

Einleitung¹

Computer haben schon längst unseren Alltag durchdrungen. Ob Bürofachleute, Privatpersonen, Anwälte, Juristen oder Polizisten, fast jeder benutzt einen PC. So verwundert es nicht, dass es auch immer mehr Computerkriminalität gibt.

Computerkriminelle sind nicht nur unter EDV-Spezialisten zu finden. Auch der durchschnittliche Benutzer kann seinen Computer für kriminelle Zwecke missbrauchen. Statistiken zeigen, dass für bekannte Formen von Kriminalität wie Betrug, Fälschungen usw. vielfach Computer eingesetzt werden.

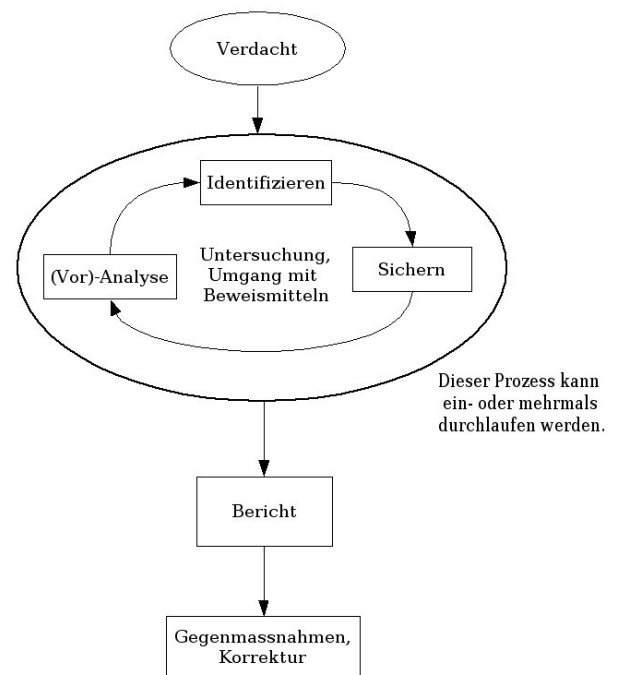
Die Ermittlung bei Computerkriminalität erfordert spezielle Techniken und Kenntnisse. Computerbasierte Beweismittel sind besonders empfindlich auf unbefugte Änderungen; sei es durch Absicht, durch Unwissenheit, oder durch Fehlverhalten. Aus diesem Grund müssen nachweisliche und überprüfbare Vorkehrungen getroffen werden, um die digitalen Beweismittel zu schützen. Dies ist eine der Hauptaufgaben der Computerforensik, wobei die Untersuchungen unter Berücksichtigung der gerichtlichen Verwendbarkeit der Beweismaterialien durchgeführt werden. Dabei kombinieren die Ermittler die strengen Massstäbe der Beweisbehandlung mit den neusten Techniken der Computerwissenschaften.

Forensische Ermittlung

Wie angetönt sind die digitalen Beweismittel von Natur aus sehr verletzlich. Leicht können diese Beweismittel durch absichtliche oder unbefugte Handlungen verändert werden, wobei dies im Nachhinein sehr schwierig nachzuvollziehen ist. Aus diesem Grund werden digitale Beweismittel möglichst nach forensischen Standards untersucht: nachvollziehbar, nachweisbar und überprüfbar. Um eine Beweiskette aufzubauen müssen Computerforensiker in der Lage sein zu beweisen, dass ihre Kopiervorgänge und ihre Analysen die ursprünglichen Daten nicht verändert haben. Daten die als Beweismittel identifiziert wurden, werden daher vor der eigentlichen

Untersuchung mit einem digitalen Fingerabdruck versehen. So kann später überprüft werden, ob die Daten verändert wurden.² Ein Kopiervorgang wird üblicherweise auch durch Logdateien protokolliert. Die Beweiskette wird mit einer Dokumentation aufgebaut, worin jeder Schritt der Beweismittelanalyse beschrieben wird. Logbucheinträge beschreiben die zeitlichen Vorgänge, Formulare beschreiben die Beschlagnahmung und Identifikation der Hardware usw.

Untersucht werden Daten, egal auf welchen Trägern sie gespeichert sind. Typischerweise können dies PC-Festplatten, Disketten, CD-ROMs, aber auch ganze Storage Systeme oder mobile Geräte wie Telefone und PDAs sein. Die einzelnen Schritte einer Ermittlung folgen fast immer dem gleichen Muster:



Ablauf einer forensischen Untersuchung

Erster Schritt: Identifikation möglicher Beweismittel

Aufgrund eines Verdachts wird eine Untersuchung eingeleitet. Da es während einer forensischen Untersuchung möglich ist, dass spätere Phasen der Ermittlung neue Beweismittel aufdecken, sollten die ersten Schritte dieser Phase möglichst umfangreich sein und genau protokolliert werden. Beispielsweise sollten bei einer Hausdurchsuchung möglichst alle Datenträger mitgenommen werden, auch wenn sich einige nachher als nicht relevant erweisen.

Zweiter Schritt: Sammeln und Sichern von Beweisen

Beweismittel müssen nach forensischen Massstäben kopiert werden. Computerforensiker machen möglichst exakte Kopien der Beweismittel. Dabei wird Datenbit um Datenbit kopiert („Bitstream“). In der Fachsprache heisst diese Art zu kopieren auch „Datenspiegelung“ oder „Klonen“. Mit einem digitalen Fingerabdruck wird anschliessend geprüft, ob die Daten der Quelle mit denjenigen der Kopie übereinstimmen. Stimmen die Fingerabdrücke überein ist Gewähr, dass der Forensiker eine identische Kopie des Originals in seinen Händen hält, welche die Basis für weitere Untersuchungen darstellt.

Wie geht der Kopiervorgang vor sich? Vorzugsweise „spiegelt“ ein Forensiker einen abgeschalteten Computer, weil dieses Verfahren „reiner“ und übersichtlicher ist. Das Erheben der Beweise bei noch laufenden Rechnern ist komplizierter und birgt viele Fallstricke für die forensische Beweissammlung. Ein gehackter Computer sollte jedoch nicht ordnungsgemäss heruntergefahren werden, da ein Hacker Löschprogramme hinterlassen haben könnte, die dann aktiv werden. Das Untersuchungsobjekt könnte auch ein Firmenserver sein und ist möglicherweise zu wichtig um heruntergefahren zu werden. Ausserdem kann das Beweismittel auch im Arbeitsspeicher liegen und würde daher nicht auf dem Datenträger aufgefunden werden. So muss der Ermittler eine Priorisierung durchführen und die Beweismittel in der Reihenfolge ihrer

Gefährdung (auch Flüchtigkeit) kopieren. Allenfalls muss danach der Stromstecker des Computers herausgezogen werden um mögliche Folgeschäden oder das Löschen von Beweisen zu verhindern. Das Kopieren von Arbeitsspeicher ist aus forensischer Sicht besonders heikel, da der Kopiervorgang auch Spuren im Arbeitsspeicher hinterlässt (das Kopiervorgang ist selber ein Prozess, der Speicher benutzt). Somit ist es unvermeidbar, dass Beweismittel verändert werden während man sie sichert. Ein digitaler Fingerabdruck kann beweisen, dass die Daten wenigstens seit dem Sammeln nicht geändert wurden. Ein solcher Vergleich mit dem Zustand der Quelle vor und nach dem Kopieren wird aber hier fehlschlagen.

Dritter Schritt: Voranalyse und Analyse

Die Kopien der ursprünglichen Datenträger werden im Anschluss auf Spuren untersucht und ausgewertet. Eine Voranalyse überprüft die Vollständigkeit des Beweismaterials. Öfters kommen auch andere Spuren zum Vorschein, welche das Vorgehen der Computerforensiker beeinflussen. Bei dem erwähnten Beispiel der Hausdurchsuchung werden alle Datenträger beschlagnahmt, aber vielleicht zuerst nur die PC-Festplatte analysiert. Wenn dort Hinweise auf CD-ROMs oder Disketten gefunden werden, werden die betreffenden Datenträger natürlich dupliziert und analysiert. Die ersten drei Schritte einer Untersuchung (vgl. oben) können sich deswegen wiederholen bis eine ausreichende oder vollständige Beweislage vorhanden ist. Weil es sich hier um ein heuristisches Verfahren handelt, ist die Abgrenzung zwischen der Voranalyse und der eigentlichen Analyse oft fließend.

Spuren werden nicht absichtlich hinterlassen, aber auch nicht immer absichtlich verwischt. Computerforensiker benutzen spezialisierte Hardware und Programme, um diese Spuren zu finden und zu analysieren. So kann der Forensiker Beweise in gelöschten Dateien, Datenfragmenten (teilweise überschriebene Dateien), unbenutzter Speicherplatz (z.B. „slack space“) oder in Meta-Daten von Anwendungen (z.B. Word, Excel) auffinden.

Das Ziel einer forensischen Untersuchung ist es, Klarheit über die Aktivitäten eines möglichen Täters zu erhalten.

Vierter Schritt: Dokumentieren

Die gefundenen Beweise werden unter Umständen während eines Gerichtsverfahrens diskutiert und ausgewertet. Die Beschreibung der Resultate, die Dokumentation des Vorgehens für den Beweismittelschutz sowie der Analyse, können eine Ermittlung glaubwürdig oder unglaubwürdig erscheinen lassen. Zusätzlich ist es die Pflicht eines Computerforensikers, die komplexen technischen Vorgänge für Laien verständlich und nachvollziehbar zu beschreiben.

Die Computerforensik ist ein relativ neues Gebiet, worin eine Kombination von forensischen Verfahren mit technischem IT-Wissen und der traditionellen Spürnase eines Ermittlers verlangt wird. Zudem wächst die Komplexität der Computerkriminalität, wegen der schnellen internationalen Verbreitung des Wissens über kriminelle Methoden und Verfahren, ständig. Deshalb muss der Ermittler immer am neusten Stand der Entwicklungen dranbleiben und sich weiterbilden.

Hilfe bei Compass Security

Compass Security verfügt über umfangreiche Erfahrungen auf dem Gebiet der Netzwerksicherheit sowie dem Hacking, forscht aktiv nach neuen Angriffs- und Testmethoden und programmiert eigene Werkzeuge für professionelle Security Assessments. Dank dem spezifischen Know-how konnte Kunden schon oft Unterstützung bei Ermittlungen geboten werden.

Compass Security beschäftigt sich seit April 2004 professionell mit dem Thema Computer Forensik. Dank kompetenten Fachpersonen und der notwendigen Hard- und Software können Gutachten für Justiz und Wirtschaft erstellt werden.

Mehr Informationen über Compass Security und unsere Dienstleistungen finden Sie unter: <http://www.csnc.ch>

Über den Autor

Mark Furner ist promovierter Historiker und Computerforensiker. Nach einer Ausbildung als Programmierer und Analytiker auf IBM Grossrechnern ist er seit 2000 in der Computerforensik tätig und hat Untersuchungen für die Justiz und Wirtschaft durchgeführt. Seit Juni 2004 arbeitet er bei Compass Security und ist Mitautor der Inhalte des dreitägigen ISACA Evidence Lab-Seminars. Der Kurs vermittelt das Wissen rund um die Beweismittelführung und -Verwertung. Eine Broschüre über das ISACA Evidence Lab finden Sie unter folgender URL:

www.csnc.ch/static/services/training/esl.html

Problem Computerkriminalität

Die folgenden Beispiele geben eine kleine Übersicht über den Umfang des Problems Computerkriminalität:

- 1988 berichtete das amerikanische Computer Emergency Response Team CERT/CC über 6 Fälle von Computerkriminalität. Im Jahre 2002 waren es bereits 82'094 und 2003 137'529 Fälle.³
- Die CSI/FBI Computer Crime and Security Survey bezifferte den Gesamtverlust durch Computerkriminalität für 2003 auf rund USD 202 Mio. Angriffe fanden gemäss der Studie hauptsächlich über das Internet statt.⁴
- In Deutschland verfasst das Bundeskriminalamt (BKA) jährlich die polizeiliche Kriminalstatistik (PKS), welche aber nur abgeschlossene Verfahren beschreibt. Dies sind nur die Fälle, die der Polizei gemeldet wurden. Spezialisten rechnen zudem mit einer massiven Grauzone von nicht deklarierten Delikten. Von 3'067 Fällen in 1987 stieg die Zahl auf 79'283 in 2001. Die PKS von 2002 zählt 40'346 Fälle von betrügerischer Ausnutzung des Lastschriftverfahrens (Debitkarten ohne PIN) nicht zur Computerkriminalität. Fügt man diese wieder hinzu, kommt man auf 97'834 Fälle, was einen Zuwachs von 23% gegenüber dem Vorjahr bedeutet.⁵
- Die PwC Global Economic Crime Survey 2003 gibt Informationen über die Lage in der Schweiz. Computerkriminalität war mit 15% weltweit die drittgrösste Form von Wirtschaftskriminalität (nach Veruntreuung mit 60% und Produktdiebstahl mit 19%). In der Schweiz nimmt die Computerkriminalität mit 20% den zweiten Platz ein (nach Veruntreuung mit 60%). Firmen erwarten die grössten zukünftigen Gefahren bei der Veruntreuung (35%) gefolgt von Computerkriminalität (31%).⁶

Referenzen

¹ Dieser Artikel basiert auf dem Artikel "First Forensic Forum Schweiz (F3-CH) Computerforensik und Computerkriminalität" publiziert in „Recht“, 05/2004, S. 210-212, <http://www.recht.ch/>

² Digitale Fingerabdrücke sind numerische Werte, die durch einen Algorithmus anhand des Inhalts einer Datei erstellt werden. Diese Werte sind gross genug, um eindeutig zu sein. Nach der Erstellung eines digitalen Fingerabdrucks kann man nachweisen, ob die Daten geändert wurden, weil der Algorithmus dann einen anderen Fingerabdruck-Wert berechnet, oder denselben Wert ermittelt. Dieser Wert, auch Prüfsumme genannt, wird so Bestandteil einer digitalen Beweiskette und bürgt für Integrität der Daten.

³ http://www.cert.org/stats/cert_stats.html

⁴ Der Bericht kann über <http://www.gocsi.com/press/20030528.jhtml> bezogen werden.

⁵ http://www.bka.de/pks/zeitreihen_2002/pdf/t01.pdf
und
<http://www.bka.de/pks/pks2002/index2.html>

⁶ Bezugsquelle für den Bericht:
http://www.pwcglobal.com/ch/ger/insol/publ/cfr/crime_survey.html

20. Oktober 2004, V1.0