Digital Forensics – CSI für ICT

Der Anruf kam um 7.50 Uhr vom CIO eines Industriekonzerns, der den Verdacht äusserte, dass ein leitender Angestellter systematisch Forschungsdaten veruntreut habe. Dieser Artikel zeigt auf, was in diesem oder ähnlichen Fällen zu tun ist. Christoph Baumgartner, Dilip Many

Die Digitale Forensik bezeichnet die Untersuchung von verdächtigen Vorfällen auf digitalen Geräten, wie beispielsweise Computern, Mobiltelefonen und Memory Sticks, üblicherweise in Verbindung mit einer vermuteten kriminellen Handlung mit dem Ziel, (gerichtsverwertbare) Beweise zu identifizieren und sicherzustellen. Es geht also salopp ausgedrückt darum, zu erkennen, wer wo, wann was und wie mit einem Gerät angestellt hat. Typische Beispiele, die eine digitale forensische Analyse nach sich ziehen können, sind: Datendiebstahl, Besitz oder Bereitstellung von digitalen Medien mit illegalem Inhalt, Malware-Befall, Hackerangriffe, Mobbing, vorsätzliches Löschen von Daten, Industriespionage/Cyber Warfare oder Betrug.

Je nach Art des Untersuchungsobjekts wird zwischen Computer-Forensik, Netzwerk-Forensik, Mobile-Forensik und Memory-Forensik unterschieden. Diese Teilbereiche der Digitalen Forensik stellen jeweils spezifische Anforderungen an das Vorgehen, an die zum Einsatz kommenden Tools und an das Know-how des mit der Analyse betrauten Personals.

Digitale Forensik ist Spurensuche und bietet keine Garantie dafür, dass auch Beweise gefunden werden.

Bild: Fotolia

Erst denken, dann handeln

Die Erfahrung zeigt, dass nur die wenigsten Fälle publik werden und/oder vor Gericht enden. Dies liegt einerseits daran, dass kein Unternehmen daran interessiert ist, in diesem negativ geprägten Zusammenhang in den Medien genannt zu werden. Andererseits sind börsenkotierte Firmen verpflichtet, jegliche Vorkommnisse bekannt zu machen, die einen signifikanten Einfluss auf den Börsenkurs haben können – als präventive Massnahme gegen Insidergeschäfte. Besonders heikel wird es, wenn Mitarbeitende verdächtigt werden, gegen geltendes Recht (Gesetze, Verordnungen etc.) oder firmeninterne Weisungen verstossen zu haben. In diesem Fall stellt sich die Frage, ob Anzeige erstattet wird, was die notwendige Bedingung für eine von der Staatsanwaltschaft verordnete digitale forensische Untersuchung ist oder ob Unternehmen/Organisationen zuerst eine Untersuchung durch unabhängige Experten durchführen lassen. Diese klären dann zunächst ab, ob der Verdacht berechtigt oder unberechtigt ist und wirken so einem allenfalls unberechtigten «Rufmord» entgegen. Es ist ratsam, sich zumindest die Option offen zu lassen, bei Bedarf den Rechtsweg zu beschreiten. Doch wer bei der Untersuchung unbedacht vorgeht, läuft Gefahr, potenzielles Beweismaterial unwiederbringlich zu zerstören oder riskiert dessen Aberkennung vor Gericht.

Bei digitalen forensischen Analysen sind einige Regeln zu beachten. Es folgt eine Auswahl:

Nr. 1: (Vermutetes) Unrecht darf nicht mit Unrecht bekämpft werden. So sind die gesetzlichen Vorgaben einzuhalten. Gerade bei Untersuchungen, bei denen die Handlungen von vermeintlich fehlbaren Mitarbeitern analysiert werden, müssen die Anforderungen des Datenschutzgesetzes eingehalten werden. Wenn kein Überwachungsreglement besteht, müssen die verdächtigten Personen über die anstehenden Untersuchungen in Kenntnis gesetzt werden. Ausserdem dürfen keine vor diesem Zeitpunkt angefallenen Daten von Nicht-Behörden analysiert werden. Wer sich mit den relevanten Gesetzen nicht auskennt, sollte juristische Unterstützung beiziehen.

Nr. 2: Es darf nicht direkt an den Originaldaten gearbeitet werden. Zur Analyse müssen Arbeitskopien erstellt werden. Die einzige Ausnahme bilden Untersuchungen, die an laufenden Systemen durchgeführt werden müssen, da sonst die Daten unwiederbringlich verloren gehen.

Nr. 3: Sämtliche Aktivitäten müssen lückenlos dokumentiert werden.

Nr. 4: Die Systeme, die zur Untersuchung verwendet werden, müssen vom normalen Netzwerk (LAN, WAN und Internet) getrennt sein und idealerweise in getrennten Räumlichkeiten stehen, um unerwünschte Manipulationen zu verhindern/vermindern.

Nr. 5: Es zählen nur belegbare Fakten, keine Vermutungen. Deshalb muss die Argumentationskette lückenlos sein.

Christoph Baumgartner ist CEO und Inhaber der auf Security Audits sowie Digital Forensics spezialisierten Oneconsult GmbH.

Dilip Many ist Security Consultant und Mitglied des Digital Forensic Teams bei der Oneconsult GmbH.
www.oneconsult.com

- Nr. 6: Es wird nach digitalen Spuren gesucht und im forensischen Bericht darauf hingewiesen, ob und welche Spuren gefunden wurden. Die Beurteilung, ob eine Straftat oder ein Verstoss gegen geltende Weisungen begangen wurde, obliegt jedoch nicht dem digitalen Forensiker, sondern ist Sache der Strafermittlungsbehörde oder des Auftraggebers.

Nr. 7: Es sollten nach Möglichkeit nur anerkannte und bekannte Werkzeuge zum Einsatz kommen, da deren Vertrauenswürdigkeit und Zuverlässigkeit vor Gericht von der Gegenpartei per se nicht angezweifelt wird.

Nr. 8: Der Personenkreis, der über die laufenden forensischen Untersuchungen Bescheid weiss, sollte so klein wie möglich gehalten werden.

Nr. 9: «Denn sie wissen, was sie tun.» Digitale forensische Analysen setzen spezifische technische Kenntnisse voraus. Dies gilt insbesondere für Untersuchungen an komplexen Systemen.

Nr. 10: Digitale Forensik ist Spurensuche und bietet keine Garantie dafür, dass auch Beweise gefunden werden – selbst wenn ein Tatbestand an sich in Form eines Geständnisses als erwiesen gilt. Dies kann einerseits daran liegen, dass die beschuldigten Personen dafür gesorgt haben, dass keine digitalen Spuren entstehen oder verbleiben oder aber an den ICT-Systemen liegen, die beispielsweise nicht mehr benötigte Daten mit neuen Daten überschreiben.

Sobald der Entscheid gefällt wurde, einem Verdacht nachzugehen und externe Hilfe beizuziehen, hat sich folgendes Vorgehen immer wieder bewährt.

Briefing/Vorbereitung

Der Auftraggeber und der Auftragnehmer unterzeichnen eine Vertraulichkeitsvereinbarung (NDA). Anschliessend schildert der Auftraggeber die Vorkommnisse und seinen Verdacht. Darauf basierend wird definiert, wo nach welchen Spuren gesucht werden soll und welche organisatorischen und technischen Rahmenbedingungen einzuhalten sind. Danach übergibt der Auftraggeber dem Auftragnehmer die zu untersuchenden Systeme oder Speichermedien, oder er gewährleistet den Zugang zu den Systemen, wenn beispielsweise Server im laufenden Betrieb analysiert werden müssen.

Forensische Datensicherung

Weil üblicherweise nicht mit den Originaldatenträgern gearbeitet werden darf, müssen Kopien erstellt werden. Dafür kommen entweder sogenannte Write-Blocker plus Imaging-Software oder ein Hardware-Datenkopiersystem zum Einsatz. Ein Write Blocker ist ein Gerät, das mit dem für den Kopiervorgang verwendeten Computer und dem originalen Datenträger verbunden wird. Es lässt nur Daten in eine Richtung zu und verhindert, dass durch den Kopiervorgang irgendwelche Daten auf den Originaldatenträger zurückgeschrieben werden. Dies ist essenziell, weil Veränderungen des Inhalts des Originaldatenträgers vor Gericht zur Aberkennung als Beweismittel führen können. Veränderungen lassen sich unschwer durch Vergleich des Hashwertes von Originaldatenträger und Kopie erkennen.

Sogenannte Forensic Duplicator oder Imager sind eigenständige Systeme, die ohne zugehörige Computer Abbilder erstellen können. Unabhängig vom Kopiersystem kann der Kopiervorgang bei modernen Festplatten mit einer Speicherkapazität von mehr als 2 TB je nach zur Verfügung stehender Schnittstelle auch über 24 Stunden dauern.

Datenanalyse und Dokumentation

Sobald die Kopien der zu untersuchenden Datenträger vorliegen, beziehungsweise die zu untersuchenden Systeme zugänglich sind, kann mit der digitalen Spurensuche begonnen werden. Hierbei kommt oft Spezialsoftware zum Einsatz, die die forensische Untersuchung vereinfacht und beschleunigt. Man kann dabei Open-Source- oder kommerzielle Software nutzen. Im Bereich Computer-Forensik dominieren zwei etablierte Hersteller kommerzieller Software den Weltmarkt: Accessdata mit «Forensic Toolkit» (FTK) und Guidance Software mit «Encase Forensic». Deren Software ist zwar kostspielig, wird aber weltweit von digitalen Forensikern und Behörden eingesetzt und ist vor Gericht anerkannt. Es gibt noch Dutzende anderer Produkte im Markt, die sich aber noch nicht international durchsetzen konnten. Einige nützliche, frei verfügbare Tools: Mandiant Redline eignet sich unter anderem für das Auslesen von Browser-Daten (History, Cookies, Download History und Form History). Exiftool vereinfacht das Auslesen von Metadaten wie beispielsweise aus Bildern die EXIF-Daten (Aufnahmezeit des Fotos, Kamera, gegebenenfalls GPS-Koordinaten bei aktiviertem GPS) oder den Speicherort der geöffneten Datei und deren Zeitstempel zum Zeitpunkt des Öffnens bei Verknüpfungsdateien. Thumbs Viewer zeigt Thumbnails an, die grundsätzlich im Cache verbleiben, selbst wenn die Originaldatei gelöscht wurde. Für Memory Forensics bei Microsoft-Betriebssystemen eignen sich beispielsweise kommerzielle Tools wie «Responder» von Hbgary. Bei Mobile Forensics, also der Analyse von Mobiltelefonen und Tablets, kommt man meist nicht mit einem einzelnen System/Tool aus, weil tausende verschiedene Gerätetypen im Umlauf sind und täglich neue hinzukommen. «UFED Touch» von Cellebrite ist eine Appliance, die sehr viele Gerätetypen analysieren kann.

Da die Dokumentation das zentrale Resultat einer digitalen forensischen Analyse ist, muss sie sehr sorgfältig erstellt werden. Üblicherweise enthält sie neben der Beschreibung des genauen Auftrags, der mit dem Projekt betrauten Akteure und der gewonnenen Fakten auch den detaillierten Ablauf der forensischen Analyse einschliesslich der Erwähnung der eingesetzten Werkzeuge. Es dürfen nur klar belegbare Fakten (z.B. mit Sceenshots) aufgeführt, aber keine Vermutungen angestellt werden – selbst wenn keine Spuren gefunden wurden, heisst dies noch lange nicht, dass keine Straftat begangen wurde. Umgekehrt belegt eine detektierte E-Mail an eine bestimmte Empfängeradresse noch keinen tatsächlichen Mailverkehr mit dem Inhaber der Adresse.

Präsentation/Diskussion

Der Auftraggeber entscheidet meist aufgrund der Erkenntnisse der forensischen Analyse, ob die interne Untersuchung eingestellt oder Anzeige erstattet wird. Diese Entscheidung sollte gemeinsam mit juristischem Beistand erfolgen, um die Erfolgschancen einer Klage und den zu erwartenden Kollateralschaden auszuloten.

Digital Forensic Readiness

Es gibt kein 100 Prozent wirksames Mittel, sich vor der Notwendigkeit forensischer Untersuchungen zu schützen. Aber man kann sich für den Ernstfall wappnen. Es gilt Prozesse zu definieren, wer wie was macht und welche Kompetenzen und Prioritäten vorliegen. Hier kann auch der Beizug von externen Spezialisten angedacht werden. Ausserdem sollte, falls noch nicht erfolgt, ein Überwachungsreglement erstellt werden. Dies kann auch Bestandteil des IT-Nutzungsreglements sein. Auf technischer Ebene ist zu definieren und zu implementieren, auf welchen Systemen was für Daten in welcher Granularität gesammelt werden und wie lange sie aufbewahrt werden sollen. Zu guter Letzt müssen die Massnahmen getestet und eingeübt werden und auch immer wieder an gemachte Erfahrungen und veränderte Bedingungen angepasst werden.

Es hat schon seinen Grund, warum die meisten Fälle mutmasslicher Datenveruntreuung nicht im Gerichtssaal, sondern im Sitzungszimmer enden, wo sich Auftraggeber und Beschuldigter zähneknirschend «in gutem Einvernehmen» trennen – nicht ohne dem Beschuldigten Redeverbot aufzuerlegen. So endete auch der eingangs erwähnte Fall. <