Einführung in die IT-Forensik

Dietmar Mauersberger

SG 210
Bayrisches Landeskriminalamt
Maillingerstrasße 15
D-80636 München
Dietmar.Mauersberger@polizei.bayern.de
dietmar@dmauersberger.de

1 Historie

Forensische Wissenschaft ist eine Wissenschaft mit Historie. Bereits um das Jahr 700 nach Christus wurde z. B. in China die Verwendung von Fingerabdrücken zur Identifizierung von Schriftstücken eingeführt. Aus dem Jahr 1248 existiert der erste dokumentierte Fall von angewandter forensischer Medizin. Der Chinese Sun Tsu veröffentlichte in seinem Handbuch „Hsi Duan Yu“ wie Unterschiede der Todesursachen festgestellt werden konnten. Es wurden die Differenzen zwischen stumpfen und scharfen Waffen oder zwischen Ertrinken und Strangulieren näher erläutert.[3]

2 Disziplinen

Im Zusammenhang mit Straftaten werden all jene Spuren sichergestellt, die in irgendeiner Form zur Aufklärung dieser beitragen können. Forensische Untersuchungen finden mit Hilfe der meisten modernen Wissenschaften nachvollziehbar und differenziert statt. Das Beispiel des Kriminaltechnischen Instituts (KTI) des Bayerischen Landeskriminalamtes deutet auf das breite Spektrum der durchzuführenden Untersuchungen hin. Wissenschafter und Techniker aus den Bereichen Serologische/medizinische Kriminalistik, Mikrospurenauswertung einschließlich biologischer Kriminalistik, Forensische Chemie, Angewandte Physik, Bewertung von Handschriften, Untersuchung von Urkunden und Papier, Forensische Waffenkunde, Allgemeine Formspurenauswertung, Phonetik, Kriminaltechnische und Forensischer Informations- und Kommunikationstechnik, arbeiten als Spezialisten an 200000 Untersuchen pro Jahr.

[3] Vgl. http://www.forensicdna.com/Timeline.htm.

3 Forensik

Als jüngstes Kind der forensischen Wissenschaften hat es sich die IT-Forensik zur Aufgabe gemacht, Sachverhalte in Strafverfahren der Informations- und Kommunikationstechnik gerichtsverwertbar darzustellen. Davon ist die Rolle der EDV bei Straftaten zu unterscheiden.

IuK-Systeme können zur Planung, Vorbereitung und Ausführung einer Straftat benutzt werden, sind jedoch nicht zwingend zur Durchführung dieser notwendig. Man spricht hier auch von Computerkriminalität im weiteren Sinne. Ist die EDV jedoch in den Tatbestandsmerkmalen einer Straftat vorhanden, wird von Computerkriminalität im engeren Sinne gesprochen. Man bezeichnet dies auch als Kriminalität im Bezug auf Daten, Dateien oder Datenträger.

Als Beweismittel dient alles, was in irgendeiner Form Daten speichern kann. Von Magnetkarten über Mobiltelefone, Faxgeräte bis hin zu Großrechneranlagen war und ist alles in Strafverfahren vertreten. Der Einzug moderner Kommunikationsmittel in allen Bereichen der menschlichen Existenz schafft eine ständig wachsende Vielfalt der zu untersuchenden Gerätschaften.

Wichtigstes Merkmal der IT-Forensik ist, sofern möglich, die objektive Datensicherung und deren Dokumentation. Eine nachvollziehbare Untersuchung mit gerichtsverwertbaren Ergebnissen sichergestellter Daten ist ohne diese nicht durchzuführen. Die Methoden dazu sind so vielfältig wie die Systeme, welche Daten beinhalten. Einmal gesicherte Systeme können nun mit proprietären Mitteln untersucht werden oder man greift auf Lösungen der Industrie und der Open-Source-Gemeinde zurück. Seit geraumer Zeit wird dieser Wachstumsmarkt mit neuen, mehr oder weniger brauchbaren Lösungen bedient.

Die Ergebnisse der Untersuchungen werden gerichtsverwertbar in Gutachten dokumentiert und vor Gericht vertreten.

4 Ausblick

Die polizeilichen Kriminalstatistiken verzeichnen seit Jahren eine stetige Zunahme von Delikten der Computerkriminalität im engeren Sinne. Eine vergleichbare, wenn nicht gar stärkere Tendenz, ist bei den Computerdelikten im weiteren Sinne feststellbar. Diese Entwicklung erfordert eine stetige Weiterentwicklung der IT-Forensik und macht diese zu einer wichtigen und bestehenden Größe in der Strafverfolgung und sie wird weiterwachsen.

Die Strafverfolgungsbehörden arbeiten an der Ausbildung von Richtern, Staatsanwälten und Ermittlungsbeamten, um digitale Beweise und deren Qualität zu erkennen. Spezialisten aus den eigenen Reihen, der Industrie und den Universitäten werden ausgebildet und eingesetzt, um die ermittelnden Beamten zu jedem Zeitpunkt fachlich zu unterstützten.