Daten löschen, aber richtig

SICHERHEIT. *Gängige Löschprozeduren bieten kaum Schutz vor Datenspionage.*

VON CHRISTIAN ZWITTNIG

Schlampig gelöschte Daten auf der Festplatte lassen sich auch von Laien leicht wieder rekonstruieren. [Begsteiger]

Wem ist das nicht schon einmal passiert: Ein falscher Knopfdruck und plötzlich ist eine wichtige Datei weg. So etwas ist ärgerlich, aber mit regelmäßigen Sicherungskopien kein Malheur.

Wirklich unangenehm kann aber der umgekehrte Fall werden: Daten, die eigentlich gelöscht sein sollten, tauchen wieder auf. Ein spektakulärer Fall aus dem Vorjahr: Ein Student aus Potsdam ersteigert eine Festplatte auf eBay. Nach Wiederherstellung der Daten findet er darauf Alarmpläne für Geiselnahmen, Namenslisten von Krisenstäben und Einsatzbefehle. Er spielt die Festplatte einem Nachrichtenmagazin zu. Es stellt sich heraus, dass die Festplatte vom Landeskriminalamt versehentlich versteigert worden ist und streng vertrauliche Polizeidaten enthielt.

Dass dieser Fall keine Ausnahme darstellt, bestätigt Nicolas Ehrschwendner von der Datenrettungsfirma Attingo: „Wir gehen davon aus, dass 90 Prozent der gebrauchten Festplatten, die weiterverkauft werden, nicht korrekt gelöscht wurden." Aber nicht nur unwissende Privatanwender verkaufen volle Festplatten. Auch Konzerne und Behörden gehen oft allzu sorglos mit ihren Daten um. „Die Vernichtungskosten dürften dabei eine Rolle spielen", vermutet Ehrschwendner.

Löschvorgänge verstehen

Dabei braucht es kein Computergenie, um eine Festplatte gründlich zu säubern. Wichtig ist es aber, die Unterschiede zwischen den verschiedenen Löschvorgängen zu verstehen: Werden Daten in den Papierkorb gezogen oder der Datenträger formatiert, gibt das System lediglich den belegten Speicherplatz zum Überschreiben frei. Wirklich gelöscht werden die Daten damit nicht: Sie sind zwar für das System unsichtbar, Spezialprogramme können aber problemlos darauf zugreifen. Werden die freien Stellen der Festplatte hingegen mit Nullen oder Zufallsinformationen überschrieben, sind die Daten ziemlich sicher vernichtet: Nur wenige Spezialfirmen weltweit sind in der Lage, überschriebene Dateien wieder herzustellen. Wobei die Kosten hierfür je nach Festplattengröße bis zu hunderttausend Euro ausmachen können. Die Software zur Datenvernichtung hingegen ist oftmals gratis im Internet erhältlich.

Notebooks schützen

Im Gegensatz zu Standgeräten, wo erst gelöscht werden muss, wenn Gerät oder Datenträger den Besitzer wechseln, empfiehlt es sich, bei Notebooks schon früher vorzusorgen: Sollte das Gerät abhanden kommen, bietet das Windows-Kennwort kaum Schutz. Die meisten Notebooks verfügen aber standardmäßig über die Funktion, ein Festplatten-Kennwort im System-BIOS zu setzen (nicht zu verwechseln mit dem normalen BIOS-Kennwort, das leicht gelöscht oder durch Ausbauen des Datenträgers umgangen werden kann). Da dieses Kennwort auf der Festplatte selbst gespeichert ist, führt kein Weg daran vorbei. Der Haken dabei: Wenn das Passwort vergessen wird, dann bleibt der Bildschirm schwarz. In solchen Fällen kann nur mehr ein professioneller Datenretter helfen.

Alternativ zum Festplattenkennwort können mobile Daten auch durch Echtzeitverschlüsselung effektiv vor unbefugtem Zugriff geschützt werden. Der Vorteil besteht darin, dass zumindest der Computer betriebsfähig bleibt, auch wenn das Passwort verloren gegangen ist. Höhere Sicherheit bietet aber in jedem Fall das Festplattenpasswort, da bei Verschlüsselungssoftware immer wieder Sicherheitslücken auftauchen.

Welche Methode ist die beste?

Jede Methode, seine Daten vor fremdem Zugriff zu schützen, hat ihre Schwachstellen. Daher muss von Fall zu Fall entschieden werden, welche die geeignetste ist. Ausschlaggebend ist, wie wichtig die gespeicherten Daten sind. Soll wirklich jede Möglichkeit der Wiederherstellung ausgeräumt werden, kann der Speicher auch bei einer Datenvernichtungsfirma physikalisch zerstört werden. Ob die Festplatte dabei geschreddert, verbrannt oder entmagnetisiert wird, ist nebensächlich. In jedem Fall sind die Daten Geschichte. Der Datenträger allerdings auch.

PORENTIEFE Reinigung

Nur mit spezieller Lösch- und Verschlüsselungssoftware kann man das Ausspionieren von Daten verhindern. Viele Programme sind gratis.

Eraser: www.heidi.ie/eraser, Löschsoftware, gratis.

CyberShredder: www.cylog.org/utils_9.asp, Löschsoftware, gratis.

PGP® Desktop Home: www.pgp.com/de, Paket für Datenlöschung und -verschlüsselung, rund 100 €.