Beweissicherung bei Computerdelikten

Ausgrabungen

Lukas Grunwald

Herkömmliche Indizien wie Fußabdrücke oder am Tatort hinterlassene Gegenstände sind für Kriminalisten in aller Regel leicht zugänglich. Ungleich komplizierter hingegen gestalten sich Spurensuche und Beweissicherung im Inneren eines Rechners, der Hilfsmittel oder Ziel einer Straftat war.

In- und ausländische Strafverfolgungsbehörden registrierten in den vergangenen Jahren eine starke Zunahme von Straftaten, die von Computern oder Rechnernetzen aus durchgeführt wurden. Das Spektrum der Straftaten reicht vom Betrug mit 0190-Dialern über die Verbreitung von illegalem Material wie Kinder- oder Tierpornografie, das Fälschen von Bilanzen und Betriebsdaten, das Verbreiten von Computerviren bis hin zum Einbruch in fremde Rechnersysteme. Angesichts der zunehmenden Delikte gewinnt der Computer in kriminalistischen Untersuchungen und Gerichtssälen an Bedeutung.

Sobald Ermittler eine Untersuchung einleiten, weil jemand per Computer eine Straftat begangen hat oder ein Rechnersystem manipuliert oder kompromittiert wurde, beginnt ein technischer und kriminalistischer Prozess, den man als Forensic Computing, häufig auch als Computer Forensic oder Digitale Forensik bezeichnet. Noch sind die Inhalte dieser verhältnismäßig jungen Disziplin nicht klar umrissen. Fachautor Michael Caloyannides etwa definiert sie als die Sammlung aller Techniken und Werkzeuge, um Beweismittel in einem Rechnersystem zu finden [1].

Diese Definition greift jedoch zu kurz. Zum Finden und Sichern der hinterlassenen Datenspuren kommt die Aufbereitung der Fakten zu einem vor Gericht verwertbaren Gutachten hinzu. ‘Evidenz’ heißt hier das Schlagwort: Die Forensik-Spezialisten stehen vor der Aufgabe, technische Sachverhalte und Indizien so darzustellen, dass auch für die in technischer Hinsicht unbedarften Prozessteilnehmer Tatbestand sowie Beweiskette augenfällig (evident) werden. Ebenfalls Bestandteil der forensischen Analyse ist die Dokumentation. Jeder Handgriff bei der Beweismittelsicherung und der Untersuchung ist zum Zweck des späteren Nachvollziehens exakt zu protokollieren.

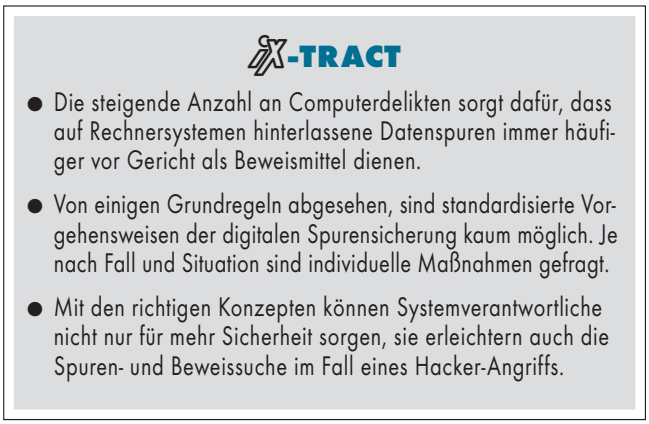
Bei der Benutzung eines Computers sammeln sich zahlreiche Daten an, die Aufschluss über den Anwender geben und im Ernstfall als Beweismittel dienen können. Zu diesen Daten gehören unter anderem die Prozessor-ID, der Swap- oder Page-Bereich, die Dateisysteme, Token, Flash-Speicher sowie die MAC-Adresse der Netzwerkadapter. Ergänzend lassen sich für kriminalistische Untersuchungen auf dem Schreibtisch liegende Datenträger, Aufzeichnungen und ausgedruckte Dokumente, Inhalte von PDAs oder Telefonverzeichnisse in Mobiltelefonen heranziehen. Alle diese Daten beinhalten eine Vielzahl an Informationen, die gegebenenfalls mit den auf dem Rechner gefundenen Daten zu korrelieren sind.

Erstellen von Daten-‘Konserven’

Vor Beginn einer forensischen Analyse müssen die Spezialisten zunächst den gesamten verfügbaren Datenbestand ermitteln und die verschiedenen Datenträger sicherstellen. Um die Originalbeweise zu ‘konservieren’ und

eine potenzielle Beeinträchtigung durch die Analyse selbst zu vermeiden, findet die eigentliche forensische Untersuchung auf einer Kopie des gesicherten Datenbestandes statt. Für die Erzeugung des Abbildes spiegelt der Fachmann die Festplatte auf physikalischer und logischer Blockebene mit einem speziellen Werkzeug, das unter anderem in Forensik-Toolkits enthalten ist. Auf diesem Spiegel kann nun im Read-only-Modus die Untersuchung erfolgen. Vorsichtig sollte man allerdings bei der Auswahl des Tools sein: Manche Klon-Methoden zerstören die für die forensische Analyse erforderlichen Meta-Daten.

Verhältnismäßig einfach ist die Datensicherung, wenn etwa in Fällen von Steuerhinterziehung, Abrechnungsbetrug oder anderen Straftaten die Strafverfolgungsbehörden einen Rechner konfiszieren. Das Spiegeln und Untersuchen der Daten kann ohne Zeitdruck stattfinden. Schwieriger gestaltet es sich bei einem Hacker-Einbruch in ein System, denn in diesem Fall gilt es, einen Vorgang beziehungsweise verschiedene Prozesse nachzuvollziehen. Ist der Einbruch bei seiner Entdeckung bereits abgeschlossen, erzeugen die Fachleute mit dem entsprechenden Forensic-Tool ein Abbild der beteiligten Prozesse. Unter Linux lässt es sich mit Systemmitteln – *dd*-Befehl und */proc*-Filesystem – erstellen.



Beweissicherung 'on the fly'

Ist der Angriff jedoch noch nicht abgeschlossen, steht der Administrator vor einer Entscheidung. In aller Regel empfehlen Forensik-Experten für einen solchen Fall die sofortige Trennung des entsprechenden Rechners vom Netzwerk. Auf diese Weise soll der Angriff abgebrochen, aber auch das Löschen verräterischer Spuren des Hackers vermieden werden. Bleibt der Rechner online, besteht andererseits die Möglichkeit, die Verbindungsdaten des Angreifers herauszufinden oder seinen Arbeitsspeicherbereich als Speicherabbild auf die eigene Festplatte zu schreiben. Ein Administrator muss in Sekundenschnelle Nutzen und Schaden gegeneinander abwägen, sich notfalls kurzfristig umentscheiden und den Stecker ziehen, wenn etwa der Hacker plötzlich beginnt, Daten zu löschen oder neu zu formatieren. Eine Gewährleistung für die Unversehrtheit der Daten ist allerdings auch dann nicht gegeben, im schlimmsten Fall hat der Angreifer ein zeitgesteuertes Programm (cron job) eingeschleust, das seine Spuren verwischt oder Daten zerstört.

Der abschließende Zustand des Systems ist umgehend 'einzufrieren', sodass für die Analyse eine Art Momentaufnahme zur Verfügung steht. Jede Veränderung, auch unwissentlich, kann dafür sorgen, dass die Daten als Beweismittel wertlos sind. Beispielsweise modifiziert ein Systemstart von Windows 2000 192 Dateien. Einen Bootvorgang sollte man daher bei Vorfinden eines ausgeschalteten Rechners vermeiden, die Analyse erfolgt nach dem Ausbau der Festplatte. Umgekehrt ist es wenig ratsam, einen laufenden Rechner herunterzufahren: Das System löscht bei diesem Vorgang flüchtige Daten wie Cache-Inhalte oder manche Log-Dateien, gelegentlich überschreibt es auch den Hauptspeicher-Swap-Bereich.

Feuerresistente Festplatten

Von besonderen Fällen im laufenden Betrieb abgesehen, erfolgt die Sicherung der Daten in der Reihenfolge ihrer Vergänglichkeit: kurzlebige Cache-Inhalte, Hauptspeicher und laufende Prozesse zuerst, Daten auf Festplatten, CDs oder Disketten zuletzt.

Aufwand und Kosten einer Analyse bemessen sich nach

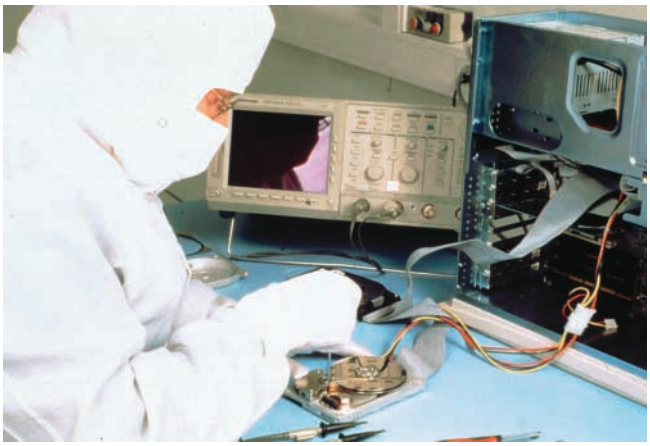
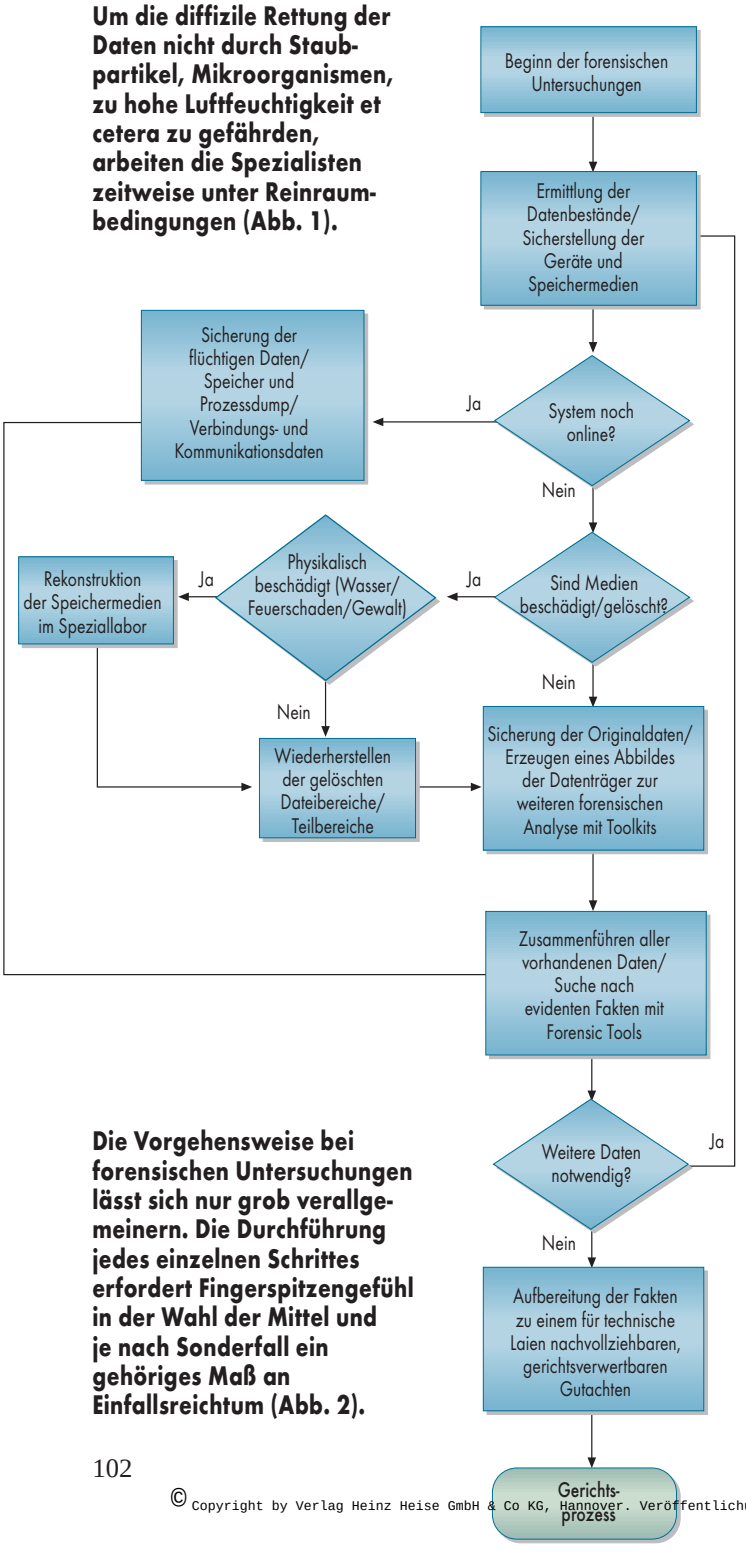


Foto: ibas

Um die diffizile Rettung der Daten nicht durch Staubpartikel, Mikroorganismen, zu hohe Luftfeuchtigkeit et cetera zu gefährden, arbeiten die Spezialisten zeitweise unter Reinraumbedingungen (Abb. 1).



Die Vorgehensweise bei forensischen Untersuchungen lässt sich nur grob verallgemeinern. Die Durchführung jedes einzelnen Schrittes erfordert Fingerspitzengefühl in der Wahl der Mittel und je nach Sonderfall ein gehöriges Maß an Einfallsreichtum (Abb. 2).

den jeweiligen Erfordernissen. Ist etwa die Festplatte beschädigt, müssen zunächst Datenrettungslabore den physikalischen Datenzugriff wiederherstellen. Die Chancen auf Erfolg stehen dank moderner Technik ziemlich gut. Und wenn ein Übeltäter glaubt, Beweise durch Verbrennen vernichten zu können, täuscht er sich. Die heute produzierten Festplatten können mehrere Minuten im Feuer liegen ohne dass der 'Curie-Punkt' – die Temperatur bei der das magnetische Speichermedium Informationen verliert – erreicht wird. Mit speziellen Verfahren lassen sich zumindest große Teile des Datenbestandes rekonstruieren (Abb. 1).

Nach der Sammlung und Sicherung aller Beweise kann die Analyse der Daten beginnen. Das Speichern einer Datei auf der Festplatte erfolgt in mehreren Schritten auf verschiedenen Ebenen des Computers (Abb. 3). Aus diesen extrahiert der Fachmann die Informationen, üblicherweise von oben nach unten (Top-down). Zunächst beginnt er mit der Beweissuche in den 'normalen' Dateien, die mit den Mitteln des Betriebssystems zugänglich sind (Stufe 7 in Abb. 3). Finden sich hier keine Indizien, so gilt es im nächsten Schritt, gelöschte Dateibereiche mit speziellen Werkzeugen wieder sichtbar und zugänglich zu machen (Stufe 6 in Abb. 3).

Stufe 6 ist noch in anderer Hinsicht aufschlussreich. In ihr lassen sich etwa Zugangsberechtigungen und – unter Unix – die verschiedenen Zeitstempel analysieren: wann die letzte Veränderung stattfand (M-), wann zuletzt zugegriffen (A-) und wann die Datei erzeugt wurde (C-). Wenn auszuschließen ist, dass jemand die Meta-Daten, die diese Stempel enthalten, manipuliert hat, kann der Untersuchende die letzten Dateizugriffe nachvollziehen. Wenn nicht, sucht er nach Beweisen, dass und in welcher Weise Meta-Daten oder Filesystem manipuliert wurden.

Für rekonstruierte Dateien sind unter Umständen keine Dateinamen und Directory-Einträge mehr verfügbar. In diesem Fall versucht der Fachmann, mit einer Mustersuche Beweise zu finden. Die Header vieler Dateiformate enthalten Informationen über die charakteristische Datenstruktur, etwa Farbtiefe oder Auflösung bei Bilddateien. Besteht nun der Verdacht, dass sich auf einem Rechner verbotenes Bildmaterial befindet, versucht man mit der Patternsuche alle Bilddateien aufzuspüren. Anschauen muss man allerdings jede einzelne 'von Hand'. In besonderen Glücksfällen kann eine Datei im Header zusätzliche Informationen über ihren Ersteller oder den Ursprungsserver enthalten. Der Datenbestand lässt sich je nach Delikt auch nach speziellen Wörtern durchsuchen. Da unterschiedliche Kodierungen gebräuchlich sind, ist es ratsam, die Pattern anhand verschiedener Kodierungsvarianten eines Begriffes zu erzeugen. Die Mustersuche erfolgt mit einem forensischen Tool auf der logischen Ebene (Stufe 5 in Abb. 3).

Client- und Serveranalyse

Je nachdem, welcher Rechner Ziel einer Untersuchung ist, unterscheidet man zwischen der Client- und der Server-Forensik. Erstere ist häufig bei der Suche nach dem Besitz oder der Verbreitung illegaler Inhalte relevant. Um Besitzer von pornografischen Bildern mit Kindern dingfest zu machen, setzen deutsche Strafverfolgungsbehörden ein vom Landeskriminalamt Wiesbaden eigens entwickeltes Programm namens Perkeo (Programm zur Erkennung Relevanter kinderpornografischer eindeutiger Objekte) ein. Allein das Programm 'schwächelt': Da der Besitz dieser Bilder strafbar ist, darf

Erste-Hilfe-Maßnahmen für Administratoren

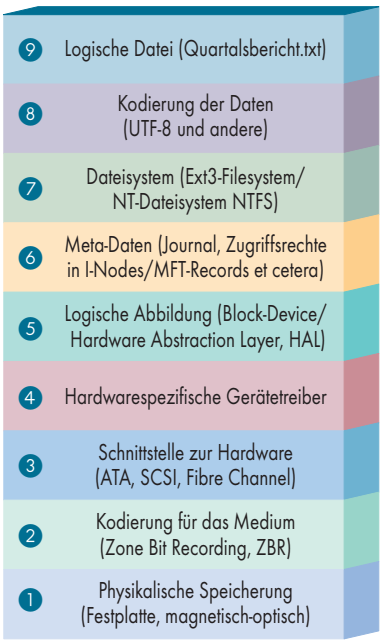
Wenn ein Angriff entdeckt wird:

– Ruhe bewahren, auf keinen Fall unüberlegt handeln;
– je nach Situation Netzwerkverbindung kappen, um weitere Vorkommnisse oder das Verwischen von Spuren zu unterbinden;
– Log-Dateien der Firewall und anderer nicht kompromitierter Systeme sichern;
– Protokoll über alle Ereignisse mit genauen Zeitpunkten erstellen;
– alle Daten möglichst rasch sichern, unabhängig von der Standardtagessicherung;
– Eine physikalische Kopie anfertigen, wenn möglich mit allen Meta-Daten;
– Profis rufen; nicht versuchen, eine Analyse durchzuführen, wenn das Fachwissen fehlt.

die Software auch keine einschlägigen Bilder als Mustervorlage enthalten. Das Programm erkennt folglich keine verbotenen Bilder per se, sondern lediglich schon bekanntes und klassifiziertes Material anhand einer digitalen Prüfsumme.

Neben der Unzulänglichkeit der Software gilt es überdies zu berücksichtigen, dass der Rechner eines Anwenders über eine Sicherheitslücke in einem Chat-Programm – beispielsweise mIRC – ohne dessen Wissen als Tauschbörse missbraucht werden kann. Eine Sicherheitsanalyse des PCs, die alle be- und entlastende Daten enthüllt, kann der Wahrheit dienlich sein. Eine solche Sicherheitsanalyse muss alle Kommunikationswege eines Rechners berücksichtigen: vom Modem, DFÜ-Netzwerk über die Internetanbindung bis hin zum Drucker. Inklusive der Suche nach Schwachstellen, die ein Eindringling genutzt haben könnte. Hilfreich sind auch Log-Dateien wie das Event-Log bei NT oder das Syslog unter Unix. Sie beinhalten eine Vielzahl für die Analyse relevanter Informationen, unter anderem, wann und wie oft sich ein Benutzer an- und abgemeldet hat, zu welchen Zeiten der PC online war und so weiter. So wurde eine 65-jährige Verwaltungsangestelle einer amerikanischen Universität entlassen, weil sie angeblich pornografische Bilder auf ihrem Rechner gespeichert hatte. Die Client-Analyse brachte es an den Tag: Da sie ihren PC bei Dienstschluss nicht abgemeldet hatte, missbrauchte das Raumpflegepersonal ihren Account zum Surfen.

Auch die serverseitige Analyse kann zum Ergreifen eines Täters führen, wie folgendes Beispiel zeigt: Ein Administrator fand eines Morgens auf der Konsole des unternehmenseigenen Web-Servers seines Unternehmens die Anzeige ‘Someone ownz this Host’ vor. Ein Root-Login führte zur Meldung ‘you don’t exist, go away’ und beim Versuch eines Reboots blieb der Bootloader mit Kernel-Panic stehen. Bei der anschließenden Untersuchung fand sich zwar noch ein Dateisystem, allein das Unix-File-System (UFS) war leer. Ein Hacker hatte den Löschbefehl *rm -rf /* eingegeben. Die Analyse der Meta-Daten und des Filservers ermöglichte es, den Einbruch nachzuvollziehen. Die Log-Dateien und die History-Datei der Shell, die der Hacker benutzt hatte, spiegelten nicht nur den gesamten Angriff wieder, sondern enthüllten überdies die Quell-IP-Adresse des Hackers.



Bis eine Datei den Weg in den Speicher findet, durchläuft sie verschiedene Stationen (Abb.3).

Wenn zusätzliche Daten von Firewall-Systemen oder die Routing- und Accounting-Daten des Internet-Providers verfügbar sind, lässt sich eine Kommunikationsbeziehungsanalyse (‘Forensic Accounting’) durchführen. Diese Verkehrsbeziehungsdaten ermöglichen es unter Umständen, die Herkunft des Angriffs oder

Forensik in der polizeilichen Arbeit

Ein Mitarbeiter einer Softwarefirma kündigt seine Arbeitsstelle und gründet ein eigenes Unternehmen. Nur kurze Zeit später verkauft das Unternehmen eine eigene Software, die derjenigen der anderen Firma verdächtig ähnlich ist. Ein Szenario aus einem Spionagefilm? Weit gefehlt. 'Informationshehlerei' nennt sich dieser Diebstahl von Betriebsgeheimnissen und ist eines der häufigsten Delikte, das die Abteilung Forensische Kommunikations- und Informationstechnik (IuK) des Landeskriminalamts Hamburg zu untersuchen hat. 'Die Chancen, den Diebstahl nachzuweisen, stehen gut', bericht Thomas Schwarze, Leiter der Abteilung. Denn die Täter hinterlassen Unmengen von Spuren auf ihren Rechnern.

Seit Mitte der achtziger Jahre bildeten sich in den Landeskriminalämtern Abteilungen, die sich auf EDV-bezogene Delikte konzentrierten. Heute gibt es in jedem LKA eine Abteilung Forensische IuK. Ausstattung und Organisationsstruktur sind jedoch alles andere als einheitlich. Während in einigen Bundesländern Fremdfirmen große Teile der Analyse übernehmen, führen in Hamburg geschulte Fachleute nahezu alle Untersuchungen selbst durch, einschließlich der Erstellung des Gutachtens und der Vertretung der Behörde vor Gericht.

Die steigende Zahl der Computerdelikte und die rasante Entwicklung der Technik erfordert die ständige Qualifizierung der Forensik-Spezialisten. 'Aus- und Fortbildung machen ungefähr ein Drittel der Arbeitszeit aus', so Schwarze, die restlichen beiden Drittel verwenden die Fachleute zu gleichen Teilen auf die Untersuchung und die Erstellung des Gutachtens. Ausreichende Mittel für den steigenden Bedarf an Personal und Know-How sind allerdings in den wenigsten Landeskriminalämtern vorhanden.

Neben diesen Schwierigkeiten haben die Beamten auch mit alltäglichen Hürden zu kämpfen: In Fällen von Abrechnungsbetrug bei Rechtsanwälten, Steuerberatern oder Ärzten müssten die Beamten strenggenommen die Rechnersysteme beschlagnahmen und mitnehmen. Damit wären Arztpraxen jedoch nicht mehr arbeitsfähig. Ein Kompromiss muss her: Nur die entbehrlichen Rechner werden beschlagnahmt, für die Untersuchung der restlichen muss eine vor Ort erstellte Spiegelung der Festplatte genügen. Überdies bereitet der Datenschutz Probleme. Auf den Computern befinden sich sensible Finanz-, Kranken- oder andere Daten, die niemand sehen darf. Beim Durchsuchen des Datenbestandes nach Beweisen bekommen die Ermittler diese jedoch unweigerlich zu Gesicht. Eine Lösung ist dafür noch nicht in Sicht, es bleibt nur das Vertrauen in die berufliche Verschwiegenheitspflicht der Beamten.

Trotz aller Schwierigkeiten ist Thomas Schwarze mit seiner Abteilung zufrieden. Die Fälle, die vor Gericht kommen, werden dank der forensischen Beweissicherung in aller Regel erfolgreich abgeschlossen. Die meisten in Hamburg erwischten Täter sind so genannte Skriptkiddies. Über die Täterstruktur im allgemeinen sagt das jedoch wenig aus. Denn, so Thomas Schwarze, 'diejenigen, die gute Fachkenntnisse haben, lassen sich eben nicht erwischen'. *Ute Roos*

des Hackers zurückzuverfolgen – sofern er nicht ein weiteres gehacktes System als Ausgangspunkt für seine Taten benutzt. Am Tatort selbst ist ergänzend festzustellen, wer Zugang zu welchen Räumen und Rechnern hat oder wie die Zugriffs- und Ausführungsrechte verteilt sind. So lässt sich unter Umständen der Täterkreis einschränken.

Der letzte Arbeitsschritt nach Analyse aller Daten ist die Aufbereitung der Beweise und Fakten zu einem gerichtlich verwertbaren Gutachten. Die kriminalistische Untersuchung führen in aller Regel eigene Ermittlungsbefugte durch, sodass sich das Gutachten der Forensik-Spezialisten auf die rein technische Beweislage beschränkt. Wie schwierig es ist, diese den am Prozess beteiligten IT-Laien zu vermitteln, zeigt allein die häufige Bitte der Beteiligten, den gesamten Inhalt einer Festplatte auszudrucken, so berichtet das Datenrettungsunternehmen ibas. Bei einer modernen 80-GigaByte-Festplatte ergäbe das einen Papierberg in der Höhe des Mount Everest.

Übersetzung für technische Laien

Die 'Übersetzung' der technischen Fakten in verständliche Beispiele erfordert einen hohen Zeitaufwand, wie Thomas Schwarze, Leiter der Abteilung Forensische Informations- und Kommunikationstechnik im Landeskriminalamt Hamburg, berichtet. Das Erstellen des Gutachtens dauert nach seinen Erfahrungen ungefähr so lange wie die eigentliche Untersuchung. Ein Trost bleibt allerdings: Sind die Beweise so evident, dass es zu einer Gerichtsverhandlung kommt, gelingt in der Regel auch die sprachliche Vermittlung, und die Anklage gewinnt den Prozess.

Da Angriffe auf ein System trotz Vorkehrungen nie auszuschließen sind, sollten Administratoren rechtzeitig Maßnahmen ergreifen, die im Ernstfall eine forensische Analyse vereinfachen. Als erster Schritt ist eine Firmen-Policy mit Sicherheitsrichtlinien zu erstellen. Bestandteil sollte auch ein Notfallplan sein, der den Themenkomplex Incident Response (Reaktion auf einen Sicherheitsvorfall) behandelt. In diesem Konzept sind die Alamierungsketten, die Zuständigkeiten und die Vorgehensweise genau zu definieren. In Schulungen sollten Benutzer für Sicherheitsthemen sensibilisiert und in die Policy eingeführt werden.

Im nächsten Schritt dokumentieren die Systemverantwortlichen das Netzwerk mit allen aktiven Komponenten. Die Aktualität der Dokumentation lässt sich durch ein Security-Change-Management gewährleisten. Die einzelnen Subsysteme mit ihren Komponenten sind einer Risikobewertung zu unterziehen und je nach Schutzbedarf mit Sicherheitsvorrichtungen wie Intrusion-Detection-Systemen oder einer Firewall auszustatten.

Zentrale Sammelstelle für Beweise

Für das spätere Nachvollziehen von Vorfällen ist es wichtig zu wissen, wann genau sich was ereignet hat. Alle neueren Microsoft-Betriebssysteme (Win2k, XP), sämtliche Unix-Derivate, Novell Netware und Ciscos IOS Software unterstützen das Network Time Protocol NTP (www.ntp.org). Es dient als Basis für die Einrichtung eines Zeitstempelservers, der sämtliche Datenzugriffe, -veränderungen und sonstige Ereignisse mit exakter Uhrzeit festhält. Die Referenzzeit kann entweder über eine Funkuhr (DFC77/GPS) empfangen werden oder, bei Systemen mit einer Standleitung, vom Server der Physikalisch-Technischen Bundesanstalt in Braunschweig (ntp1.ptb.de).

Empfehlenswert ist ebenfalls der Betrieb eines zentralen Log-Servers. Mit einem sicheren Verfahren sammelt er alle Log-Meldungen aus dem Netz (Serverfarm) und schreibt sie manipulationssicher auf ein Medium, etwa auf ein optisches WORM-Laufwerk (Write Once Read Many). Alle protokollierten Ereignisse der Firewall, des Intrusion-Detection-Systems sowie die Logmeldungen der einzelnen Server treffen hier zusammen. Für einen Angreifer dürfte es somit schwierig sein, seine Spuren zu verwischen.

Um Manipulationen am Betriebssystem, beispielswei-

RESSOURCEN IM WEB

Forensic-Toolkit TASK: www.atstake.com/research/tools/task/ TASK
Forensic-Toolkit TCT: www.fish.com/tct TCT
Forensic-Toolkit EnCase: www.guidancesoftware.com/products/software/encaseforensic.shtm
Windows-Tool für Patternsuche auf der Festplatte: www.x-ways.com/
Tool für Suche nach pornografischen Bildern: www.perkeo.net/index.html

se durch Rootkits, zu erkennen, sollte der Administrator bei einem 'sauberen' Systemstand eine Liste mit MD5-Checksummen von allen System-Binaries und dem Systemkern anlegen. Im Falle eines Angriffs zeigt ein Vergleich der Checksummen, welche Daten verändert wurden.

Auch wenn die beschriebenen Maßnahmen die Spurensuche im 'worst case' vereinfachen, können sich Hindernisse ergeben. Eine Schwierigkeit ist die unterschiedliche Kodierung der gespeicherten Daten je nach Betriebssystem (ASCII unter DOS, EBCDIC bei IBM Mainframes AS/400, Unicode unter Linux, Windows 2k und XP). Eine Vielzahl von Binärformaten kommt hinzu, wenn sich auf dem System Bild- oder Sound-Daten befinden. Eine weitere Hürde für die Analyse sind verschlüsselte Dateisysteme, wie sie beispielsweise das Programm PGP disk erzeugt. Erfolgsgarantie gibt es keine, unter Umständen lässt sich jedoch mit etwas Mehraufwand auch mit diesen Daten etwas anfangen.

Damit die Forensik-Spezialisten nicht mit einem Hex-Editor alle Sektoren der Festplatte von Hand durchsuchen müssen, existieren Werkzeuge und Toolsammlungen, die verschiedene Analyseschritte durchführen. Dennoch sind für eine forensische Untersuchung tiefgehende Kenntnisse von Betriebs- und Dateisystemen, Netzwerken sowie Dateiformaten und Meta-Daten unerlässlich.

Griff in die Werkzeugkiste

Ein Beispiel für eine solche Toolsammlung ist The @tstake Sleuth Kit (TASK), die unter der IBM Public License Version 1.0 zur Verfügung steht. TASK basiert auf dem zwei Jahre alten The Coroner's Toolkit (TCT), der ersten verfügbaren forensischen Werkzeugsammlung. Die Sammlung besteht zum Teil aus Unix-Befehlen wie *file*, der anhand des Dateianfangs versucht, die Dateiart zu bestimmen. Mit diesen Befehlen ist der Ermittler in der Lage, das Image einer mit *dd* erzeugten Festplatte unter Unix zu analysieren. Ein mit TASK erzeugtes Image liefert die folgende Ausgabe des Hauptinhaltsverzeichnisses:

```
[root@sherlock bin]# fls -f ntfs /
images/winxp.dump
r/r 4-128-4:        $AttrDef
r/r 8-128-2:        $BadClus
r/r 8-128-1:        $BadClus:$Bad
r/r 6-128-1:        $Bitmap
r/r 7-128-1::       $Boot
d/d 11-144-4:       $Extend
r/r 2-128-1:        $LogFile
r/r 0-128-1:        $MFT
r/r 1-128-1:        $MFTMirr
r/r 9-128-0:        $Secure:$SDS
r/r 9-144-1:        $Secure:$SDH
r/r 9-144-2:        $Secure:$SII
r/r 10-128-1:       $UpCase
r/r 3-128-3:        $Volume
d/d 21344-144-1: .ssh
d/d 3241-144-6:     Documents and
                    Settings
r/r 3223-128-1:     hiberfil.sys
r/r 27-128-1:       pagefile.sys
d/d 3640-144-6:     Program Files
d/d 9627-144-1:     RECYCLER
d/d 9382-144-1:     System Volume
                    Information
d/d 19996-144-6: tmp
d/d 11772-144-5: wincmd
d/d 28-144-6:       WINDOWS
d/d 9820-144-5:     WUTemp
```

Aus dem Image lassen sich alle benötigten Daten und Meta-Daten extrahieren, vorausgesetzt das Festplattenoriginal war lesbar. Andernfalls sind wieder einmal die Fertigkeiten eines Datenretters gefragt. Wer es bequem mag: Für TASK existiert ein grafisches Frontend namens Autopsy.

Ausgesprochen beliebt ist das kommerzielle Toolkit EnCase Forensic 3.0, da diese Alles-in-einem-Sammlung keine Unix-Kenntnisse erfordert. Mit ihr lassen sich Festplatten klonen, Analysen auf dem Image durchführen sowie Datenbestände nach Bildern, Dokumenten und anderen Pattern durchsuchen.

Ein spezielles Feature von EnCase ermöglicht die Suche nach Dateien, deren Extension nicht mit ihrem Inhalt in Einklang steht. Eine JPEG-Bilddatei, die zur Verschleierung etwa in *readme.doc* umbenannt wurde, erkennt das Programm augenblicklich. EnCase kann auch in Outlook-Express-Ordnern nach E-Mail-Anhängen suchen. Es lässt sich auf einem System ohne zusätzliche Installation von einer Boot-Diskette aus starten und kann über eine Netzwerk-, eine Parallel-Port- oder eine serielle Verbindung von einem mobilen Ermittlungs-PC aus nach Beweisen suchen. Dieses Tool-Kit ist speziell für die Untersuchung von Windows-Client-PCs gedacht, funktioniert aber ebenfalls bei Mac OS und Linux-Systemen sowie CDs und DVDs. (ur)

LUKAS GRUNWALD

arbeitet als Consultant bei DN Systems, Hildesheim.

Literatur

[1] Michael Colayannides; Computer Forensics and Privacy; Artech House 2001