

# Elektronische Beweisführung oder wie begegnet man Cyberkriminalität

**Der Begriff elektronische Beweisführung, im englischen auch Computer Forensics genannt, tauchte im Jahr 1991 erstmals auf und beschreibt den Einsatz von auf Computern basierenden Untersuchungs- und Analysetechniken um potenzielle elektronische Beweise für Gerichte zu liefern.**

Artur P. Schmidt

Von James Borek stammt eine Kurzdefinition aus dem Jahr 2001, die besagt, «dass Computer Forensics das Gleiche ist wie das Sichern eines Tatortes oder das Durchführen der Autopsie an einem Opfer.» Damit die Sammlung und Analyse von Daten Beweiskraft vor Gericht haben, müssen diese zugänglich, authentisch, vollständig, vertrauenswürdig und glaubhaft sein. Hierbei gilt es, eine Vielzahl von Problemen zu bewältigen wie die Änderungsrate von Daten, die mangelnde Sichtbarkeit von Daten, die Heterogenität von Daten und deren Unschärfe. Letztere lässt sich derart beschreiben, dass ähnlich der Unschärferelation der Quantenphysik, entweder eindeutig der Ort der Daten bekannt ist oder deren Inhalt, aber oftmals beides gleichzeitig nicht eindeutig vorliegt. Damit kann eine notwendige Strafverfolgung von Cyberkriminellen bereits sehr schnell im Keime erstickt werden. Wenn Sie aufgefordert werden: «Geben Sie uns Ihre E-Mail-Adresse, Anschrift und Kreditkartennummer» sollten beim Kunden rote Alarmlichter angehen. Heute durchläuft die Bestellung eines Konsumenten das Internet wie ein nicht verschlossener Brief. Es ist kein Problem für computerbewanderte Nutzer der ein paar einfache Kniffe beherrscht, die persönlichen Daten von Kunden abzulesen. Deshalb wird es zukünftig immer wichtiger, dass Daten ausreichend verschlüsselt sind, umso einen wirksamen Schutz herbeizuführen.

Themen wie Tele-Shopping, Online-Banking, Kryptographie und Steganographie müssen Hand-in-Hand weiterentwickelt werden, damit es gelingt der Manipulierung von Daten Einhalt zu gebieten. Die Experten des Kommissariats für Ermittlungen IT der Bundeskriminalpolizei sehen die grössten Bedrohungspotenziale hierbei insbesondere durch Cyberstalking (Belästigung von Personen im Internet), WLAN sowie mobile Kommunikationsmittel der vierten Generation.

## Vom Datenklau zum virtuellen Bankraub

Die kommerzielle Nutzung des Netzes birgt eine neue Qualität von Rechtsproblemen, insbesondere im Rahmen der elektronischen Beweisführung. Die hierbei auftretenden Konfliktfelder reichen von vertragsrechtlichen Fragen, dem Persönlichkeits- und Datenschutz, Urheberrechtsstreitigkeiten bis hin zum elektronischen Zahlungsverkehr. Allen gemeinsam hierbei ist, dass ohne ausreichende Beweisführung das Durchsetzen von Rechtsansprüchen sehr schwierig ist. Da die Gerichtsbarkeit an der Staatsgrenze endet, das World Wide Web jedoch ein globales Medium ist, ergeben sich zwangsläufig quasi-rechtsfreie Räume, die Cyberkriminelle immer mehr für sich ausnützen. Die mit fremden Kartennummern bestückten Netzverbrecher können sehr leicht jede Menge Produkte bestellen und ihre elektronischen Spuren verwischen. Der Karteninhaber hat dann die Zeche zu bezahlen. Zwar zeigen sich Kreditkartenfirmen noch kulant wenn dem

Karteninhaber keine grobe Fahrlässigkeit im Umgang mit seinem Plastikgeld nachzuweisen ist, jedoch dürfte sich dieser Trend umkehren, wenn die Häufigkeit der Angriffe weiter deutlich zunimmt. Der in Hamburg ansässige «Chaos Computer Club» hat deutschen Banken schon öfters vorgeführt, wie leicht ein sogenannter «Kontoklau» durchgeführt werden kann. Die trojanischen Cyberpferde traben mittlerweile immer häufiger durch die Festplatten der User und spähen diese nach Passwörtern aus. Mit dem schlichten Betrachten einer Webpage oder mit einem Computerspiel fangen sich die User immer häufiger unliebsame Gäste ein und der ahnungslose User verliert die Kontrolle über seinen Rechner. Trotzdem neigen deutsche Banken, insbesondere die Deutsche Bank, immer wieder zur Verharmlosung. Immer öfter verschicken Betrüger E-Mails, bei denen Kunden aufgefordert werden, Zugangsdaten zu ihren Bankkonten einzugeben. Das sogenannte Phishing, ein Kunstwort aus Password und Fishing, könnte ein grosses Problem werden, wie Christian Pauli, Jurist beim Bundesverband der Verbraucherzentralen (VZBV), betont. Die Attacken kommen hierbei überwiegend aus Osteuropa, wie jüngst, als Kunden der Postbank von Massenmails überschwemmt wurden, die auf eine gefälschte Postbank-Webseite mit dem Länderkürzel für Russland führten. In den USA ist in den vergangenen zwölf Monaten nach Schätzung der Marktforschungsfirma Gartner ein Schaden von 2,4 Mrd. USD entstanden. Um solchen Attacken begegnen zu können, hat Deutschlands grösster Internetanbieter T-Online jetzt seine Geschäftsbedingungen geändert. Nunmehr behält sich der Konzern vor, «bestimmte Leistungsfunktionalitäten, insbesondere die E-Mail-Kommunikation» zu sperren, wenn Kunden wissentlich oder unwissentlich zur Verbreitung von Internetschädlingen beitragen. Auch bei den Banken wird ausdrücklich darauf verwiesen, dass Kunden zum sorgfältigen Umgang mit ihren Zugangsdaten verpflichtet sind.

## Spielregeln der Computer Forensics

Bei der elektronischen Beweisführung gilt es bestimmte Spielregeln einzuhalten. Vor allem sollte das Original

so wenig wie möglich benutzt und mit Kopien gearbeitet werden, damit kein Datenverlust auftritt. Dies ist vielleicht die wichtigste Regel der Computer Forensics. Hierbei muss sichergestellt werden, was das Original und was die Kopie ist. Jede Veränderung am Original muss eindeutig erfasst und dokumentiert sein. So kann es beispielsweise beim Booten oder beim Herunterfahren von Maschinen zu unvermeidlichen Veränderungen im Speicher oder bei temporären Files kommen. Hierbei sollten die Sicherstellung von Beweisen mit den Spielregeln der elektronischen Beweisführung übereinstimmen. Wenn das Wissen zum Sichern von Beweisen nicht ausreicht, sollte dieser Vorgang jeweils auf die nächst höhere Wissens Ebene übertragen werden. Zum Fundamentwissen im Umgang mit der elektronischen Beweisführung zählen hierbei Programmier- und Computererfahrung, Kenntnisse über Betriebssysteme und Anwendungsprogramme, stark ausgeprägte analytische Fähigkeiten, Kenntnisse über die grössten Verwundbarkeiten von Computersystemen, ein aktuelles Wissen über die neuesten Bedrohungen, Kenntnisse über die neuesten forensischen Werkzeuge, Wissen über die Anwendung von Kryptographie und Steganographie, sowie ein ausgeprägtes Verständnis über die Regeln der elektronischen Beweisführung und den Umgang mit Beweisen. Diese Punkte zeigen auf, dass der Umgang mit digitalen Beweisen an Betroffene, die Polizei, Strafverteidiger, Staatsanwälte und Richter viel höhere Ansprüche stellt als der Umgang mit konventionellen Beweisen. Nur wer sich den Herausforderungen der elektronischen Beweisführung stellt und seine Daten durch modernste Sicherungsme-

thoden schützt, ist in der Lage eine forensische Untersuchung zu führen und mögliche finanzielle Schäden vorbeugend zu vermeiden. Allerdings ist es sehr schwierig eine integrale Strategie zur Abwehr von Cyberkriminalität durchzuführen, wie die Ermittlungsexperten der Bundeskriminalpolizei einräumen. Für sie ist eine umfassende Abwehrstrategie aufgrund der Diversifizierung zu kostspielig, wenn nicht gar undenkbar. Wichtig ist für sie, dass die Entwicklungen eng verfolgt werden und eine Flexibilität in der Beschaffung und Ausbildung bei neuen Technologien gewahrt bleibt.

## Schlüsselfaktoren der Beweisführung

Die elektronische Beweisführung wird genutzt, um die Untersuchung computerbasierter Vorfälle durchzuführen, sei es durch ein externes Eindringen in einen Computer, interne Attacken oder den Missbrauch der Sicherheitspolitik in Unternehmen durch Mitarbeiter. Die Frage, welche Strategie bei der elektronischen Beweis-

führung eingeschlagen werden soll, wird auch für das Management von Unternehmen von immer grösserer Bedeutung. Wie entscheidet ein Manager, ob in der IT oder nicht, einen Vorfall zu untersuchen? Wird der Vorfall von internem Personal, der Polizei oder von einer auf elektronische Beweisführung spezialisierten Firma durchgeführt? Für Unternehmen gibt es hier vier entscheidende Komponenten:

### **1. Beweisidentifizierung**

Es müssen Beweise erkannt werden. Es muss klar sein, wo und wie diese gespeichert sind. Und es muss bekannt sein, welches Betriebssystem benutzt wird. Durch diese Informationen kann ein Unternehmen eine angemessene Recovery-Methodologie erarbeiten.

### **2. Beweiserhalt**

Hierbei handelt es sich um den Prozess des Erhaltens der Integrität der elektronischen Beweise. Die Daten müssen auf stabile Medien kopiert werden, bei denen eine Manipulierung ausgeschlossen ist. Hierbei müssen alle Veränderungen an den Beweisen dokumentiert werden, z. B. was die Veränderung war und warum diese durchgeführt wurde.

### **3. Beweisanalyse**

Hierbei handelt es sich um den Prozess des Sichtens und der Untersuchung von Daten. Werden Daten hierbei auf redundante Medien gesichert, können diese ohne das Risiko von versehentlichen Änderungen ausgewertet werden.

### **4. Beweispräsentation**

Hierbei handelt es sich um den Prozess des Präsentierens von Beweisen in einer legal akzeptierbaren und verständlichen Form. Werden solche Beweise Geschworenen oder Richtern mit wenig Computererfahrung nicht glaubhaft präsentiert, können alle Anstrengungen der Beweisführung oftmals umsonst sein.

## **Unternehmen müssen sich umstellen**

Wichtig ist auch, dass bei multinational operierenden Firmen, wo z. B. ein Delikt in Tokyo oder New York begangen werden kann, weltweit die gleichen Spielregeln im Umgang mit Beweisen gelten. Für Unternehmen ist es wichtig, dass Daten, die für Beweise herangezogen werden, auch tatsächlich zugänglich sind. Ist dies nicht oder nicht mehr der Fall, kann keine Anklage erfolgen. Des Weiteren müssen die Beweise für die Vorfälle authentisch sein. Lassen sich die Beweise nicht eindeutig bestimmten Vorfällen zuordnen, kann eine Beweiskette sehr schnell durchbrochen werden oder erst gar nicht aufgebaut werden. Gleiches gilt für die Vollständigkeit von Daten. Ist diese nicht gegeben, kann dies ebenso geschehen oder das Vertrauen in die Beweiskraft kann dramatisch schwinden. So reicht es eben heute nicht aus zu zeigen, dass ein Angreifer zum Zeitpunkt eines kriminellen Aktes eingeloggt war, sondern es muss auch aufgezeigt werden wer sonst noch eingeloggt war. Dies wird im englischen Exculpatory Evidence genannt. Hierzu betonen die

Experten des Kommissariats für Ermittlungen IT der Bundeskriminalpolizei, dass die forensischen Beweismittel aus der Informatik längst nicht die einzigen sind welche in einem Strafverfahren verwendet werden können. Sind jedoch keine anderen Beweismittel vorhanden, muss unbedingt sichergestellt werden, dass die elektronischen Daten absolut vertrauens- und glaubwürdig sind. Sonst wird es sehr schwierig, einem Angeklagten die Schuld nachzuweisen. Ohne ein sauberes Management der Beweisführung, kann im Falle des Auftretens von Cyberverbrechen das Recht nicht durchgesetzt werden. Jedes Unternehmen sollte deshalb ein spezielles «Response Team» für Vorfälle haben. Dieses Team sollte schriftliche Prozeduren haben, um auf diese reagieren zu können. Hierzu zählen beispielsweise Aktivitäten wie das Sichern des Tatortes, das Herunterfahren der Computer, die Kennzeichnung der Beweise, die Dokumentierung der Beweise, der Transport der Beweise oder die Dokumentierung der Beweiskette. Eine grosse Hilfe kann hierbei für Unternehmen das Einführen von forensischen Standards sowie die Nutzung von Checklisten sein. Je komplexer die elektronischen Systeme werden, desto wichtiger ist es, die Beweisbarkeit mit einer Art juristischem Cockpit zu lenken, damit kein Glied in der Beweiskette vergessen oder falsch dokumentiert wird. ■

Quelle: [www.wissensnavigator.com](http://www.wissensnavigator.com)