Leitfaden für die polizeiliche Ermittlung im Umfeld der IT-Forensik

Nadja Huonder

Betriebswirtschafterin HF
Master in Economic Crime Investigation

Nach einer mehrjährigen Tätigkeit bei der Kantonspolizei Graubünden im Bereiche der Wirtschaftskriminalität und bei einer Grossbank in Zürich als Security Specialist gründete Nadja Huonder im Jahre 2014 ihr eigenes Unternehmen. Dort führt sie nebst Dienstleistungen im Finanzbereich insbesondere Ermittlungen in Wirtschaftsdelikten.

Die professionelle Sicherung elektronischer Daten gewinnt zunehmend an Bedeutung, da die Polizei im Rahmen ihrer Ermittlungen immer häufiger mit digitalen Beweismitteln konfrontiert wird. Dabei werden die gleichen Rechtsgrundlagen angewendet wie für andere Dokumente. Gesetzliche Grundlagen zur Beschlagnahme finden sich in der Bundesverfassung (BV) und - da sich die vorliegende Arbeit auf die bündnerische Rechtsordnung stützt - im Gesetz über die Strafrechtspflege des Kantons Graubünden (StPO) sowie im Polizeigesetz des Kantons Graubünden (PolG).

Im Prozess der forensischen Analyse ist zu beachten, dass digitale Beweismittel sehr verletzlich sind und eine Wiederholbarkeit der Spurensicherung in der Regel nicht möglich ist. Über den gesamten Prozess der Sicherstellung ist eine lückenlose Dokumentation erforderlich. Die Daten dürfen bei der Erhebung und Auswertung nicht verändert werden und an den Originaldatenträgern dürfen keine Arbeiten ausgeführt werden.

Bei einer professionellen IT-Ermittlung wird in einer ersten Phase der Auftrag detailliert analysiert und die Ziele, welche mit der Hausdurchsuchung erreicht werden sollen, werden genau festgelegt. Es wird ein Zeitplan erstellt, welcher den Zeitbedarf und den zur Verfügung stehenden Zeitraum für die Einsatzplanung und Durchführung des Einsatzes beurteilt. Danach ist zu definieren, welche Informationen vom betroffenen System im Vorfeld der Sicherstellung benötigt werden und wer in der Lage ist, diese Informationen zu liefern. Schliesslich wird ein Vorgehensplan ausgearbeitet und durch den zuständigen Untersuchungsrichter wird ein Hausdurchsuchungsbefehl ausgestellt.

Daraufhin werden in der zweiten Phase alle frei verfügbaren Informationen des zu erwartenden Computersystems beschafft, um konkretere Anhaltspunkte für die Beweismittelsicherung zu gewinnen und damit den Zeitaufwand vor Ort zu reduzieren.

In der dritten Phase wird definiert, welche Spezialisten für die Sicherstellung der Daten notwendig sind und ob allenfalls externe Fachleute beizuziehen sind. Auch wird ein Koordinator bestimmt, welcher während der Aktion im Hintergrund für IT-Probleme zuständig ist.

Bei der Sicherstellung von IT-Strukturen kommt es nicht selten vor, dass Anpassungen vor Ort notwendig sind. Bereits im Vorfeld der Hausdurchsuchung sind deshalb in einer vierten Phase mögliche Szenarien durchzudenken und vorbehaltene Entschlüsse zu fassen.

Während der Hausdurchsuchung (Phase 5) muss der für das Unternehmen oder für Einzelpersonen entstehende Arbeitsausfall minimiert werden. Alle Personen sind von den Geräten fernzuhalten und ein Eingriff in die Stromversorgung oder auf das Netzwerk ist durch geeignete Massnahmen zu vermeiden. Die angetroffene Situation ist detailliert zu beschreiben und sämtliche am System vorgenommenen Aktionen müssen genau protokolliert werden. Die Computerbenutzer sind auch zu den entsprechenden Login-Informationen zu befragen.

Die Sicherstellung von Daten bildet die sechste Phase der IT-Ermittlung. Zunächst wird entschieden, welche Geräte bzw. Medien vor Ort gesichert werden müssen und welche vorübergehend beschlagnahmt werden können. Eine Stilllegung ganzer Informationssysteme darf nur nach Massgabe der Verhältnismässigkeit und nach Rücksprache mit dem zuständigen Untersuchungsrichter erfolgen. Eingeschaltete, nicht hoch verfügbare Geräte sollten nach der Untersuchung und Sicherstellung der flüchtigen Daten durch Ziehen des Netzsteckers abrupt abgeschaltet und nicht heruntergefahren werden. Ein ausgeschalteter Computer darf niemals einfach eingeschaltet werden. Für den Beweis der Integrität der elektronischen Spuren wird mittels einer speziellen Software vor dem Kopiervorgang der Hashwert berechnet. Dieser wird wenn möglich von der Gegenpartei unterzeichnet und stellt ein elektronisches Siegel der Daten dar. Sämtliche sichergestellten Datenträger sind detailliert im IT-Sicherstellungsprotokoll aufzulisten und für den Transport fachgerecht zu verpacken.

In einer siebten Phase wird der gesamte Inhalt des verdächtigen Rechners bzw. der Speichermedien mithilfe einer Software für die Datenanalyse auf die Zielmedien kopiert. Dabei wird ein zweiter Hashwert errechnet, welcher mit dem Initial-Hashwert übereinstimmen muss. Die identische Kopie der Daten wird danach in ein passendes Analysetool importiert, damit die Daten ausgewertet werden können. Dabei ist

eine optimale Zusammenarbeit zwischen dem IT-Ermittler und dem Sachbearbeiter anzustreben. Datenträger, welche für die Untersuchung unerheblich sind, sind nach Rücksprache mit dem Untersuchungsrichter baldmöglichst gegen eine Empfangsbestätigung zurückzuerstatten. Die anderen Beweismittel werden bis zum Abschluss des Verfahrens aufbewahrt und sind durch geeignete Massnahmen vor Zugriff, Veränderung oder anderen Gefahren zu schützen. Die Berichterstattung über die Ergebnisse bildet den Abschluss der forensischen Arbeit.

Der IT-Ermittlung sind durch verschiedene Gründe Grenzen gesetzt. So fordert die rasante technische Weiterentwicklung eine stetige Weiterbildung der IT-Spezialisten. Die immer komplexeren Verschlüsselungstechniken bilden ein neues und ressourcenintensives Arbeitsfeld. Zudem erhöhen die steigenden Kapazitäten der Speichermedien den Zeitbedarf für die IT-Ermittlung und die wachsenden Speicherdichten erleichtern das Verstecken von grossen Datenmengen. Je häufiger neue Daten in einem System gespeichert werden bzw. das System defragmentiert wird, umso schwieriger ist eine Wiederherstellung der Daten. Auch der physische Zustand der Speichermedien übt einen grossen Einfluss auf den Erfolg einer Ermittlung aus. Hinzu kommt, dass viele Täter generationsbedingt über ein grosses Know-how im Informatikbereich verfügen. Da die Daten oft ausserhalb eines lokalen Systems abgelegt werden, werden die Ermittlungen noch zusätzlich erheblich erschwert. Schliesslich bildet auch die internationale Rechtshilfe in Strafsachen eine Barriere für die Strafverfolgungsbehörden.

Die Folgen eines Schadens aus einem polizeilichen Eingriff werden im Gesetz über die Staatshaftung des Kantons Graubünden geregelt. Die Haftung des Staates setzt Widerrechtlichkeit, einen Schaden sowie einen adäquaten Kausalzusammenhang voraus. Die Gemeinwesen haften aber auch für rechtmässig zugefügten Schaden, wenn einzelnen oder wenigen Personen ein unverhältnismässig schwerer Schaden zugefügt wird und es nicht zumutbar ist, dass der Geschädigte den Schaden selbst trägt. Das direkte Klagerecht des geschädigten Dritten gegen die fehlbaren Organe und Personen ist ausgeschlossen. Ansprüche aus dem Staatshaftungsgesetz beurteilt das Verwaltungsgericht, wobei der Geschädigte neben der Beweislast für die Existenz des Schadens auch die Beweislast für dessen ziffernmässige Höhe trägt.

Die computerforensische Untersuchung gewinnt immer mehr an Bedeutung. Gleichzeitig nehmen auch die Anforderungen, welche an die IT-Forensik gestellt werden, laufend zu. Die Polizei muss sich deshalb mit stetiger Aus- und Weiterbildung der Herausforderung stellen, diesen erhöhten Ansprüchen gerecht zu werden.

Hochschule Luzern - Wirtschaft
Institut für Finanzdienstleistungen Zug IFZ
Grafenauweg 10
Postfach 7344
CH-6302 Zug
+41 41 757 67 67
ifz@hslu.ch