17. EDV-Gerichtstag

Arbeitskreis Forensik

Zeit und Ort: **18.09.2008, 15:00 Uhr im Hörsaal 116**
Referenten: **Wilhelm Uhlenberg, (öbv Sachverständiger)**
Dipl- Ing. Mathias Gärtner, (öbv Sachverständiger)
Moderation: **Dr. Simone Richter**
Protokoll: **Anna Marie Tschirley**

Der Arbeitskreis „Forensik“, bot einen Einblick in die Arbeitsweise sowie die sich stellende Problematik für öffentlich bestellte und vereidigte Sachverständige in der IT-Forensik.

Zunächst erläuterte Herr Uhlenberg, dass sich die IT-Forensik mit der Analyse und Auswertung von Computerdaten, also der digitalen Beweismittelsicherung, befasst. Nach dieser kleinen Einleitung referierte er über das Thema Verschlüsselung und Zugriff auf Daten im Arbeitsspeicher eines Rechners. Hierbei wurden die Schwierigkeiten der Spurensicherung und anschließenden Analyse für die IT-Forensiker aufgezeigt.
Um einen „Datenschatz“ zu heben, bedarf es einer durchdachten Vorgehensweise, welche vielfach durch die Antiforensik inspiriert wird. Das Hauptproblem ist, dass nicht alle Daten beweiszugänglich sind.

Die Aufgabe der Sachverständigen liegt darin, eine möglichst umfangreiche forensische Auswertung von Datenträgern zu liefern. Dabei muss forensisch gesehen mit einer Kopie gearbeitet werden. Eine besondere Herausforderung besteht darin, die zu untersuchenden Daten nicht durch die eigene Arbeit zu zerstören, sondern sie vielmehr zu konservieren und nachvollziehbar zu analysieren. Hierfür existieren zwar Standardprogramme, diese decken die Anforderungen jedoch nur unzureichend ab, so dass hauptsächlich selbsterstellte, auf den Einzelfall angepasste Analyseverfahren angewandt werden. Bei der Analyse werden vier bis sechs wesentliche Bereiche untersucht, so beispielsweise der physikalische Hauptspeicher oder der virtuelle Speicher einzelner Applikationen.

Ein weiteres Anliegen war es, aufzuzeigen, dass oftmals Anwendungen auf Privatrechnern laufen und Daten unverschlüsselt im Cache ablegen, ohne dass die Nutzer davon Kenntnis haben. So lesen und kopieren selbst betriebsinterne Sicherheitsapplikationen ständig Daten. So ist es wichtig, dass nach der Eingabe eines Pins eine Überschreibung der Daten erfolgt, da diese sonst noch aus den Auslagerungsdateien ausgelesen werden könnten. Dabei wissen private Nutzer häufig nicht, wie ihre Daten verwandt werden können. Bewusst kann jedoch beispielsweise eine starke Verschlüsselung eingesetzt werden, um den Zugriff zu erschweren. Werden jedoch verschlüsselte Daten abgerufen, werden sie dechiffriert und dabei in einem internen Puffer gespeichert, den aber der private Nutzer nicht kennt. Folglich bleibt die Klarschrift im internen Puffer des Programms zurück, außer das Programm überschreibt ihn automatisch mit Zufallsdaten. Auch innerhalb von Windows, z.B bei Netzwerken werden Passwörter ausgetauscht. Sobald dies

stattgefunden hat, kommt es für eine Datenüberschreibung darauf an, wie das lebende System benutzt wird.

Zum Auslesen der Daten benötigt der Sachverständige ein Programm. Dadurch wird jedoch das zu analysierende System bereits verändert und die Daten könnten so die Messmittel zerstören. Hauptspeicherinhalte können extern nur durch eine Methode wiedergewonnen werden, ohne eine Veränderung des „Schatzes“ zu verursachen.

Sodann wurde die Frage beantwortet, wie man letztendlich an die Daten gerät.
Dies erfolgt durch unabhängige Hardwarelösungen, Software, Rootkits, Trojaner, Keylogger, VW-Hijacker (also generell Schadsoftware). So kann beispielsweise über eine Firewire-Schnittstelle der gesamte Hauptspeicher ausgelesen werden, ohne direkt etwas zu verändern. Dieses Auslesen wird nicht bemerkt. Davon kann natürlich ein Kopie erstellt werden und forensisch untersucht werden. Dadurch erlangt man aber nur eine eingefrorene Momentaufnahme.

Ein Sachverständiger muss jedoch den kompletten Datenfluss mitschreiben können. Währenddessen kann es jedoch passieren, dass die Daten durch die eigene Arbeit zerstört wird. Dieses große Risiko wird jedoch häufig totgeschwiegen.
Rootkits und andere Schadprogramme, lesen bereits während des Betriebs unerkannt Daten aus und wären nur über den Hauptspeicher nachzuweisen. Aus diesen Anwendungen können Sachverständige neue Wege erkennen, um Systeme ordentlich zu untersuchen, zumal es keine Literatur dazu gibt, wie man Rechner ausspähen kann, während parallel der Computer in Betrieb ist. Zudem ist auch der menschliche Faktor beim Datenauslesen und Datenklau nicht zu unterschätzen. So wurden USB-Sticks absichtlich verteilt, um die Vorsicht der Computernutzer zu testen. Von 15 verteilten Sticks haben 10 bereits nach 2 Wochen „nach Hause telefoniert.“

Als eine der kontroversen Diskussionspunkt der IT-Forensik wurde die Frage aufgeworfen, ob
bei forensischen Untersuchungen tatsächlich die Black-Box Ergebnisse, Logs, Traces, etc. mitgeliefert werden müssen. Als Spezialfall wurde die Nachvollziehbarkeit auf dem Gebiet der Geldspielgeräte aufgezeigt. Die gesetzlichen Voraussetzungen der Spielverordnung sehen vor, dass auch der Computerinhalt eines Automaten verifiziert werden muss. Über die gewonnenen Daten wird eine Prüfsumme gelegt, die jedoch relativ schwach ist. Die Auslesung dabei geschieht aber mit einem Gerät, sowie mit einer Software, die vom Hersteller stammen. Dadurch kann es nicht zu einer unabhängigen Prüfung kommen und es könnte Manipulation stattfinden. Die Herkunft der Informationen kann also nicht einwandfrei festgestellt werden. Objektiv kann also nicht festgestellt werden, woher was kommt.

Zusammenfassend wurde erklärt, dass ein System für die forensische Analyse weiterlaufen sollte, da sich durch das Abschalten zwar der Schaden nicht mehr vergrößern kann, jedoch kann dann die Entstehungshistorie im RAM nicht mehr vollständig nachvollzogen werden.
Zudem wurde darauf hingewiesen, dass es Anwendungen auf unseren Rechnern gibt, von denen wir nicht wissen, die aber trotzdem Daten auslesen.
Die IT-Forensik wurde als ein mühsames Geschäft beschrieben, in dem man von den Fehlern, die man begeht viel lernt. So muss jeder Analysefall individuell angepasst werden, denn automatisierte Auswertungen sind derzeit nicht bekannt.

Im Anschluss an diesen Teil des Arbeitskreises folgte eine Diskussion um die Vorlage des „Fahrtenschreibers“ durch Sachverständige. Dabei wurde die Meinung vertreten, dass die Vorlage entbehrlich sei, zumal auch das Blut nach einer Blutanalyse nicht mit den Ergebnissen an den Richter oder die Staatsanwaltschaft geschickt wird.

Zudem wurde die Frage aufgeworfen, ob sich beim Einsatz einer fritzbox der cleverer Nachbar in meine fritzbox hacken könnte. Dabei werden die eingegebenen Daten zwar nur als Pünktchen dargestellt, liegen im Hauptspeicher aber in Klarschrift vor. Daran kann der Nachbar also nicht gelangen. Möglich ist jedoch, dass sich der Nachbar an den virtuellen Speicher des Browsers klemmt, und so Datenfragmente der fritz-box findet. So könnte er also das Passwort rückgewinnen. Dies darf allerdings nicht mit WAP-Schlüsseln etc. verwechselt werden. Der virtuelle Adressbereich hat also eine physikalische Datenzelle im virtuellen Datenspeicher.

Im Anschluss sprach Herr Gärtner über die Bedeutung der Computerforensik speziell für die Staatsanwaltschaft. Was muss er leisten, um das richtige Ergebnis für das Verfahren zu gewinnen? Wie kann er die Wahrheit für den Verfahrenslauf beleuchten?

Die Arbeit der Sachverständigen ist sehr unterschiedlich und kann mal das Nachmessen von Chips etc. beinhalten, mal die Analyse von Daten. Dabei muss immer im Hinterkopf bleiben, dass man nie sicher ein komplett richtiges Ergebnis erlangen kann.So gilt ein Sachverständiger als ein Hilfsmittel. Er soll die Wahrheit für den Verfahrensverlauf beleuchten und dabei sämtliche, also sowohl be- als auch entlastende, Erkenntnisse liefern. Somit besteht die Aufgabe darin, dem Staatsanwalt die Entscheidung über Anklage oder Einstellung zu liefern, sowie dem Richter die Entscheidungsfindung bezüglich der Schuld zu ermöglichen. Vereinfacht gesagt muss der Sachverständige als ein Dolmetscher zwischen der Technik und der Justiz aufgefasst werden. Daher müssen die Erkenntnisse lückenlos und nachvollziehbar dokumentiert und kommentiert werden. Dabei liegt es auch am Sachverständigen abzuwägen, was möglich und was nötig ist, um eine Meinungsfindung zu erleichtern. So kann es in einem Gutachten auch durchaus erforderlich sein, dass ausdrücklich geschrieben wird, dass bestimmte Dinge nicht gefunden wurden.

Zusammenfassend stellt sich Sachverständigen bei jedem Fall eine andere Aufgabenkonstellation, die Objektivität und Neutralität als oberste Prämisse erfordert und jederzeit nachprüfbare und verständliche Ergebnisse verlangt. Ein Richter sollte daher auch die Sachverständigenquelle hinterfragen, um zu vermeiden, dass wirtschaftliche Interessen von privaten Sachverständigen mitspielen. Die jederzeitige Nachprüfbarkeit der Befunde ist ein Muss. Ein zweiter Sachverständiger müsste die gleichen Voraussetzungen finden. Daher muss immer mit Kopien gearbeitet werden. Zudem muss der Sachverständige auch Unverständnis bzw. Unkenntnis der Juristen ausräumen, so z.B. darüber, wie Bilder in den Cache eines Browsers gelangen. Dabei muss auch beachtet werden, dass die Unverständlichkeit des Gutachtens zur Unverwertbarkeit führt. Der Sachverständige muss bei der Auswahl seiner Ergebnissee selektiv sein und soll den Beteiligten eine Hilfe und keine Bürde sein.

Des Weiteren gilt: Erst denken, dann prüfen! Brute force ist in der IT-Forensik nicht angebracht.

Im Anschluss an die Vorträge folgte eine angeregte Diskussion um die Zuverlässigkeit und Vertrauenswürdigkeit privater IT-Forensik-Sachverständiger, bei denen ein gewisses wirtschaftliches Interesse die Arbeit möglicherweise beeinträchtigen könnte. Zudem wurde der richtige Zertifizierungsweg für einen öffentlich bestellten Sachverständigen der IT-Forensik, sowie die Anzahl der derzeit tätigen Sachverständigen erfragt.