbreitete „Standard-Systemschwäche" unter Nutzung eines bereits verfügbaren Installationsmechanismus (bspw. ein „Less Than Zero Day Exploit") verwendet werden kann, oder Betriebssystem und gefundene Sicherheitsschwächen die Entwicklung eines neuen Installationsmechanismus erfordern. Ein bereits existierender Installationsmechanismus für ein Standard-Betriebssystem lässt sich in wenigen Stunden anpassen; ein neuer Mechanismus kann mehrere Wochen Entwicklungsaufwand erfordern.

- Entwicklung resp. Anpassung einer Durchsuchungssoftware: Die Durchsuchungssoftware muss entweder gezielt für eine gefundene Schwachstelle entwickelt oder zumindest an das Betriebssystem des Zielsystems angepasst werden. Das BMI spricht sogar davon, dass die „entwickelte Software [...] grundsätzlich nur einmal zum Einsatz kommen" soll [BMI1_07]. Ggf. sind weitere Spezifika des Zielsystems, möglicherweise auch spezielle Leistungsmerkmale in der Software zu berücksichtigen.

Der Aufwand für die Entwicklung ist erheblich; ein leistungsfähiges System kann bis zu einem Personenjahr erfordern. Offenbar wurde im BKA bereits ein fast einsatzfähiger Prototyp entwickelt [BMI2_07], der nach Aufhebung des verfügten Entwicklungsstopps kurzfristig verfügbar wäre. Die dabei entwickelte Software kann jedoch nur für Zielsysteme mit demselben Betriebssystem wiederverwendet werden. Sie ließe sich mit begrenztem Aufwand (wenige Tage oder Wochen) auf jeweils neue Betriebssystemversionen portieren. Unterschiedliche Betriebssysteme erfordern jedoch eine weitgehende Neuentwicklung; muss eine andere Programmiersprache (z. B. Java für Smartphones) verwendet werden, ist eine vollständige Neuprogrammierung erforderlich.

Die Kosten einer einzelnen Online-Durchsuchung lassen sich senken, indem eine leistungsfähige Standard-Durchsuchungssoftware entwickelt und auf mehrere verbreitete Betriebssysteme portiert wird. Sie könnte in vielen Fällen ohne oder mit nur wenigen Anpassungen eingesetzt werden. Zu berücksichtigen ist allerdings, dass jährlich wenigstens eines der verbreiteten Betriebssysteme in einer neuen Version herausgegeben wird und dadurch möglicherweise Anpassungen der Software respektive zusätzliche Portierungen erforderlich werden können. Wird die Durchsuchungssoftware einem Hersteller von Anti-Virus-Lösungen bekannt, muss die Lösung erheblich umprogrammiert werden, damit die Software bei Wiederverwendung nicht von Anti-Virus-Lösungen automatisch erkannt und beseitigt wird.

Die Durchführung einer Online-Durchsuchung nach erfolgreicher Installation der Durchsuchungssoftware auf dem Zielsystem erfordert – bei Verwendung einer leistungsfähigen Durchsuchungssoftware – nur wenige Stunden oder (abhängig vom Ermittlungsziel) eine automatisierbare Überwachung über einen längeren Zeitraum (z. B. Suche nach Schlüsselworten, URLs, Passworteingaben etc.). Das BMI spricht von zwei Personen „zur Konfiguration und Bedienung (Schichtdienst)" und ggf. Übersetzern und weiteren Ermittlern während einer aktiven Überwachung [BMI2_07].

Der für die anschließende Auswertung der gefundenen Daten erforderliche Aufwand hängt vom konkreten Ermittlungsziel ab und lässt sich daher nicht allgemein beziffern. Die Tätigkeit dürfte vergleichbar sein der Auswertung von Papierdokumenten nach einer Beschlagnahme bzw. herkömmlichen Durchsuchung.

7 Risiken der Online-Durchsuchung

Online-Durchsuchungen können nahezu spurlos realisiert werden. Außer externen Protokolldaten (z. B. auf einer Firewall oder beim Internet-Provider) oder auf Backups bleiben keine Zugriffsdaten zurück, wenn die Durchsuchungssoftware über die erforderlichen Rechte auf dem lokalen System verfügt und sich zum Abschluss selbst vom System entfernt.

Wird eine Online-Durchsuchung auf dem Zielsystem erkannt, könnten die Strafverfolgungsbehörden durch das Unterschieben geeigneter Desinformationen irregeleitet werden. Möglicherweise besitzt eine solche, gut gemachte Desinformation besondere Glaubwürdigkeit, weil sie vermeintlich unbeobachtet gewonnen wurde.

Umgekehrt könnte die Verbreitung von Online-Durchsuchungen den Beweiswert beschlagnahmter Systeme senken, da nicht ausgeschlossen werden kann, dass die gefundenen Dokumente im Rahmen einer Online-Durchsuchung gezielt auf dem System platziert wurden.

Der Missbrauch einer eingesetzten Online-Durchsuchungssoftware durch Dritte, die die Software auf einem Zielsystem entdecken und analysieren (z. B. für eigene Angriffe) ist grundsätzlich nicht auszuschließen. Nach Auskunft des BMI soll dies durch die Verwendung kryptographischer Verfahren zumindest erschwert werden [BMI1_07]. Andererseits gibt es zahlreiche freie und bekannte Angriffs-Programme im Internet, die sich für vergleichbare Angriffe eignen und sogar direkt genutzt oder, falls als „Open-Source"-Software verfügbar, modifiziert in eine Eigenentwicklung integriert werden können.

Eine allgemeine Bedrohung der Sicherheit von IT-Systemen durch Durchsuchungssoftware besteht – anders als in zahlreichen Äußerungen in den Medien befürchtet – nicht, sofern die Durchsuchungssoftware auf ein bestimmtes Zielsystem zugeschnitten und nur dort installiert wird.

Erfolgt die Installation der Durchsuchungssoftware unter Ausnutzung eines so genannten „Less Than Zero Day Exploits", so ist sicherlich problematisch, dass durch die Geheimhaltung solcher Schwachstellen, von denen eine Bundesbehörde durch Kauf oder eigene Recherche Kenntnis erhält, die reale Bedrohung von vielen Millionen IT-

Systemen verlängert wird. Eine behördliche Nachfrage nach „Less Than Zero Day Exploits“ könne zudem einen gefährlichen Markt fördern und zu Geheimhaltung und Verkauf gefundener Sicherheitsschwachstellen motivieren, die heute üblicherweise publiziert und den Herstellern zur Entwicklung von Patches mitgeteilt werden.

8 Fazit

Zusammenfassend sind die folgenden Fakten festzuhalten:

- Online-Durchsuchungen ermöglichen den Strafverfolgungsbehörden prinzipiell den Zugriff auf Daten, die bei einer Beschlagnahme nicht erreicht werden (z. B. flüchtige Kommunikationsdaten, Klardaten verschlüsselter Dateien oder Kommunikationsinhalte).
- Da die verschiedenen technisch möglichen Dienste und Leistungsmerkmale unterschiedlich stark in die Persönlichkeitsrechte der Zielpersonen eingreifen, sind möglicherweise eine gesetzliche Abgrenzung des Leistungsumfangs einer Online-Durchsuchung oder ein Richtervorbehalt sinnvoll.
- Nicht leicht ist die vom BMI vorgenommene Abgrenzung von „Quellen-Telekommunikationsüberwachung“ und Online-Durchsuchung im praktischen Betrieb, wenn über einen (Software-) „Key-Logger“ alle Eingaben, also auch die (unverschlüsselten) Inhalte von Kommunikationsverbindungen, mitgeschnitten werden.
- Online-Durchsuchungen müssen technisch auf das Zielsystem abgestimmt werden. Nach Auskunft des BMI ist lediglich eine einmalige Verwendung vorgesehen [BMI1_07]. Aber selbst bei Wiederverwendung von Teilen der Durchsuchungssoftware bleibt die technische Vorbereitung der Online-Durchsuchung sehr aufwändig.
- Will man sicherstellen, dass die Durchsuchungssoftware auf keinem anderen als dem gewünschten Zielsystem installiert wird, gibt es keine Alternative zur manuellen Installation (physischer Zugang zum System). Alle anderen Methoden sind zudem sehr zeitaufwändig, technisch komplex und teuer.
- Die Durchführung von Online-Durchsuchungen kann mit gängiger Sicherheitstechnik vergleichsweise leicht aufgedeckt oder wirksam verhindert werden und ist daher nur erfolgreich, wenn das Zielsystem mit Sicherheitsschwächen (Sicherheitslücken in der Software, Konfigurationsfehler, Fehlen wichtiger Sicherheitssoftware) betrieben wird. Das ist im Rahmen der Voranalyse feststellbar.
- Der Beweiswert von mit Online-Durchsuchungen gewonnenen Erkenntnissen ist deutlich schwächer als bei herkömmlichen forensischen Untersuchungen, da Quelle, Urheberschaft und Durchsuchungsablauf nicht bezeugt werden können. Auch kann nicht belegbar nachgewiesen werden, dass z. B. ein belastendes Dokument nicht zuvor gezielt auf dem Zielsystem platziert wurde.
- Das allgemeine Sicherheitsniveau und die Bedrohungslage informationstechnischer Systeme wird durch Online-Durchsuchungen nicht beeinträchtigt oder verändert, sofern keine Hintertüren in Software eingebaut (nicht geplant) und eine zielgenaue Installation der Durchsuchungssoftware ausschließlich auf dem designierten Zielsystem erfolgt.
- Die Verwendung von „Less Than Zero Day Exploits“ (unveröffentlichte Schwachstellen) und deren Erwerb durch Strafverfolgungsbehörden könnte eine erhebliche Erhöhung der allgemeinen Bedrohungslage zur Folge haben, falls die behördliche Nachfrage dazu motivieren würde, auf die (bisher übliche) Veröffentlichung und Weitergabe entdeckter Schwachstellen an die betroffenen Hersteller zu Gunsten eines Verkaufs zu verzichten.

Referenzen

[BMI1_07] Bundesministerium des Inneren: *Fragenkatalog der SPD-Bundestagsfraktion*, AG Kultur und Medien, AG Neue Medien. 22.08.2007 http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf

[BMI2_07] Bundesministerium des Inneren: *Fragenkatalog des Bundesministeriums der Justiz*. 22.08.2007 http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf

[Buer_07] Buermeyer, Ulf: *Die „Online-Durchsuchung“. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme*. HRRS, April 2007, S. 154-166. http://www.hrr-strafrecht.de/hrr/archive/07-04/index.php?sz=8

[HaPf_07] Hansen, Markus; Pfitzmann, Andreas: *Online-Durchsuchung. Technische Grundlagen von Online-Durchsuchung und –Beschlagnahme*. DRiZ, August 2007, S. 225-228. http://www.heymanns.com/servlet/PB/menu/1226897/index.html

[Pohl_07] Pohl, Hartmut: *Zur Technik der heimlichen Online-Durchsuchung*. DuD, 9/2007, S. 684-688.