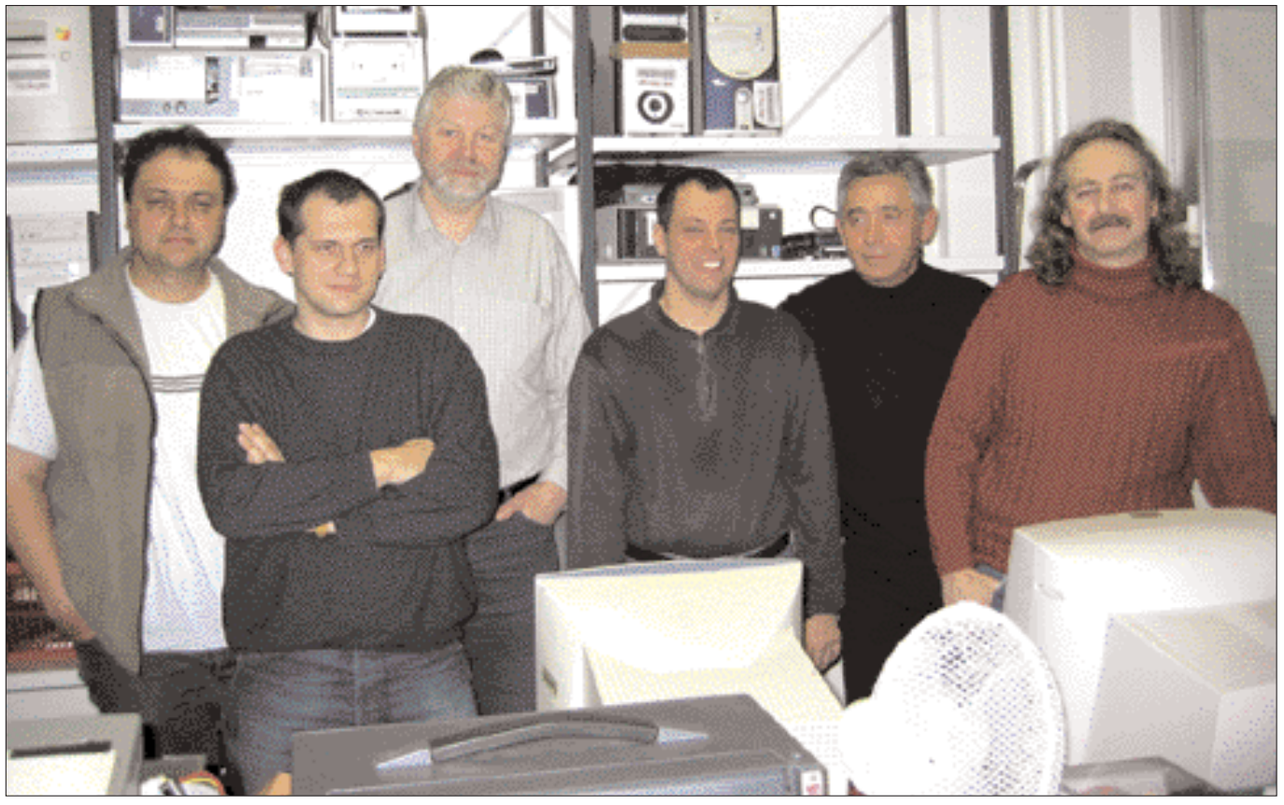


Heikle Missionen auf digitalen Spurenträgern: die Datensicherungsgruppe der Wiener Kriminaldirektion 3.

FOTO: G. BRENNER

Spuren auf Chips und Boards

Computer, CDs, Handys & Co können bei fast jedem Delikt eine Rolle spielen. Mit der Zunahme an Elektronikvarianten und Datenmengen wird die Arbeit schwerer für die Datensicherer.

Mindestens fünf Mädchen im Alter von 12 bis 14 Jahren soll ein 45-jähriger Wiener bis zum Sommer 2004 zu „Sexspielen" in einen Bus gelockt haben. Seine 18-jährige Freundin soll die Kinder mit einem Pudel angelockt und zu ihm gebracht haben. Als eines der Opfer Anzeige erstattete, bekamen die Kriminalisten des Kriminalkommissariats (KK) Zentrum-Ost (Gruppe Deuschlinger) in Wien vage Personenbeschreibungen, eine ungefähre Beschreibung des Busses, in den die Mädchen gelockt worden waren, sowie den Hinweis, dass die 18-Jährige auf dem Weg zu dem Bus an einer Tankstelle ausgestiegen sein sollte.

„Wir haben von dem Tankstellenpächter die Videodaten aus der Überwachungskamera bekommen", schildert der leitende Kriminalbeamte Günther Matjazic. Die Sicherung und Auswertung musste die Polizei vornehmen – der Tankstellenpächter hätte sonst einen kostenpflichtigen Dienst bezahlen müssen. Hier kamen die Beamten der Datensicherungsgruppe der Kriminaldirektion 3 (KD 3) zum ersten Mal in diesem Fall ins Spiel: Sie werteten die digitalen Videoaufnahmen aus und lieferten den Beamten des KKs den fertigen Film und Bilder der Verdächtigen.

Mit Hilfe der Bilder gelang es den Kriminalisten des KKs, zwei Verdächtige auszuforschen. Doch der Mann hatte alle Spuren beseitigt – fast alle. Eines der Opfer erinnerte sich, es sei gefilmt worden. Auch daran hatte der mutmaßliche Sexualtäter gedacht: Er hatte die SIM-Karte verschwinden lassen und die Foto- und Filmdateien von seinem Handy gelöscht. Die Kriminalisten des KKs suchten erneut Rat bei ihren Kollegen aus der KD 3. Diese zauberten aus dem Datenträger im Handy die „Kronzeugen" des Falles: Video- und Fotoaufnahmen des 45-jährigen Beschuldigten. Er wurde zu acht Jahren Haft verurteilt; seine Komplizin zu einem Jahr. Die Urteile sind noch nicht rechtskräftig.

„Als wir Mitte der neunziger Jahre mit der Datensicherung begonnen haben, hat es ausgereicht, sich mit einigen Betriebssystemen auszukennen", sagt Gruppenführer Karl Heindl. „Heute sind die Speichermöglichen unbegrenzt. Das hat uns die Arbeit nicht leichter gemacht." Es gibt USB-Sticks in allen Variationen: MP3-Player, Schlüsselanhänger, Diktiergeräte. Uhren sind mit MP3-Player-Chips ausgestattet – die Dateien dafür bekommen sie über Blue-Tooth drahtlos per UV-Licht zugeschickt. „Auf einen Datenträger, auf dem ich einen MP3-Song speichern kann, übertrage ich auch jede andere Datei", erklärt Datensicherer Hermann Pretz.

Speicherkarten sind in unzähligen elektronischen Geräten verwendbar: Der Chip im Handheld kann in der Kamera verwendet werden, man kann Daten herunterladen und in einem Diktafon zwischenspeichern; kann die Daten mit der Karte dann auf ein Handy laden, von dort verschicken oder direkt in einen PC eingeben. „Die Möglichkeiten sind grenzenlos", sagt Karl Heindl. „Wir als Polizisten dürfen keine ausschließen oder vergessen."

In einem Fall hatte ein Verdächtiger den gesuchten Datenträger in der Brust-

tasche seines Hemdes stecken – ein schwarzes Plastikgehäuse, das genauso gut ein Taschenrechner sein hätte können, auch vom Gewicht her.

Hinzu kommen die immer größer werdenden Speicherkapazitäten. Waren vor zehn Jahren Computerfestplatten mit 500 Megabyte im Speicher der letzte Schrei, so sind es heute 300 Gigabyte. Während sich ein Normalhaushalt vor zehn Jahren höchstens einen PC leisten konnte, steht heute fast in jedem Zimmer ein leistungsfähiges Gerät aus dem Diskontmarkt und im Keller sowie am Dachboden dümpeln ausrangierte PCs vor sich hin – jeder Datenträger ist für Kriminalisten ein potenzielles Versteck. „Das bedeutet für uns: Wir brauchen immer länger, die Dateien zu sichern und auszuwerten“, erklärt Heindl.

Von jedem beschlagnahmten Datenträger fertigen die Kriminalisten eine Sicherungskopie an, bevor sie ihn auswerten. Das Originalmedium bleibt unberührt. Damit ist gewährleistet, dass die Beamten während des Auswertens keine sichergestellten Dateien beschädigen oder verändern. Eine 200-Gigabyte-Festplatte zu sichern, kann bis zu zehn Stunden dauern – je nach Leistungsfähigkeit des Rechners. „Wir arbeiten hauptsächlich auf zwei Arten: Entweder wir beschlagnahmen die Datenträger – dann nehmen wir in der Dienststelle eine forensische Beweissicherung vor, oder wir arbeiten am Ort der Hausdurchsuchung am ‚lebenden‘ Computer“, erläutert Heindl. Manche Firmen wären ohne Computer-Netzwerk nicht betriebsfähig; und oft sind die Server so groß, dass sie nicht beschlagnahmt und mitgenommen werden könnten. „In solchen Fällen sind wir außerdem auf den EDV-Verantwortlichen der betroffenen Firma angewiesen“, sagt Heindl. „Er kennt die Zugriffsrechte, weiß, wo welche Daten sind.“ Für die Ermittler wäre es unmöglich, sich allein zurecht zu finden.

Karl Heindl: Speichermöglichkeiten sind unbegrenzt.

In solchen Fällen suchen Ermittler, Datensicherer und der Systemverantwortliche des betreffenden Unternehmens nach den Daten. „Wir sind Serviceleister für die ermittelnden Kollegen“, sagt Karl Heindl. „Sie wissen vom Akt her, wonach wir suchen sollen.“ Nicht genug wäre es, sich auf einen Datenexperten ohne kriminalistische Kenntnisse zu verlassen.

„Ein Nichtkriminalist denkt anders“, erklärt Heindl. „Ein Kriminalist sieht auch nach, was hat der Verdächtige mit Chatprogrammen gemacht, oder mit welchen Adressen war er im Internet in Kontakt.“ Die Kriminalbeamten sichten nicht nur die Daten, sie stellen fest, welche Programme geladen sind. Dadurch bringen sie in Erfahrung, ob es dem Verdächtigen möglich war, größere Datenmengen über FTP weiterzugeben. Das etwa geschieht in Hinblick darauf, ob ein Besitzer von Kinderpornografie mit verbotenen Bildern und Videos auch gehandelt hat – was den Strafrahmen erhöht.

Pro Jahr sind die Spezialisten der KD 3 bei etwa 50 Hausdurchsuchungen dabei, um Datenträger selbst zu beschlagnahmen oder an Ort und Stelle auszuwerten. In den meisten Fällen handelt es sich um Wirtschaftsdelikte. „In den Anfängen waren wir drei- bis viermal pro Woche bei Hausdurchsuchungen dabei“, erzählt Heindl. „Heute sind die ermittelnden Kollegen so weit, dass sie selber PCs und Datenträger sicherstellen können, ohne Daten zu lö-

FOTO: BRENNER

schen. Und wir können uns in der Dienststelle auf die Auswertung konzentrieren."

Bei der „forensische Beweissicherung" wird die gesamte Festplatte ausgelesen – auch gelöschte Daten. Die meisten Computer speichern die Daten über die ganze Festplatte verstreut nach Zufall. Ein PC-Benutzer, der ein Datenstück in den Papierkorb verschiebt und auf „Papierkorb entleeren" klickt, hat die Festplatte noch lange nicht sauber gewischt. Erst wenn der Computer die Datei – zufällig – überschrieben hat, ist sie weg. Die Kriminalisten der Datensicherung finden solche Datenstücke auf und machen sie wieder sichtbar.

„Es ist eine Grobsichtung", sagt Fritz Breitsching. „Welche Daten benötigt werden, wissen nur die Ermittler. Wir kennen den Ursprung, warum ein Rechner beschlagnahmt worden ist. Die ermittelnden Kollegen kennen beispielsweise in der Kinderpornografie die Spruchpraxis der Gerichte – welche Aufnahmen strafbar sind und welche nicht." In einem Fall entdeckte Breitsching auf einem Computer 170.000 Bilddateien, bei 70.000 davon hatte er den Verdacht, dass es sich um Kinderpornografie handelte. Er bereitete die

FOTO: BRENNER

Hermann Pretz: Kaum ein Delikt ohne Datenspuren.

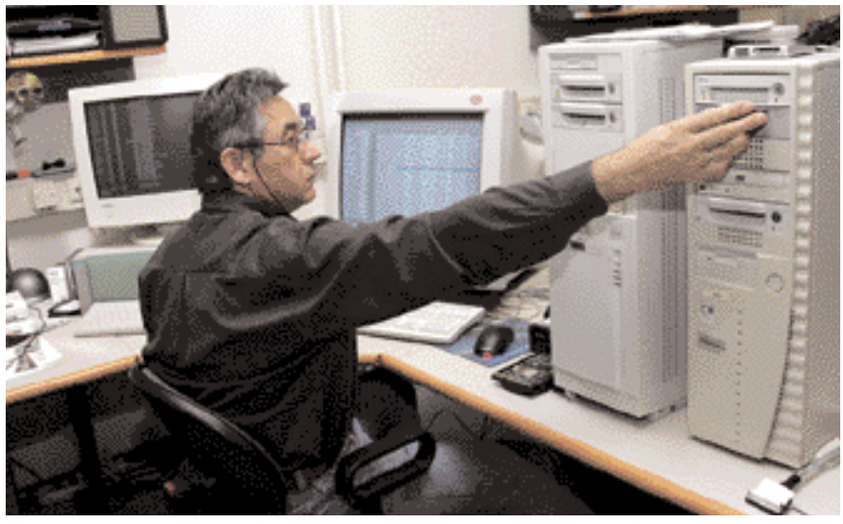
Daten auf, die genaue Sichtung mussten die Kriminalisten der Kriminaldirektion vornehmen.

„Oft kommt es vor, dass wir Beweise für einen Betrug auf Datenträgern suchen und Kinderpornografie aufdecken", berichtet Pretz. Auch der umgekehrte Fall komme vor. In einer Ermittlung wegen Kinderpornografie entdeckten die Kriminalisten in den E-Mails des Verdächtigen seltsame Anlageangebote. Die Beamten regten bei den Ermittlern an, gegen den Mann auch wegen Betrugs zu erheben. „Es gibt kaum ein Delikt, weswegen wir noch keine Datenmedien durchsucht hätten", sagt Pretz.

In einem Mordfall nahmen die Ermittler der KD 1 bei der Hausdurchsuchung nur „der Vollständigkeit halber" den Computer des Verdächtigen mit. Die Datensicherer der KD 3 fanden heraus, der Mann hatte im Internet recherchiert, wie Mordanschläge als Haushaltsunfälle getarnt werden und wie Sprengfallen gebastelt werden könnten. Diese Erkenntnisse stellten ein Mosaikstück in der Beweisführung dar.

In einer Brandermittlung deckten die Datensicherer ein falsches Alibi des Hauptverdächtigen auf. Ein Funktionär eines Klubs hatte das Vereinslokal in Brand gesteckt, weil er Geld unterschlagen hatte. Der Kriminalpolizei gegenüber behauptete er, er sei zum Tatzeitpunkt zu Hause vor dem PC gesessen. Als Beweis dafür legte er eine Sendebestätigung seiner E-Mailadresse vor. Die Kriminalisten der Datensicherung wiesen ihm nach, dass der PC die E-Mail automatisch versendet hatte – zu dem Zeitpunkt, den er programmiert hatte.

In einem anderen Fall überführten sie einen Handy-Hehler. Der Mann war erwischt worden, als er ein Handy verkaufen wollte. In seiner Wohnung fanden die Kriminalisten einen PC vor und beschlagnahmten ihn. Den Datensicherern gelang es, die Protokolle eines Programms aufzudecken, mit dem der Hehler die Handys „entsperrt" hatte. Handys, die mit einer Erstanmeldung gekauft werden, werden ausschließlich für den Netzbetreiber (z. B. *Mobilkom*) freigeschaltet, bei dem die Erstanmeldung erfolgt. Am Schwarzmarkt gibt es Programme, die Handys „entsperren",



Datensicherung: Mit der Zunahme an Elektronikvarianten und Datenmengen wird die Arbeit schwerer für die Spezialisten.

damit auch die SIM-Karten anderer Netzbetreiber im Handy funktionieren.

Das Programm des Handyhehlers protokollierte allerdings mit, welches Handy mit welcher IMEI-Nummer wann entsperrt worden war. Jedes Handy ist mit einer IMEI-Nummer gekennzeichnet, die weltweit einzigartig ist. Mit Hilfe dieser Nummern erhielten die Ermittler eine Liste mit Dutzenden Handydiebstahlsopfern.

„Wenn Sie dieses Kochrezept herunterladen wollen, müssen Sie nur noch ein Zugangstool auf ihrem Computer installieren – klicken Sie auf DOWNLOAD." Wer das befolgte, bekam unbemerkt ein „Dialer"-Programm auf den PC geladen, der die Internetverbindung auf eine kostenpflichtige Nummer umleitete und binnen Minuten Hunderte Euro Telefonkosten verursachte.

„Wenn wir beweisen wollen, dass der Geschädigte den Dialer unbemerkt auf den PC gespielt bekommen hat, müssen wir den Vorgang selber starten, um die Betrugsabsicht nachzuweisen", erklärt Breitsching. Die Behördenleitungen der Polizei blocken aber den Einwahlknoten (Mehrwertnummer) ab – egal, ob ihn jemand absichtlich laden würde oder unabsichtlich.

Die Computerauswertung kann mehrere Wochen in Anspruch nehmen. „Wir müssen Prioritäten setzen", sagt Karl Heindl. „Haftakten werden sofort erledigt, ebenso Fälle, in denen ein Kollege die Ergebnisse braucht, damit er weiterermitteln kann." Von den 200 Akten, die die Datensicherer jährlich bearbeiten, geht es in jedem zweiten Fall um Kinderpornografie.

Spezialwerkzeuge. „Manchmal müssen wir vor Hausdurchsuchungen erheben, wo ein Server physisch steht", erläutert Fritz Breitsching. „Dazu setzen wir sowohl Standardwerkzeuge der Betriebssysteme ein, als auch Hilfsprogramme aus dem Netzwerkbereich." In der Regel kann dadurch der Standort eingegrenzt werden. Auch dazu benötigen die Kriminalisten einen eigenen anonymen Internet-Zugang.

„Der anonyme und unbeschränkte Internetzugang ist das Standardwerkzeug für die Datensicherer, ohne den heute der Kampf gegen die Computerkriminalität aussichtslos wäre", sagt Hermann Pretz, „denn der Ermittler kann nur mit den gleichen Waffen arbeiten wie sein kriminelles Gegenüber."

Für die „forensische" Auswertung von Datenträgern stehen den Kriminalisten eigene Programme zur Verfügung. Diese legen alle Daten offen, die sich irgendwo auf der Festplatte befinden – auch wenn sie in den Papierkorb befördert und gelöscht worden sind. Damit nichts unabsichtlich verändert wird, schalten die Kriminalisten einen „Hardwareblocker" zwischen den beschlagnahmten Computer und den Arbeitscomputer. Der „Hardwareblocker" verhindert den Schreibzugriff auf die Festplatte, die zu untersuchen ist. Es gibt Softwarelösungen – sie sind aber langsamer.

Ob ein PC durch Ziehen des Netzsteckers beschlagnahmt wird oder auf normalem Weg heruntergefahren werden kann, hängt vom Fall ab. „Wenn es zum Beispiel in einem Erpressungsfall darum geht, eine kleine Datei zu sichern, beispielsweise einen Drohbrief, dann wäre der Steckerzug die beste Lösung", sagt Datensicherer Breitsching. „Wenn Gefahr besteht, dass durch die harte Maßnahme Teile des Computers oder eine geöffnete Datenbank kaputt gehen, wäre ich für's ordnungsgemäße Herunterfahren." Entschieden werden müsse das in jedem Einzelfall.

FOTO: F. GERMADNIK

ELEKTRONIKMARKT

Hardware

Der Hardware-Markt wird immer unübersichtlicher, der Software-Markt ebenso. Ermittlungswerkzeuge, mit deren Hilfe die Daten ausgelesen werden können, hinken hinterher. „Deshalb ist es wichtig, dass bei der Sicherstellung von Datenträgern, wie externe Laufwerke, Handhelds oder Handys, auch das Zubehör, Beschreibungen und Handbücher beschlagnahmt werden", sagt Datensicherer Fritz Breitsching. „Bei dem Tempo, das der Elektronikmarkt hat, können wir maximal sechzig Prozent der aktuellen Hardwarekomponenten kennen." Auch Adapterkabel sollten sichergestellt werden, die beispielsweise einen exotischen Stecker an einem Gerät USB-tauglich werden lassen.

Sichergestellte Handys sollten nicht abgeschaltet werden. „Wenn uns der Verdächtige den PIN nicht verrät, mit dem es eingeschaltet wird, wird es schwierig für uns", sagt Breitsching. Auch Ladegeräte sollten die Kriminalisten bei Hausdurchsuchungen nicht vergessen. „Wir haben nicht jedes Ladegerät und nicht jeden Akku für jedes Handy oder jedes Notebook in der Dienststelle."

In manchen Fällen können sich die Datensicherer helfen, indem sie die Festplatte ausbauen und in einem anderen Gerät starten. „Bei einem bestimmten Notebook lässt sich die Festplatte nur im Originalrechner mit Passwort starten", sagt Breitsching. „Selbst der Hersteller behauptet, dass er nur mit dem Passwort und dem Originalrechner auf die Daten zugreifen zu kann."

Breitsching rät, im Zweifelsfall mehr zu beschlagnahmen, als auf den ersten Blick notwendig scheint. „Es ist uns selbst schon passiert, dass wir ein Laufwerk mitgenommen haben, das leer und nutzlos war", schildert er. „In anderen Fällen war es so, dass wir vermutet haben, es sei leer – bei genauem Hinsehen haben wir festgestellt, dass die CD-Rom mit den gesuchten Daten noch drinnen gesteckt ist."