

# Verräterische Magnetspuren

Speicher von Computern, Digitalkameras oder Kopierern werden meist unzureichend gelöscht – vertrauliche Daten lassen sich leicht rekonstruieren.

**J**e schlauer die Geräte werden, desto dümmer stehen bisweilen ihre Benutzer da. In Norwegen zum Beispiel dachte ein Angestellter, er sei ganz besonders gerissen. Bevor er bei seiner Firma kündigte und zur Konkurrenz wechselte, vervielfältigte er noch schnell vertrauliche Unterlagen am Bürokopierer. Obwohl er keine sichtbaren Spuren hinterließ und niemand ihn dabei beobachtete, wurde er verpöffen – vom Kopierer, der den Vorgang in seinem Speicher festhielt.

Svein Willassen kennt Dutzende solcher Anekdoten. Täter, die über die Tücken der Technik stolpern, sind sein Alltag – Willassen ist Datendetektiv. Der 30-jährige Informatiker leitet das fünfköpfige Computer-Forensik-Labor der norwegischen Firma Ibas. Bislang bestand seine Aufgabe nur darin, in kniffligen Fällen die Festplatten nach verräterischen Spuren zu durchforsten. Doch neuerdings untersucht er immer häufiger noch andere Alltagsgegenstände wie Digitalkameras, Faxgeräte oder Handys; denn diese sind von ihren Komponenten her auch nur verkappte Computer.

„Fast alle Digitalgeräte haben einen Speicher“, sagt Willassen, „und wo ein Speicher eingebaut ist, finden sich meist auch irgendwelche Spuren alter Dateien.“ In schwierigeren Fällen untersucht er die ausgebauten Speicher sogar in der staubfreien Atmosphäre eines „Reinraums“, um die verletzlichen Datenspuren nicht zu gefährden. Sein bester Verbündeter aber ist der Leichtsinn: Die meisten Nutzer behandeln ihre Digitalgeräte immer noch so, als wären es mechanische Werkzeuge ohne Langzeitgedächtnis.

Computer zum Beispiel werden meist völlig achtlos entsorgt oder weiterverkauft, ohne Rücksicht auf Intimsphäre oder Datenschutz. Rund 90 Prozent aller gebrauchten Festplatten sind wahre Datenschleudern. Zu diesem erschreckenden Ergebnis kommt der Sicherheitsexperte Simson Garfinkel am Massachusetts Institute of Technology bei Boston. Mit seinem Team hatte Garfinkel wahllos gebrauchte Computerfestplatten zusammengekauft. Fazit:



Datenrettung im Reinraum: Werkzeuge mit Langzeitgedächtnis

Von 158 waren 146 nicht sachgemäß gelöscht worden. Garfinkel rekonstruierte Liebesbriefe, pornografische Bilder, Kreditkartennummern, Patientendaten. Sogar die Festplatte eines Geldautomaten war mit dabei – mit Kontoständen und Kontonummern.

„Viele Computernutzer machen sich Sorgen über Datenpiraten im Internet“, wundert sich Garfinkel, „aber auf ihrer eigenen Festplatte halten sie sich nicht einmal an die einfachsten Regeln der Datenhygiene.“

In Deutschland sieht es nicht besser aus, mahnt Bettina Sokol, die Datenschutzbeauftragte von Nordrhein-Westfalen. Anlass für ihre Warnung ist ein Aufsehen erregender Fall: Auf der ausgemusterten Fest-

platte eines Behördencomputers hatte der Käufer Daten eines Nachlassregisters gefunden.

Einer der Gründe für den ungewollten Daten-Exhibitionismus ist die Begriffsverwirrung um das Wörtchen „Löschen“: Wer per Mausclick eine Datei „löscht“, entfernt in Wahrheit nicht deren Daten, sondern ändert lediglich den Verweis, wo sie auf der Festplatte zu finden sind. Sie lassen sich weiterhin auslesen mit Datenrettungsprogrammen (siehe Grafik).

Um Dateien tatsächlich vollständig zu löschen, müssen sie mehrfach mit neuen Daten überschrieben werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet dafür ein entsprechendes Überschreibprogramm na-

## Schwierigkeiten beim Löschen vertraulicher Daten

### DAS PROBLEM

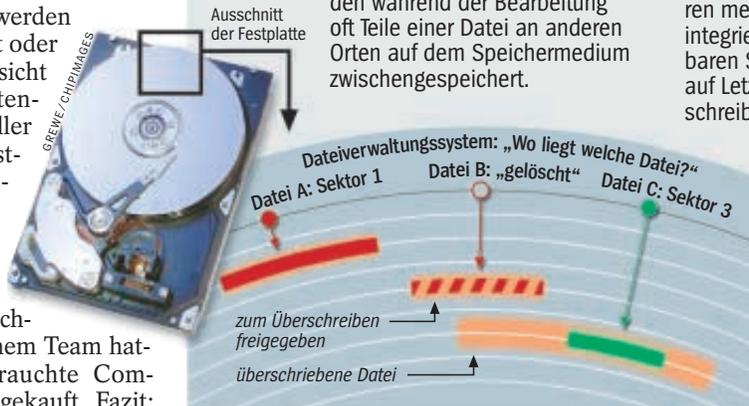
- ▶ Beim **normalen „Löschen“** einer Datei wird lediglich ein Eintrag im Dateiverwaltungssystem („Inhaltsverzeichnis“) geändert. Die Datei wird damit zwar zum Überschreiben freigegeben, aber nicht entfernt.
- ▶ Auch das **einmalige Überschreiben** einer einzelnen Datei garantiert nicht ihr Verschwinden. Denn eine Restmagnetisierung bleibt erhalten und kann von Spezialisten ausgelesen werden. Außerdem werden während der Bearbeitung oft Teile einer Datei an anderen Orten auf dem Speichermedium zwischengespeichert.

### BETROFFENE GERÄTE neben Computern

- ▶ **Fotokopierer, Faxgeräte, Scanner, Drucker** verfügen heutzutage häufig über Festplatten als Zwischenspeicher. Eine spezielle Lösch- oder Überschreibfunktion gibt es meist nicht.

- ▶ **Digitalkameras, MP3-Player, PDAs, Diktiergeräte** funktionieren meist mit einer Mischung aus fest integriertem Speicher und auswechselbaren Speicherkarten. Zumindest auf Letzteren ist das sichere Überschreiben am PC möglich.

- ▶ Moderne **Mobiltelefone** verfügen über immer größere interne Speicher für Fotos, Adressen und SMS. Das sichere Entfernen der Daten ist schwierig.



mens „VS-Clean“ an ([www.bsi.de](http://www.bsi.de)) – eine Methode, an der sich Büros der öffentlichen Verwaltung orientieren, wenn es um die Entsorgung ausgemusterter Geräte geht.

„Eigentlich müsste jedes Gerät einen kleinen roten Knopf haben, mit dem sich alle Daten nachhaltig entfernen lassen“, meint der Datendetektiv Willassen. Bislang existiert ein solcher Amnesie-Knopf für Computer aber nur in der Phantasie.

Und selbst das vom BSI empfohlene Standardlöschverfahren biete nur trügerische Sicherheit, kritisiert Roy Pfitzner, Fachmann für Computersicherheit beim Brandenburgischen Innenministerium, in einer bislang unveröffentlichten Studie. „Viele Bereiche der Festplatte werden dadurch nicht umorientiert“, heißt es in dem brisanten Papier, das auch dem BSI vorliegt.

Hintergrund der Meinungsverschiedenheit: Während das BSI für alltagstauglichen Schutz gegen Normalhacker eintritt, fordert Pfitzner maximale Sicherheit, die auch Geheimdiensten trotzen würde.

„Datenrettung funktioniert ein bisschen wie Archäologie“, erläutert Pfitzner. „Schicht für Schicht kann ich mit Filterprogrammen die alten Daten herauspräparieren – auch wenn eine Festplatte 20-mal überschrieben worden ist.“ Denn jeder Speichervorgang hinterlässt ganz reale, physische Spuren aus Restmagnetismus auf dem Trägermedium – Daten sind eben doch nicht so immateriell, wie gern angenommen wird.

„Um einen Datenträger richtig zu löschen, reicht auch VS-Clean nicht aus“, sagt Pfitzner, „dazu müsste man die Festplatte tiefenlöschen.“ Tiefenlöschen bedeutet, dass Festplatten mit eigens errechneten Zufallszahlen überschrieben werden – „über 30-mal“, so Pfitzner. Andere Experten meinen, dass auch zehn Löschvorgänge reichen würden. Unstrittig ist: Eine solche Prozedur kann bei großen Festplatten mehrere Tage dauern.

Wenn es um wirklich wichtige und sensible Daten geht, raten Experten daher zu anachronistischen anmutenden Brachialmethoden: physische Vernichtung durch Zerschneiden, Verbrennen, Schreddern.

Wirklich praktikabel ist dies aber auch nicht. Fast jedes Elektronikgerät verfügt heute über irgendeine Form von Speicher. Aber nur in den seltensten Fällen lässt dieser sich einfach und preiswert austauschen. Eine Flut immer klügerer Geräte unterhöhlt den Datenschutz weiter.

„In letzter Zeit untersuchen wir zunehmend Drucker, Faxgeräte, Digitalkameras

und Handys“, bestätigt der Datendetektiv Willassen. Kürzlich löste er etwa den Fall eines Selbstmörders, der keinen Abschiedsbrief hinterlassen hatte. Weil die Familie unbedingt wissen wollte, warum der Mann sich umgebracht hatte, beauftragte sie Willassen.

Er befragte den einzigen Zeugen – das Handy des Selbstmörders. Willassen las aus dem Handy-Speicher alte, „gelöschte“ SMS-Nachrichten aus. Dabei stieß er auf feindselige Botschaften von der Ex-Freundin des Selbstmörders. Offenbar war Liebeskummer das Motiv für den Freitod.

Neuerdings untersucht Willassen zudem Digitalkameras, zum Beispiel, weil deren Nutzer versehentlich Bilder „gelöscht“ haben. Er wurde auch schon von der Kriminalpolizei beauftragt, um Produzenten von Kinderpornografie anhand ihrer Tatwerkzeuge zu überführen.

Vor allem aber Kopierer stellen mittlerweile ein massives Datenschutzproblem dar, erklärt der Sicherheitsspezialist Andreas Marx.

Speziell Leasing-Kopierer, die regelmäßig ausgetauscht und an andere Firmen weitergegeben werden, seien ein Einfallstor für Wirtschaftsspionage: „Meist läuft es darauf hinaus, dass die Serviceteams nur die Funktionsfähigkeit checken, nicht aber überprüfen, welche Dokumente noch gespeichert sind. Wenn sie das tun, finden sie alles Mögliche: Rechnungen, Handbücher, Briefe vom Finanzamt.“

Zumindest ein Hersteller hat auf das bislang fast

unbekannte Spionagerisiko reagiert: Sharp bietet neuerdings Kopiergeräte an, die zumindest bereits über einige Schutzmechanismen verfügen. So werden die Daten auf der Festplatte verschlüsselt abgelegt, und ein spezielles Löschmodul über schreibt bei Bedarf die Festplatte bis zu siebenmal.

Doch für Datendetektive wie Willassen sind auch derlei Sicherheitsbarrieren keine unüberwindbare Hürde: Der Kopierer hat lediglich das Sicherheitszertifikat „EAL2“, maximal möglich wäre „EAL7“. Im Klartext: Fachleute und geübte Hacker könnten relativ leicht rekonstruieren, was mit dem Gerät alles kopiert worden ist.

„Meine tägliche Arbeit beweist, wie katastrophal es um den Datenschutz steht“, sagt Willassen, „die meisten Nutzer haben einfach keine Ahnung, was ihre Geräte alles über sie verraten.“

Warum der Datendetektiv das alles so freimütig erzählt? Die Firma Ibas, bei der er arbeitet, bietet nicht nur das Rekonstruieren von Daten an. Sondern auch die professionelle Löschung.

HILMAR SCHMUNDT



KRISTOFFER EILASSEN

**Datendetektiv Willassen**  
*Liebeskummer als Motiv*