Artikel für Deutsche Richterzeitung, August 2007, Seite 225-228

Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme

Markus Hansen, ULD, Kiel
Prof. Dr. Andreas Pfitzmann, Fak. Informatik, TU Dresden

1 Einführung

In der politischen Diskussion wird gefordert, polizeilichen Ermittlern den Online-Zugriff auf PCs Verdächtiger zu gestatten, um diese Systeme zu durchsuchen und ggf. darauf befindliche Daten als Beweismaterial zu beschlagnahmen. Informationen von offizieller Seite, wie dies technisch realisiert werden soll, sucht man vergeblich.

2 Technisch-organisatorische Anforderungen an die Beweiserhebung in Computersystemen

Sollen derzeit Daten als Beweise in einem Verfahren dienen, so werden in der Regel ganze Computer, zumindest aber deren Festplatten, sichergestellt und von sachverständigen Kriminaltechnikern einer forensischen Analyse unterzogen. Um sicherzustellen, dass versteckte Dateien nicht übersehen werden, und um eine Veränderung des Untersuchungsgegenstandes auszuschließen, ist die jeweilige Festplatte schreibgeschützt auszulesen und eine Kopie in Form eines identischen Abbildes (1:1-Kopie, „Image“) anzufertigen. Über diese Image-Kopie wird eine kryptographische Prüfsumme („Hash“) berechnet, die zu dokumentieren ist. Erst danach werden anhand der Image-Kopie – niemals anhand des Originaldatenträgers – inhaltliche Untersuchungen, die ebenfalls zu dokumentieren sind, vorgenommen.[1] Nur so ist später im Verfahren die Echtheit der gefundenen Dateien belegbar, so dass sie als Beweismittel geeignet sind.[2] Die Nichtveränderung der sichergestellten Originaldatenträger ist wesentliche Grundlage für die Revisionsfähigkeit und damit die Verlässlichkeit der Untersuchungsmethode.

Ob ein revisionsfestes Beweiserhebungsverfahren, das einer kritischen Prüfung standhält, auch bei der Durchsuchung von Systemen und der Beschlagnahme von Dateien mittels Online-Zugriff per Internet möglich ist, wird im Folgenden diskutiert.

Da die Untersuchungen nicht an sichergestellten Systemen durchgeführt werden können, ist eine Software-Komponente auf dem zu untersuchenden System zu installieren (sofern nicht bereits durch Unachtsamkeit oder vorauseilenden Gehorsam seines Herstellers vorhanden[3]), die Ermittlern den Online-Zugriff per Internet ermöglicht. Eine derartige Software wird Trojanisches Pferd (ugs. Trojaner) genannt. Ein Trojanisches Pferd kann über einen (verdeckten) Eingabekanal Handlungsanweisungen empfangen, über einen (verdeckten) Ausgabekanal Daten senden, auf dem System diese Daten gewinnen wie auch manipulieren. Bereits die Installation des Trojanischen Pferdes, die Infiltration des Rechners, ist eine Modifikation des Zielsystems, das zudem durch den Verbrauch von Ressourcen durch das Trojanische Pferd in seiner Funktionalität beeinträchtigt wird.[4] Nach der Phase der Infiltration folgen die Phasen von Datengewinnung und Kommunikation (Datenübermittlung) sowie der Beendigung der Maßnahme. Über alle Phasen hinweg wäre ein standardisiertes Verfahren zu konzipieren und technisch abzubilden, um ein einheitliches und nachvollziehbares Vorgehen auf Seiten der Ermittler sicherzustellen, da eine Revisionsfähigkeit auf dem infiltrierten System nicht zu gewährleisten ist.

---

1 Alexander Geschonneck: Computer-Forensik, 2., aktualisierte Auflage, dpunkt.verlag, Heidelberg, 2006, S. 84.

2 Vergl. Fall am AG Lübeck; Peter Mühlhauber: Wie verläßlich sind digitale Beweise?, in Telepolis, Verlag Heinz Heise, 2007, http://www.heise.de/tp/r4/artikel/24/24638/1.html.

3 Dann wäre sogar eine Hardware-Komponente möglich.

4 Vergl. Andreas Pfitzmann: Sicherheit in Rechnernetzen: Mehrseitige Sicherheit in verteilten und durch verteilte Systeme, Dresden, 2000, S. 9 ff, online: http://dud.inf.tu-dresden.de/~pfitza/DSuKrypt.pdf.

2.1 Infiltration

Infiltration bezeichnet den Vorgang, das Zielsystem zu kompromittieren, indem ein Trojanisches Pferd, d.h. die Softwarekomponente, die Ermittlern den Zugriff per Internet erlaubt, installiert wird. Bei der Infiltration ist zwischen Methoden zu unterscheiden, die eine (unbewusste) Unterstützung durch den Nutzer des Zielsystems erfordern, sowie solchen, die ohne (unbewusste) Hilfe des Nutzers auskommen.

Zu den bekannten Methoden der Rechnerinfiltration, die Nutzerverhalten einkalkulieren, zählt das Zusenden verheißungsvoller Dateien per E-Mail. Der Nutzer muss diese bewusst öffnen bzw. starten, um die Infiltrationsroutine zu aktivieren, wozu ihn der Begleittext verleiten soll. Neben Hinweisen auf pornographische Inhalte finden bei der Verbreitung von Trojanischen Pferden auf diesem Weg zunehmend auch Bedrohungsszenarien[5] Verwendung. Ferner können Nutzer beim Besuch von Web-Seiten verleitet werden, Dateien zu öffnen oder auszuführen, die Trojanische Pferde enthalten. Beim gezielten „Herumliegenlassen“ von präparierten Datenträgern wie CDs oder USB-Sticks können dem Opfer ebenfalls Installationsdateien zugespielt werden. Will der Nutzer die Datenträger auf seinem System lesen, kann es leicht passieren, dass allein durch das Einlegen einer CD ein Trojanisches Pferd unbemerkt installiert wird.[6] Insbesondere die letzte Methode impliziert allerdings die Möglichkeit, dass ein anderes System als das der eigentlichen Zielperson, für das keine Durchsuchungserlaubnis besteht, mit dem Trojanischen Pferd infiltriert wird. Neben den daraus resultierenden Problemen für die Betroffenen entsteht bei mehreren Systemen, die mit einem Trojanischen Pferd infiltriert wurden, zudem die Notwendigkeit, die von den einzelnen Systemen an die Ermittler übersandten Daten zu filtern. Finden die Ermittler heraus, dass sie auf dem falschen System ermitteln, wurde bereits in die Privatsphäre Unbeteiligter eingedrungen.

Methoden, die ohne Hilfe des Nutzers auskommen, sind z.B. das gezielte Ausnutzen von Sicherheitslücken in Programmen (z.B. Web-Browser oder E-Mail-Client) oder Betriebssystemen. Sofern es sich um bereits allgemein bekannte Lücken handelt, besteht in der Regel nur ein kleines Zeitfenster von wenigen Stunden bis Tagen, bevor gute Hersteller reagieren und entsprechende Updates bereitstellen. Bei Sicherheitslücken, die nur den Angreifern bekannt sind, beträgt dieses Zeitfenster jüngeren Untersuchungen zufolge durchschnittlich ein Jahr.[7] Informationen über derartige „unentdeckte“ Lücken können gegen Bezahlung erworben und von Angreifern ausgenutzt werden. Eine andere Frage ist, ob und ggf. wie schnell bereitgestellte Updates genutzt werden. Insbesondere, wer Überwachung fürchtet, wird diesbezüglich schnell sein.

Weiter können, wie bereits erwähnt, Hintertüren für Ermittler „ab Werk“ in Software-Produkte eingebunden werden, um eine Online-Durchsuchung zu ermöglichen.[8] Hierfür wäre allerdings ein Zugriff auf den Produktionsprozess erforderlich. Die Maßnahme lässt sich zudem nur dann auf den Rechner eines bestimmten Nutzers begrenzen, wenn das Softwareprodukt eine sichere Authentifizierung der jeweiligen Nutzer durchführt. Das Trojanische Pferd ist jedoch auf allen Systemen vorhanden und zur Nutzung bereit, auf denen die kompromittierte Software installiert wurde.

Liegt der Produktionsprozess der Software nicht im Zugriff, kann auch bereits fertig produzierte Software, die über Internet-Server verteilt wird, um die Funktionalität des Trojanischen Pferdes erweitert werden. Hierzu muss in den entsprechenden Server eingedrungen und dort die Software manipuliert werden. Ist dies nicht möglich, besteht ferner die Möglichkeit, die Programmdaten während des Downloads zu verändern, indem auf die Internetanbindung des Verdächtigen zugegriffen wird. In kleinem Rahmen kann dies beim jeweiligen Zugangs-Provider geschehen.

---

[5] Z.B. wurde ein Trojanisches Pferd u.a. verteilt, in dem Mails mit gefälschtem Absender des LKA Rheinland-Pfalz versandt wurden. Im Rahmen einer Online-Durchsuchung sei belastendes Material auf dem System gefunden worden, Details fänden sich im Anhang (der das Trojanische Pferd installierte).

[6] Vergl. Markus Hansen: DRM-Desaster: Das Sony BMG-Rootkit, in DuD 2/2006, Vieweg Verlag, Wiesbaden, S. 95-97, online: https://www.datenschutzzentrum.de/drm/DuD(2)2006-Hansen.pdf.

[7] Heise Newsticker: Durchschnittliche Haltbarkeit von Zero-Day-Lücken liegt bei einem Jahr, Meldung vom 10.07.2007, http://www.heise.de/newsticker/meldung/92457.

[8] Der Chaos Computer Club hatte passend zum 1. April die (Falsch-)Meldung verbreitet, in der Software zur Erstellung der elektronischen Steuererklärung ELSTER sei ein „Bundestrojaner“ gefunden worden.

Denkbar ist auch, an einem größeren Verbindungsknoten, z.B. DECIX in Frankfurt, in die Internet-Infrastruktur einzugreifen und Downloads zu manipulieren. Auch hier wären Unbeteiligte in großem Maße ebenfalls von der Maßnahme betroffen.

Die einzige Möglichkeit der Infiltration, die sowohl ohne Hilfe des Nutzers des Zielsystems auskommt als auch ausschließt, dass Rechner Unbeteiligter ebenfalls in den Fokus der Maßnahme geraten, ist der physische Zugriff auf den Zielrechner, z.B. durch heimliches Eindringen in die Räumlichkeiten, in denen dieser untergebracht ist.

Mindestens in den Fällen, in denen kein physischer Zugriff auf den Rechner erfolgt, ist eine erfolgreiche Infiltration ein Beleg dafür, dass der Zielrechner nicht nur vom Eigner, sondern auch von Dritten (d.h. auch von Nicht-Ermittlern) kontrolliert werden könnte, die auf dem Rechner z.B. ohne Wissen des Nutzers Daten speichern[9] oder E-Mails versenden können.

Da Ermittler auf die gleichen Methoden der Infiltration angewiesen sind, die auch Virenautoren und Betreiber von Bot-Netzen[10] verwenden (wie auch fremde Geheimdienste und die organisierte Kriminalität), müssen sie ebenfalls mit aktiven Gegenmaßnahmen in Form von Anti-Viren-Software, Firewalls etc. rechnen – gerade auch von gesetzestreuen Bürgern.[11]

2.2 Datengewinnung und Kommunikation

Nach der erfolgreichen Infiltration folgt die eigentliche Online-Durchsuchung. Mit Hilfe des Trojanischen Pferdes greifen Ermittler per Internet auf den Rechner zu und können die auf dem System vorhandenen Daten auslesen oder verändern. Da das Zielsystem weder vom Nutzer noch von den Ermittlern allein kontrolliert wird, kann zwangsläufig eine Echtheitsbestätigung der übertragenen Daten nicht erfolgen. Eine solche Bestätigung, z.B. in Form einer digitalen Signatur einer kryptographischen Prüfsumme, kann grundsätzlich nur verlässlich vorgenommen werden, wenn eine exklusive Kontrolle über ein System vorliegt. Bei einem infiltrierten System kann zudem nicht ausgeschlossen werden, dass neben Nutzer und Ermittlern auch Dritte (z.B. über ein weiteres Trojanisches Pferd) ggf. sogar gleichzeitig partiell Kontrolle ausüben und zu Täuschungszwecken auf den Rechner zugreifen.

Auf infiltrierten Systemen können darüber hinaus Tastatureingaben, z.B. Passworte, abgefangen und übertragen werden. Ist während des Abfangens eine Internetverbindung nicht gegeben, können die Daten zwischengespeichert werden. Dies ist nicht nur eine weitere Veränderung des Untersuchungsgegenstandes, sondern zudem eine Gefährdung des Nutzers des Zielsystems, da insbesondere bei unverschlüsselter Speicherung ein unbefugter Zugriff auf das nun gespeicherte Passwort nicht ausgeschlossen werden kann. Auch ist es mittels eines Trojanischen Pferdes möglich, Ende-zu-Ende-Kommunikation zwischen Rechnern (Textnachrichten, Internet-Telefonie, Videokonferenzen etc.) abzufangen sowie auf ggf. an den Rechner angeschlossene Mikrofone und Kameras zuzugreifen und damit die Umgebung des Rechners zu überwachen.

Eine Entdeckung des Trojanischen Pferdes durch die Zielperson ist nicht auszuschließen. Laut Presseberichten ist dies bei den ohne Rechtsgrundlage durchgeführten Online-Durchsuchungen auch geschehen, da z.B. die Menge der übertragenen Daten auffiel.[12] Eine Entdeckung kann zur Folge haben, dass der Nutzer das Trojanische Pferd entfernt und die Online-Durchsuchung so vorzeitig beendet. Er kann es sich aber auch zu Nutze machen und ausgewähltes unverdächtiges Datenmaterial übermitteln, um die Ermittler zu täuschen. Möglich ist sogar, die Datenübertragung des Trojanischen Pferdes zu nutzen, um den Rechner der Ermittler zu infiltrieren, auszuspionieren und zu manipulieren. Um dem vorzubeugen, sollte eine Online-Durchsuchung stets so verdeckt

---

9 Zdnet Security: Guerilla Storage – Symantec warnt vor unbekannten Daten, Meldung vom 06.06.2007, http://www.zdnet.de/security/news/0,39029460,39155056,00.htm.

10 Ein Bot-Netz ist eine Menge von Rechnern, die mit einem Trojanischen Pferd infiltriert wurden und gemeinsam unter Kontrolle eines Angreifers stehen. Bot-Netze werden z.B. zum Versand von Spam-Mails oder für verteilte Angriffe auf Internet-Dienste genutzt und vermietet.

11 Vergl. das Angebot „BSI für Bürger“ des Bundesamts für Sicherheit in der Informationstechnik unter http://www.bsi-fuer-buerger.de/.

12 Vergl. Deutschlandfunk: Brecheisen für den Bundestrojaner, Online-Durchsuchung kämpft mit technischen Problemen, Manfred Kloiber im Gespräch mit Peter Welchering, Beitrag vom 28.04.2007, http://www.dradio.de/dlf/sendungen/computer/620126/.

wie möglich durchgeführt und Datenübertragungen nur in geringem Umfang vorgenommen werden. Technisch ausschließen lässt sich eine Aufdeckung nicht.

2.3 Beendigung der Maßnahme

Da eine richterliche Anordnung zur Online-Durchsuchung eines eindeutig bestimmten Systems sicherlich eine zeitliche Befristung beinhaltet, ist eine Funktion zur Beendigung der Maßnahme vorzusehen, die das Trojanische Pferd vom Zielrechner verlässlich wieder entfernt. Insbesondere in Fällen, in denen der Verdacht gegen die Zielperson entkräftet wird, muss das Trojanische Pferd jederzeit deaktivierbar sein. Dabei ist darauf zu achten, dass nicht durch z.B. das Wiedereinspielen eines Backups, das der Nutzer während der Durchführung der Maßnahme angefertigt hat, Sicherheitslücken resultieren oder eine weitere, nicht mehr durch die Durchsuchungserlaubnis abgedeckte Datenübertragung.

3 Fazit

Technisch lässt sich nicht ausschließen, dass ein Trojanisches „Ermittlungspferd“ Fehler enthält und die Sicherheit untersuchter Systeme dadurch nachhaltig beeinträchtigt wird. Mit Ausnahme des physischen Zugriffs beinhalten alle Infiltrationsverfahren die Gefahr, dass (auch) Systeme Unbeteiligter von der Maßnahme getroffen werden. Wird das Trojanische Pferd entdeckt, was ebenfalls nicht auszuschließen ist, so kann es benutzt werden, um einen gezielten Gegenangriff zu starten, um im Gegenzug Rechner der Ermittler zu infiltrieren oder mit falschen Daten zu versorgen.

Daten, die per Online-Durchsuchung gewonnen wurden, sind nicht annähernd so verlässlich, wie auf herkömmlichem Wege erlangte Daten, die von einem sichergestellten Rechner stammen. Da die Online-Durchsuchung mit einer Veränderung des zu untersuchenden Rechners beginnt, sofern dieser nicht bereits von sich aus eine Möglichkeit zum heimlichen Fernzugriff bietet[13], und während des Betriebs ein exklusiver Zugriff durch die Ermittler technisch nicht sicherzustellen ist, ist vielmehr regelmäßig die Echtheit der übertragenen Daten anzuzweifeln. Denn eine Online-Durchsuchung widerspricht allen Anforderungen, die aus technisch fundierten Gründen an einen sachverständigen Gutachter im Rahmen einer forensischen Analyse gestellt werden.

[13] Vergl. Abschnitt 2.1, Fn.8. Denkbar wäre eine generelle Hintertür im Betriebssystem.