DER BEWEISWERT VON MITTELS REMOTE FORENSIC SOFTWARE GESAMMELTEN DATEN

Michael Sonntag

Michael Sonntag Assoz.-Prof., Johannes Kepler University Linz, Institute of Networks and Security
Altenbergerstr. 69, 4040 Linz, AT
michael.sonntag@ins.jku.at; https://www.ins.jku.at/

Schlagworte: ***Beweiswert, Remote Forensik Software, Bundestrojaner***

Abstract: *Bei besonders schweren Straftaten soll es in Zukunft möglich sein, verschlüsselte Kommunikation zu überwachen, indem beteiligte Endgeräte kompromittiert werden; entweder aus der Ferne oder mittels physischem Zugriff. Dies ist als polizeiliche Maßnahme gedacht, weshalb dem Beweiswert damit erhobener Daten besondere Wichtigkeit zukommt – um sie später in Gerichtsverfahren verwenden zu können. Die Zulässigkeit als Beweismittel an sich ist kein Problem, doch der Beweiswert auf diese Art gesammelter Daten ist fraglich. Dieser Beitrag versucht an Hand konkreter Kriterien herauszuarbeiten, wie dieser Wert im Vergleich zu einer konventionellen Sicherstellung näher bestimmt werden kann. Daraus lassen sich dann auch Schlüsse ziehen, inwieweit eine solche Maßnahme geeignet und verhältnismäßig ist.*

1. Einleitung

Bis vor kurzem wurde über die Verfassungsmäßigkeit[1] des sogenannten «Bundestrojaners» (Remote Forensic Software, RFS; ein oft verwendeter aber irreführender Name, da dies mit einer forensischen Untersuchung wenig gemein hat – wie hier untersucht wird) gestritten. Doch welchen Beweiswert hätten damit erhobene Daten überhaupt gehabt? Denn dass dadurch erlangte Beweise nicht prinzipiell unzulässig sind, steht fest[2]. Hierbei handelt es sich um Maßnahmen der Strafverfolgung, nicht nachrichtendienstlicher Aufklärung, sodass dies wesentlich ist. Dieser Beitrag stellt das Problem aus technischer Sicht der Antragsteller dar, insb da nicht auszuschließen ist, dass ähnliche Vorschriften in Zukunft wieder eingeführt werden sollen.[3]

In immer umfangreicherem Ausmaß eingesetzte Verschlüsselung bedeutet, dass mit passivem Abhören von Nachrichten (E-Mails, Netzwerkverkehr, VoIP, Chat-Anwendungen etc) nur nicht-auswertbare Inhaltsdaten[4] erlangt werden können. Aufgrund guter Implementierungen ist es inzwischen oft unmöglich, die Verbindung unerkannt aufzubrechen und den Inhalt mittels man-in-the-middle Angriffs zu überwachen. Eine Möglichkeit zur Problemumgehung ist daher die Überwachung der Kommunikation, bzw. Zugriff auf darin übertragene sowie potentiell rein lokale Dateien[5], indem heimlich zusätzliche Software auf den Endgeräten installiert wird. Damit kann auf die Kommunikation zugegriffen werden, bevor sie verschlüsselt wird (bzw. nach der – bei Dateien – Entschlüsselung). Der Einsatz derartiger Remote Forensic Software wird in den vor dem VfGH bekämpften Paragraphen erlaubt.

---

1 VfGH, G 72-74/2019: § 134 Z 3a und § 135a der Strafprozeßordnung idF BGBl. I 27/2018 (https://www.ris.bka.gv.at/eli/bgbl/I/2018/27) wurden wegen Verstoßes gegen Art. 8 EMRK bzw. gegen Art. 9 StGG iVm dem Gesetz vom 27. October 1862, zum Schutze des Hausrechtes, RGBl. 88/1862, mit dem Erkenntnis vom 11.12.2019 als verfassungswidrig aufgehoben.

2 Kirchbacher in *Fuchs*/*Ratz*, WK StPO § 246 (Stand 1.8.2009), RZ 103: Mangelnder Beweiswert ist kein Beweisverbot. Die Zuverlässigkeit von Beweismitteln ist durch das Gericht zu prüfen.

3 Der Autor war technische Auskunftsperson der Antragsteller bei der mündlichen Verhandlung vor dem VfGH.

4 Pretz, Online-Durchsuchung und Quellen-TKÜ, Feilaw 2/2016, 133.

5 In der derzeitigen Fassung des Gesetzes nicht enthalten; wird aber von RFS üblicherweise unterstützt, technisch trivial und deutlich einfacher als die Überwachung ausschließlich von Kommunikationsvorgängen, insb falls zusätzlich beschränkt auf bestimmte Kommunikationspartner.

2. Der Wert mittels RFS erlangter Beweise

Unabhängig davon, wie der Systemzugriff erreicht wurde, ist der Wert dadurch erlangter Beweise u.U. zweifelhaft[6]. Hintergrund ist, dass es bei Ausnützung einer Sicherheitslücke oder physikalischem Zugriff immer möglich ist, dass auch Dritte hierzu in der Lage waren – oder die Polizei einfach einen zweiten Zugriff durchführte.[7]

Darüber hinaus ist es eine typische Funktionalität derartiger Software, weitere Programme nachinstallieren zu können. Dies ist z.B. notwendig, falls ein zu überwachendes Programm aktualisiert wurde (etwa mittels Updates), oder wenn weitere Daten (= zusätzliches Kommunikationsprogramm) ausgeleitet werden sollen. Die Funktion eines solchen Paketes kann aber auch darin bestehen, beliebige Dateien auf das überwachte System aufzuspielen – oder gleich bei der Installation (heimlich) abzulegen. Auf diese Weise können daher beliebige Daten erzeugt bzw. existierende verändert werden. Selbst ohne zusätzliche Installation neuer Software/Module ist es möglich, bereits vorhandene Software zu solchen Zwecken einzusetzen[8] (oder mit einer in diesen enthaltenen Sicherheitslücke hierfür zu missbrauchen!). Einzige Abhilfemaßnahme dagagen wäre eine extreme Beschneidung der Möglichkeiten der Software – sodass diese aber nur mehr geringen Nutzen besäße. Dies alleine reduziert den Wert etwaiger Beweise stark.

Als Gegenmaßnahme wird angeführt, dass eine genaue Protokollierung jeden Zugriffs erfolgen soll, um Derartiges auszuschließen. Dies stößt auf das Problem, dass einerseits nicht unbedingt genau bekannt ist, was in einem Installationspaket enthalten ist, bzw. welche Funktion(en) dieses Modul erfüllt. So erlaubt es evtl. einen Zugriff auf das zu untersuchende System auch über andere Kommunikationskanäle, welche nicht protokolliert werden (z.B. direkt über das zu überwachende Kommunikationsprogramm, welches zur gezielten Überwachung ohnehin verändert werden muss). Gleiches gilt identisch für die Überwachungssoftware selbst.

Dies könnte nur durch die Offenlegung des Quellcodes (der Software inkl aller Module wie auch aller Updates) überprüft werden. Nur dann lässt sich eine derartige Funktionalität nachweisbar ausschließen. Die in der mündlichen Verhandlung vor dem VfGH dargstellte Methode, bei der Software-Prüfung eine «Blase» rund um diese zu erstellen und damit jede Verbindung nach innen bzw. außen festzustellen, ist hingegen nicht geeignet. Damit kann z.B. nicht entdeckt werden, wenn neben den dokumentierten Funktionen A, B und C (welche keine Manipulationen oder zusätzlichen Datenabfluss erlauben) noch eine weitere dies unterstützende unbekannte Funktion J enthalten ist. Mangels Kenntnis ihrer Existenz ist ihre Auslösung – und damit Entdeckung bei der Prüfung – unmöglich. Auch ein «Durchprobieren aller Funktionen» kann trivial (z.B. durch ausschließliche Beantwortung von mit einem geheimen Schlüssel signierter Befehle) verhindert werden. Eine Quellcode-Überprüfung ist jedoch sehr Zeit- und Kostenintensiv – und müsste für jedes Update erneut durchgeführt werden. Dies ist insb deswegen zusätzlich problematisch, da eine (u.U. absichtliche) Sicherheitslücke darin auch dazu genützt werden könnte, Beweise zu platzieren[9]. Und es dürfte praktisch ausgeschlossen sein, nachzuweisen, dass diese Lücke nicht durch Dritte (oder die Behörden) entdeckt oder ausgenützt wurde. Ein weiteres Problem ist, dass selbst bei Hinterlegung des Quellcodes bei Gericht[10] (bei kommerzieller Software unwahrscheinlich, dass der Hersteller darauf eingeht, da dies sein wichtigstes Geschäftsgeheimnis ist) damit nicht sichergestellt ist, ob tatsächlich der diesem Quellcode entsprechende ausführbare Code bei der Ermitt-

6 Dies geht über die «normalen» Probleme des Beweiswertes digitaler Daten (siehe dazu Deutsch, Die Beweiskraft elektronischer Dokument, JurPC Web-Dok. 188/2000) hinaus.

7 Bzw. Verdächtige dies zumindest jederzeit behaupten können und es kaum von der Polizei wiederlegt werden kann.

8 Z.B. durch Überschreiben mit einer Logdatei (Konfiguration des Dateinamens durch die RFS), welche später bei Entfernung der RFS automatisch gelöscht wird.

9 Arbeitskreis «Technische und organisatorische Datenschutzfragen» der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Technische Aspekte der Online-Durchsuchung, 21.9.2007, https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Materialien/Technische_Aspekte_der_Onlinedurchsuchung.pdf (abgerufen am 12. Dezember 2019).

10 Siehe dazu den Fragenkatalog der SPD-Bundestagsfraktion und der Antwort des Innenministers (22.8.2007), https://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (abgerufen am 12. Dezember 2019).

lung eingesetzt wurde. Denn dieser soll am Ende vom untersuchten System rückstandslos entfernt werden, sodass eine Nachprüfung unmöglich ist.

Die Fähigkeit einer RFS, sich vor dem Benutzer zu verbergen, ist zusätzlich problematisch: Wird diese oder ähnliche Software von verschiedenen Stellen/Staaten gegen ein System eingesetzt (durchaus wahrscheinlich, da sie nur bei sehr schweren Straftaten zum Einsatz kommen und von kommerziellen Anbietern erworben werden soll), so verstecken sich beide Instanzen (vom selben oder anderen Hersteller) auch voreinander. Es ist damit nicht feststellbar, ob auch Andere Systemzugriff besaßen und potentiell Änderungen durchführen konnten. Die Möglichkeit hierfür wurde durch den eigenen (technisch erfolgreichen) Einsatz bereits bewiesen.

Ein weiteres Problem ist, dass der Trojaner sich innerhalb des zu überwachenden Systems befindet. Er kann dieses daher naturgemäß nicht von außen untersuchen. Wenn es sich hierbei allerdings um ein virtuelles System handelt (oder die Software entdeckt wird, und der physische Rechner in ein virtuelles System umgewandelt wird – was bei ausgeschaltetem System erfolgt und daher ebenfalls unerkennbar ist), kann trivial die Kommunikation überwacht und verändert werden. Weiters können dem System beliebige Kommunikation bzw. beliebiger Inhalt vorgespiegelt werden. Genau dies findet z.B. bei sogenannten «Honeypots» statt: Bekannt unsichere Systeme zum Anlocken von Angreifern, deren Vorgehensweise dann beobachtet wird. Auf die gleiche Art können Forensik-Tools ausgespäht (und dann ggf. selbst verwendet) werden. Dies betrifft z.B. organisierte Kriminialität oder Terroristen, die durchauch über IT-Fähigkeiten und finanzielle Ressourcen verfügen und davon ausgehen (müssen), dass sie u.U. das Ziel derartiger Maßnahmen sind.[11]

Eine Voraussetzung der RFS ist, dass sie nach dem Zugriff rückstandslos entfernt werden kann oder zumindest funktionsunfähig[12] ist. Ist es auf dem Gerät später nicht mehr möglich, das (frühere) Vorhandensein solcher Software nachzuweisen, so wird hierdurch gleichzeitig der Beweis erbracht, dass eine Manipulation durch Dritte möglich war, aber es keine Chance gibt, diese später nachzuweisen. So kann z.B. immer agrumentiert werden, dass die RFS (von derselben oder einer anderen Person/Behörde/…) installiert und die Beweise eingebracht wurden, worauf eine Deinstallation erfolgte. Unmittelbar anschließend kann dann eine (offizielle: überwachte, protokollierte etc) Suche nach diesen gerade eben erzeugten Beweisen erfolgen.

3. Kriterien für den Beweiswert

Der Wert von Beweisen[13] kann nicht nur allgemein diskutiert, sondern auch nach verschiedenen Kriterien «gemessen» werden; dies ergibt zwar kein mathematisches Ergebnis, aber ein deutlich besseres und detaillierteres Bild.

3.1. Sichere Aufbewahrung bis zur Sicherstellung

Bis zum Zeitpunkt der Sicherstellung werden die Daten im System des Verdächtigen gespeichert (und nicht z.B. auf einem separaten und besonders gesicherten Logserver). Da es sich meist um Endnutzer handelt, sind diese Systeme normalerweise nicht besonders abgesichert. Im Hinblick auf die Zielgruppe einer solche Maßnahme ist jedoch davon auszugehen, dass u.U. bessere Sicherheitsmaßnahmen als allgemein verbreitet vorhanden sind. Es ist dennoch jederzeit durch die Person selbst, wie aber auch durch Dritte (z.B. über Schadsoftware) möglich, die Daten zu verändern.

---

[11] Ziercke, Pro Online Durchsuchung, Springer Informatik Spektrum 2008, 63.

[12] Dies ist technisch nur möglich, indem essentielle Teile überschrieben werden, also eine Teillöschung. Dies ist jedoch besonders «gefährlich», da nach Bekanntwerden der Maßnahme diese Reste analysiert werden können, um spätere Untersuchungen sofort erkennen zu können.

[13] § 272 Abs 1, 3 ZPO: Die Beurteilung von Beweisen erfolgt nach freier Überzeugung des Gerichts, die Umstände und Erwägungen hierfür sind jedoch zu begründen.

Da bei Fernzugriff durch die RFS nicht nur vermutlicherweise sondern nachgewiesenermaßen das System tatsächlich unsicher ist, muss der Beweiswert in dieser Kategorie dennoch reduziert werden.

3.2. Sichere Aufbewahrung nach der Sicherstellung

Da die Sicherstellung der Daten aus der Ferne erfolgt, kann diese unmittelbar auf sichere Systeme bei der Polizei erfolgen, wobei auch Hashwerte, Signaturen oder Zeitstempel miteinbezogen werden können. Vom technischen Gesichtspunkt ist dies daher ein sehr guter Beweiswert. Dass im Gegensatz zu einer normalen Durchsuchung und Sicherstellung hier keine unabhängigen dritten Personen als Zeugen eingesetzt werden dürften, reduziert diesen Wert allerdings[14]. Denn es ist später bzw. für keinen Außenstehenden überprüfbar, ob die vorgesehen Prozeduren tatsächlich befolgt wurden (und z.B. die Daten unverändert gespeichert und gehasht wurden – oder erst nach einer «manuellen Nachbearbeitung»). Dies gilt umso mehr, als die entsprechende Software zugekauft werden soll, es sich also nicht um ein einziges geschlossenes System handelt, sondern bestenfalls um individuelle Anpassungen an lokale Schnittstellen.

3.3. Elektronische Signaturen

Elektronische Signaturen sind hier doppelt relevant: Signaturen durch die Polizei nach der Übermittlung der Daten bringen keinen besseren oder schlechteren Beweiswert als bei einer normalen Durchsuchung – hier ergibt sich keine Änderung.

Ein Signatur der Daten vor der Übermittlung auf dem zu untersuchenden System ist hingegen nicht sinnvoll: Da der hierfür verwendete Schlüssel zwangsweise auf dem untersuchten System vorhanden sein muss, kann dieser auch dort ausgelesen und zur Signierung falscher Daten verwendet werden[15]. Dies ist einerseits der Polizei möglich, andererseits in gleicher Weise dem Betroffenen (der damit falsche Daten signiert zurückschicken kann), ebenso wie als (nachträgliche) Beweis-Erschütterung (Signierung harmloser Daten und Behauptung, dies wären die tatsächlich übermittelten Daten gewesen).

Signaturen der von der Durchsuchung Betroffenen werden jedoch durch ein solches Vorgehen entwertet: Nach der eIDAS-VO Art 26 lit c[16] muss eine fortgeschrittene Signatur (welche Voraussetzung für eine qualifizierte Signatur ist) unter Verwendung elektronischer Signaturerstellungsdaten erstellt werden, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann. Durch den Einsatz der RFS ist dies jedoch gerade nicht mehr gegeben: Während des Signierungsvorgangs besaß ein Dritter volle Kontrolle über das Gerät, auf welchem der Vorgang stattfand. Es war diesem daher möglich die Daten zu verändern, oder (je nach eingesetzter Hardware), sogar die Auslösedaten (PIN) mitzuschneiden. Es werden daher erstellte Signaturen mit Bekanntwerden der Durchsuchungsmaßnahme nachträglich ungültig – worauf sich sowohl der Betroffene wie auch Dritte berufen könnten. Sie können zwar weiterhin als Beweismittel dienen (Art 25 Abs 1 eIDAS-VO), doch sind sie kein Äquivalent zur handschriftlichen Unterschrift mehr, was bei Rechtsakten welche dieses voraussetzen ein besonderes Problem darstellt.

[14] Logging durch den Verkäufer der Software stellt zwar einen Dritten dar, doch ist dieser, da Auftragnehmer und an weiteren Gechäften interessiert, keinesfalls als «unabhängig» zu betrachten.

[15] Rehak, Angezapft. Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, Diplomarbeit, Berlin, Humboldt-Universität zu Berlin 2012, 65.

[16] Verordnung (EU) Nr. 910/2014 des Europäischen Parlamentes und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, Abl L 257/73 vom 28.8.2014.

3.4. Zeitliche Einordnung/Zeitstempel

Zeitstempel erlauben es, die Existenz bestimmter Daten vor einem Zeitpunkt nachzuweisen. Durch Verdächtige erzeugte Zeitstempel dürften in der Praxis selten vorkommen. Falls doch, ist zu berücksichtigen, dass sowohl vor ihrer Erzeugung (Stempelung modifizierter Daten) Manipulationen durch die RFS möglich sind, ebenso wie danach (Ungültigkeit des Stempels). Auch ein späteres Ersetzen der gestempelten Daten (und des Zeitstempels) ist möglich, wenn zum gleichen Zeitpunkt andere Daten beim Ersteller der Zeitstempel eingereicht wurden. Im Gegensatz zu einer späteren Durchsuchung ist dieser Angriff nur bei Live-Überwachung realistisch – Daten werden vorbereitet und beim Erkennen eines Stempelvorgangs gleichzeitig eingereicht. Dies entwertet den Zeitstempel, da nun realistische Manipulationsmöglichkeiten existieren.

Zeitstempel bei der Sicherstellung sind möglich, erhöhen jedoch nicht den Beweiswert, da Nachvollziehbarkeit fehlt, egal in welcher Stufe des Datensammlungsprozesses sie erfolgten. Da die RFS vom untersuchten Gerät zu entfernen ist, können dort ebenso wenig Protokolle zur Bestätigung des Zeitpunktes vorhanden sein.

3.5. Hashwerte

Für Hashwert gilt Ähnliches wie für Zeitstempel: Hashwerte überwachter Kommunikation sind zwar möglich, doch dienen diese im Allgemeinen dazu nachzuweisen, dass die untersuchten/vorgelegten Daten identisch zum «Original» sind. Dieses ist jedoch das zu untersuchende System, welches schon durch die Entfernung der RFS (abgesehen von sonstigen Aktionen) verändert wurde. Darüber hinaus wird bei Kommunikation diese oft überhaupt nicht gespeichert, z.B. bei VoIP-Telefonaten oder Skype-Videokonferenzen. Vergleichsdaten zur Überprüfung des Hashwertes existieren daher nicht. Lediglich die bei der Polizei befindlichen live aus der Kommunikation abgegriffenen Daten können mit Hashwerten versehen werden – dies bringt jedoch mangels Kontrolle des Vorgangs keinen Gewinn an Beweiswert sondern nur, dass die gesicherten Daten seit dem Zeitpunkt der Speicherung unverändert blieben. Hier ist jedoch anzufügen, dass auch bei normaler Beschlagnahme die Erstellung von Hashwerten aus Zeitgründen oft erst später erfolgt, sodass ebenso wenig eine Verschlechterung vorliegt.

3.6. Darlegung der Datenerzeugung

Die Beschreibung der Datenerzeugung beruht auf Grund bzw. Ort, Art und Weise wie die Daten ursprünglich produziert werden. Hier ist der Beweiswert sogar etwas höher, da die RFS speziell auf Kommunikation ausgerichtet werden soll. Es ist daher exakt bekannt, wie und unter welchen Umständen (Software, Version, Konfiguration…) die Daten erzeugt wurden: Ein Skype-Gespräch, ein WhatsApp-Chat etc. Da der Verdächtige nichts von der Datensammlung bemerken soll, könnte man annehmen, dass der Inhalt besonders verlässlich ist. Da die Software jedoch nicht feststellen kann, ob dies tatsächlich der Fall ist oder sie entdeckt wurde[17] (und daher mit falschen Informationen versorgt wird), ist der Beweiswert in diesem Aspekt sogar schechter zu bewerten: Die offene Beschlagnahme eines Gerätes erlaubt nur äußert selten Manipulationsmöglichkeiten, etwa wenn das Bevorstehen der Maßnahme der Zielperson ausnahmsweise schon vor ihrer Durchführung bekannt ist. Hier steht hingegen für die Entdeckung bzw. Manipulation u.U. sehr viel Zeit zur Verfügung.

Eine Vollständigkeit der Daten kann durch die RFS nicht garantiert werden, da nur spezifische Programme überwacht werden sollen[18]. Wird daher eine andere Kommunikationssoftware verwendet, später installiert etc., so werden nicht alle Daten aufgezeichnet, obwohl es so aussieht, als ob dies der Fall wäre. Dies ist daher eine weitere, wenn auch geringfügige, Minderung des Beweiswertes.

---

[17] Pohl, Zur Technik der heimlichen Online-Durchsuchung, DuD 31 (2007), 9.

[18] Um festzustellen, ob weitere/neue (und damit potentiell zu überwachende) SW existiert, muss das gesamte System durchsucht werden – Eine Funktionalität zur vollständigen Durchsuchung der Datenträger nach bestimmten Dateien/Inhalten ist daher notwendiger Teil einer RFS.

3.7. Chain of Custody

Die Chain of Custody (CoC) sichert Identität und Integrität von Beweisen. Da bei Fernzugriff keine physischen Beweise erhoben werden, ist als Äquivalent der Identität die exakte Identifikation des Zielsystems zu sehen. Erfolgt die Installation der RFS durch physischen Zugriff, so ist dies gegeben, doch bei einer Installation aus der Ferne ist es sehr schwierig, das Zielgerät im Vorhinein zu identifizieren. Im Nachhinein, nach erfolgter Infiltration, ist jedoch eine Feststellung, ob man im Gerät der richtigen Person ist, im Allgemeinen möglich. Bezüglich der Integrität ist auf obige Ausführungen zu verweisen: Nachdem die Daten bei der Polizei gespeichert wurden, ist ihre Integrität gut gesichert. Die CoC intendiert jedoch eine ununterbrochene Kette von der Erhebung bis zum Gerichtssaal. Und zwischen der eigentlichen Erhebung auf dem System des Verdächtigen, das unter der Kontrolle der RFS steht, bis zum Beginn der Dokumentation besteht ein erheblicher Unterschied. So ist es z.B. nicht immer möglich, die Daten sofort auszuleiten, sondern sie werden lokal zwischengespeichert. Dies reduziert den Beweiswert weiter. Da von einer gesicherten Übertragung zur Polizei auszugehen ist, ist diese Reduktion allerdings gering, da insb. keine Dritten Personen Zugriff darauf besitzen[19].

3.8. Dokumentation des Sicherstellungsvorgangs

Die Dokumentation des Sicherstellungsvorgangs ist potentiell gut, da jede Verwendung der Software protokolliert werden kann. Es ist jedoch möglich, eine Software auch ohne (bzw. mit anschließend gelöschter) Protokollierung einzusetzen. Der Beweiswert protokollierter Vorgänge ist daher gut, gibt jedoch keinen Hinweis, ob weitere Vorgänge erfolgten. Sofern die Software keinen unmittelbaren Zugriff über andere Programme als sich selbst ermöglicht (im Sinne einer zusätzlichen Hintertür), ist eine automatisierte Dokumentation jeder Aktion möglich, was gegenüber einer klassischen Durchsuchung (mit u.U. weniger strikter und vollständiger Dokumentation) sogar einen erhöhten Beweiswert erzeugen kann.

3.9. Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen nach der Übertragung zur Polizei dürften exakt denen entsprechen, die bei sonstigen sichergestellten Daten Anwendung finden – der Beweiswert bleibt daher in dieser Hinsicht gleich. Auch anderweitig wird gelegentlich eine Übertragung von Beweisdaten über öffentliche Netzwerke stattfinden; bei entsprechenden Sicherheitsmaßnahmen (von denen auszugehen ist: Verschlüsselung, Identifizierung der Gegenstelle etc.), ergibt sich ebenso wenig eine Änderung.

Problematisch ist jedoch das zu untersuchende Gerät selbst. Bei diesem kann gerade nicht von einem sicheren Zustand ausgegangen werden. Im Gegenteil wurde durch die Installation des RFS unmittelbar bewiesen, dass die Sicherheitsvorkehrungen dort nicht ausreichen. Die u.U. erforderliche Deaktivierung von Schutzprogrammen (um selbst Zugriff zu erlangen bzw. nicht entdeckt zu werden) reduziert die Sicherheit des Systems weiter[20]. Es ist daher von einem geringeren Beweiswert auszugehen, insb da nicht sichergestellt werden kann, dass die gleiche Sicherheitslücke nicht auch an andere Personen/Institutionen verkauft oder von Dritten unabhängig entdeckt und ausgenützt wurde. Aus früheren Einsätzen der RFS können ebenfalls Informationen zur Entdeckung gewonnen werden (z.B. kann eine Entfernung der RFS von Backups nicht realistisch – jedenfalls nicht ohne Mitwirkung von Betroffenen – erfolgen), was insb. bei organisierter

[19] Zwischengespeichert Daten können etwa verschlüsselt und signiert werden (siehe jedoch oben zum Problem des notwendigerweise lokal vorhandenen Schlüssels), sodass Manipulationen durch den Verdächtigen, Mitbenutzer des Gerätes etc. zumindest oft erkannt werden können.

[20] Dies ist ein weiteres Problem: Durch den Einsatz dürfen dritte Systeme nicht geschädigt werden. Durch die Deaktivierung entsteht ein Einfallstor für Viren, welche sich von dort aus z.B. innerhalb eines Unternehmens oder in der Familie der Betroffenen weiterverbreiten und damit weiteren Schaden anrichten können.

Kriminalität relevant ist. Hierzu ist auf die Informationspflicht[21] hinzuweisen, sodass nach Bekanntwerden der durchgeführten Maßnahme vorhandene Backups gezielt durchsucht und analysiert werden können. Dies führt darüber hinaus schon aus Selbstschutz der Betroffenen zu einer Weiterleitung an Schutzprogramm-Hersteller und damit der Inklusion in diesen, sodass eine signifikante (Zeit- und Kostenintensive) Änderung für jeden Einsatz erforderlich ist.

3.10. Redundanz bzw. unterstützende Daten

Da eine RFS nur dann eingesetzt werden soll, wenn andere Maßnahmen keinen Erfolg zeigen oder versprechen, dürften keine sonstigen Daten zur Unterstützung vorhanden sein. Daher ergibt sich hier keine Veränderung des Beweiswertes. Redundanz fehlt ebenfalls, da z.B. Chat-Protokolle aus der selben Quelle stammen wie die Chatnachrichten selbst, sodass hier lediglich eine Kopie derselben Daten existiert. Die einzige Chance für einen höheren Wert bestünde darin, sowohl Quelle als auch Ziel der Kommunikation zu überwachen, da Daten dann tatsächlich zwei Mal unabhängig voneinander gesammelt würden. Da der Einsatz bei verschlüsselter Kommunikation erfolgen soll, erzeugt auch eine direkte Überwachung des Datenverkehrs, da verschlüsselt, keine unterstützenden Daten (längenerhaltende Manipulationen dürften meist trivial sein).

Lediglich bei gespeicherten Dateien können diese evtl. später bei einer physischen Sicherstellung erneut gefunden werden. Sollten sie in der Zwischenzeit verändert worden sein (z.B. weitere Nachrichten im Protokoll, Bearbeitung von Dokumenten etc.), sind selbst Signaturen der gesicherten Daten (sofern vorhanden) nutzlos. Der Beweiswert ist daher hier u.U. in Einzelfällen (Datei-Übermittlung, lokale Speicherung, keine Veränderung seitdem…) leicht erhöht: Anstatt bloß eine Datei zu finden die empfangen wurde, ist zusätzlich ihr Übermittlungsvorgang aufgezeichnet und dokumentiert.

3.11. Wiederholungsmöglichkeit

Eine Wiederholung der Beweiserhebung ist nicht möglich, da die RFS die Kommunikation während sie stattfindet überwachen soll. Von der Kommunikationssoftware erzeugte Protokolle sind lediglich Kopien (siehe oben), und erlauben daher ebenso keine Wiederholung. Dies ist ähnlich zu der Untersuchung von Live-Systemen (z.B. Server-Einbruch), sodass der Beweiswert hier gleich wie bei diesen anzusetzen ist: Leicht verringert gegenüber einer Offline-Sicherstellung. Hinsichtlich der Auswertung sind die Wiederholungsmöglichkeiten unverändert, daher auch der Beweiswert.

3.12. Determinismus

Ob eine Analysemethode von Daten deterministisch ist, dh immer das selbe Ergebnis liefert, betrifft nicht die Aufnahme der Grunddaten, sodass sich in diesem Aspekt keine Änderung des Beweiswertes ergibt – lediglich der Vorgang der Datensammlung erfolgt durch RSF anders als sonst, nicht ihre Auswertung.

3.13. Anzahl der Auswertungsschritte

Gleiches wie für den Determinismus gilt großteils für die Anzahl der Auswertungsschritte – es gibt keinen Unterschied bei der Auswertung und daher keine Veränderung des Beweiswertes. Hier ist jedoch zu beachten, dass hier u.U. bereits bei der Sammlung selbst ein Teil der Auswertung erfolgt: Es werden nicht unbedingt alle Daten gesammelt, sondern nur die Kommunikation mit bestimmten Gegenstellen (sofern technisch möglich), nur relevante Teile (oder umgekehrt: inhaltlich besonders geschützte Teile werden ausgeblendet) etc. Diese

[21] Siehe § 138 Abs 5 StPO der Novelle.

Schritte würden zwar auch sonst erfolgen, aber im Gegensatz zu «normal» sichergestellten Daten ist eine spätere Überprüfung und ggf Korrektur dann nicht mehr möglich. Insb die Vollständigkeit der Daten und die Korrektheit ihres Kontextes sind daher in solchen Fällen vom Beweiswert her reduziert.

3.14. Alternative Darstellungsmöglichkeiten

Mehrere Möglichkeiten der Darstellung machen es wahrscheinlicher, dass die Interpretation der Rohdaten korrekt ist. Dies ist jedoch wiederum eine reine Frage bei der Auswertung bzw. Präsentation der Daten, welche sich durch RFS nicht ändert.

3.15. Angreifer-Charakterisierung

Da die RFS gerade bei schwersten Straftaten und organisierter Kriminalität eingesetzt werden soll, ist davon auszugehen, dass es sich hierbei um «Profis» handelt, bzw. Arbeitsteilung existiert. Es ist daher weiters anzunehmen, dass Verdächtige zumindest leicht bessere Sicherheitsmaßnahmen einsetzen als Durschnittsnutzer. Dies kann den Einsatz von RFS kaum verhindern (noch unbekannte Sicherheitslücken oder physikalischer Zugriff), erhöht jedoch die Chance ihrer Entdeckung. Dies vermindert zwar nicht den Wert von Beweisen, bringt jedoch eine höhere Wahrscheinlichkeit für eine Entdeckung mit sich. Dass der Einsatz im Nachhinein jedenfalls bekannt wird, ermöglicht die Argumentation, dass man dies schon viel früher erkannt hätte und daher die Kommunikation gefälscht wurde («zum Spaß» etc.) – was zwar unwahrscheinlich erscheinen wird, aber kaum technisch widerlegt werden kann.

Zusammen mit der Anforderung, die Software nach Abschluss der Untersuchung rückstandsfrei zu entfernen, führt dies dazu, dass der Zeitraum einer Überwachung durch Betroffene exakt festgestellt werden kann, und es ihnen daher gleichfalls möglich ist, Spuren einer tatsächlichen Entdeckung bzw. Manipulierung der RFS zu beseitigen. Es ist dann kaum noch nachweisbar, dass eine inhaltlich falsche Datenerhebung stattfand.

Beide Probleme (falsch Behauptung der Entdeckung sowie Verstecken tatsächlicher Entdeckung) führen dazu, dass der Beweiswert dadurch erlangter Daten zu reduzieren ist – da Manipulationen möglich sind und ihre Abwesenheit nicht nachweisbar ist.

4. Zusammenfassung

Wie die umfangreiche Verbreitung von Schadsoftware beweist, ist ein Zugriff auf Computersysteme aus der Ferne, um daraus Daten zu gewinnen, technisch möglich. Wie aber die Praxis gleichfalls zeigt, ist es nur sehr eingeschränkt möglich, diesen Zugriff auch nur für eine gewisse Zeit geheimzuhalten. Wie (gute) Verschlüsselungstrojaner nachweisen, können Daten auf dem System beliebig verändert werden, ohne dass Betroffene dies verhindern oder nachvollziehen können. Umgekehrt beweisen Honeypots, dass eine glaubwürdige Vorspiegelung falscher Daten gegenüber Angreifern ebenso möglich ist.

All dies bedeutet, dass bis auf kleine Aspekte der Wert von Beweisen, welche durch RFS gwonnen wurde, stark reduziert ist[22]. Mit anderen Worten, durch eine sehr gefährliche und teure Maßnahme werden höchst

[22] Siehe dazu selbst Ziercke, Pro Online Durchsuchung, Springer Informatik Spektrum 2008, 63 relativierend: «Damit möchte ich verdeutlichen, dass die unmittelbare Beweiserhebung durch die Online-Durchsuchung nur einen Aspekt dieser Maßnahme darstellt. Der Beweiswert einzelner Erkenntnisse ist stets im Kontext weiterer kriminaltaktischer bzw. strafprozessualer Maßnahmen zu beurteilen.» sowie Fox, Stellungnahme zur «Online-Durchsuchung», 29.9.2007, https://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf (abgerufen am 12. Dezember 2019) «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.».

zweifelhafte Ergebnisse gewonnen, die vielfältigen Angriffen auf ihre Glaubwürdigkeit ausgesetzt sind. Dies entspricht deutlich mehr der Beschreibung von Geheimdiensten als dem Character von Strafverfolgungsbehörden. Zusätzlich ist anzuführen, dass je professioneller die Verdächtigen sind, desto geringer der Beweiswert ist. Gerade die angepeilte Zielgruppe hat daher die besten Chancen, die Sammlung der Beweise zu verhindern, für sich selbst auszunutzen, oder ihren Wert später zu erfolgreich anzuzweifeln[23].

Es ist daher äußerst zweifelhaft, ob Eignung und Angemessenheit einer solchen Maßnahme basierend auf den dadurch möglichen Ergebnissen gegeben ist.

[23] So schon Buermeyer, Die «Online-Durchsuchung», HRRS 4/2007, S. 165.