

Sind Ihre Daten wirklich gelöscht?

Sie wollen Ihren alten Computer verschenken, verkaufen oder entsorgen? Sie haben vorher alle Dateien mit Ihren persönlichen Daten sowie die selbst installierte Software von der Festplatte gelöscht? Sie haben auch den Windows-Papierkorb geleert? Oder haben Sie sogar die ganze Festplatte formatiert und sind nun völlig sicher, dass alle Daten weg sind? Dies ist ein leider weit verbreiteter Irrtum!

➤ Werden Daten von einer Festplatte (oder Diskette) nur mit dem herkömmlichen Löschbefehl gelöscht, sind sie im Allgemeinen leicht wiederherstellbar. Gleiches gilt auch beim Formatieren.

Immer wieder wird über die erfolgreiche Rekonstruktion von sensiblen Daten auf vermeintlich gelöschten Festplatten berichtet. So fanden Forscher 2003 in den USA unter 158 gebrauchten Festplatten nur 12 ohne wiederherstellbare Datenspuren. Auf den anderen Festplatten konnten medizinische Daten, Kreditkarten- und Kontoinformationen oder private Briefe rekonstruiert werden. Eine schwedische Studie aus dem Jahr von 2004 zeigte bei 70% der untersuchten Festplatten verwertbare Datenreste, u.a. von einem großen europäischen Finanzdienstleister.

➤ Vermeiden Sie die Fehler anderer! Verhindern Sie, dass Unbefugte Ihre persönlichen Daten auf alten oder ausgemusterten Festplatten wiederherstellen und missbrauchen können!

Warum reicht das herkömmliche Löschen von Dateien nicht aus?

Alle gängigen Betriebssysteme (z.B. Windows oder Linux) realisieren das Löschen von Dateien wegen der schnelleren Reaktionszeit in der Regel so, dass die zu löschende Datei nur in den Verwaltungsstrukturen des Dateisystems als „gelöscht“ und die von ihr belegten Blöcke als „frei“ markiert werden. Die eigentlichen Daten bleiben so lange unangetastet, bis sie mehr oder weniger zufällig und oft nur unvollständig durch neue Daten überschrieben werden.

Auch beim Formatieren von Festplatten oder einzelnen Festplattenabschnitten (Partitionen) werden die Datenbereiche im Allgemeinen nicht modifiziert. Vielmehr wird nur das Dateisystem eingerichtet (z.B. bei Windows NTFS und FAT32, bei Linux ext3 und ReiserFS), Verwaltungsinformationen in wenige Blöcke geschrieben und ein Oberflächentest durchgeführt.

Das normale Löschen von einzelnen Dateien reicht auch deshalb nicht aus, weil alle Betriebssysteme und die meisten Anwendungsprogramme temporäre Dateien, Arbeits- und Sicherungskopien verwenden (z.B. Textverarbeitungen und Packprogramme) oder Bereiche des Hauptspeichers regelmäßig auf Festplatte auslagern. In diesen besonderen Dateien finden sich auch Duplikate nutzerspezifischer Daten.

Wie die obigen Beispiele zeigen, gelingt es durch die Nutzung spezieller Softwarewerkzeuge zur Datenrettung oder durch Analysetechniken von Speziallaboren relativ häufig, Dateien oder Dateireste erfolgreich wiederherzustellen. Was nach dem versehentlichen und unbeabsichtigten Löschen von Dateien eine willkommene Hilfe ist, kann jedoch von Unbefugten auch missbraucht werden.

Wie können Festplatten sicher gelöscht werden?

Für das sichere, d.h. vollständige und nicht umkehrbare Löschen lassen sich zwei Varianten anwenden:

- physikalische Maßnahmen - mechanische, thermische oder magnetische Zerstörung,
- Löschen durch ein- oder mehrmaliges, gezieltes Überschreiben der Daten.

Zu beachten ist, dass nach der Anwendung der genannten physikalischen Maßnahmen die Festplatte nicht mehr verwendbar ist. Nur nach dem Löschen durch Überschreiben kann sie wieder für Neuinstallationen genutzt werden.

Bei der mechanischen Zerstörung werden die einzelnen Scheiben der Festplatte so weit zerkleinert, dass aus den verbleibenden Resten keine sinnvollen

Informationen mehr gewonnen werden können. Das Pulverisieren oder das Abschleifen der magnetisierbaren Oberfläche sind ebenfalls denkbar. Die thermische Zerstörung besteht darin, das Material einer hohen Temperatur (>750°C) auszusetzen, wobei es seine magnetischen Eigenschaften verliert. Auch das magnetische Durchfluten mit einem starken äußeren Magnetfeld führt zum Löschen aller Daten. Sowohl die thermische als auch die magnetische Zerstörung sind aber nur dann sicher, wenn sie bis ins Innere der Festplatte reichen. Dies kann jedoch meist nicht zuverlässig garantiert werden.

➤ Nutzen Sie physikalische Maßnahmen wie die mechanische Zerstörung zum Löschen defekter Datenträger, die sich nicht mehr mittels Software überschreiben lassen!

Bei der zweiten Variante, dem Löschen durch Überschreiben werden spezielle Softwarewerkzeuge verwendet, die die Festplatte ein- oder mehrfach mit gleichen oder wechselnden Datenmustern oder mit Zufallszahlen überschreiben. Mittlerweile gibt es eine Reihe von Standards und Empfehlungen zur Anzahl der Überschreibvorgänge und zur Art der Daten, mit denen überschrieben wird.

Was ist beim Löschen durch Überschreiben zu beachten?

Wegen der bereits angesprochenen Eigenschaften des herkömmlichen Löschens und der Besonderheiten des Speicherns von temporären Dateien, Sicherungskopien und Auslagerungsdateien ist das Löschen von einzelnen Dateien durch Überschreiben meist mit Risiken verbunden.

➤ Wenn Sie Ihren Computer verschenken, verkaufen oder entsorgen wollen, löschen Sie vorher alle Festplatten bzw. Partitionen, die persönliche Daten enthalten können, vollständig durch komplettes Überschreiben!

Das Löschen einzelner Dateien eignet sich nur dann, wenn sichergestellt ist, dass keine Kopien der Daten

an anderen Orten auf der Festplatte abgelegt wurden oder diese Orte eindeutig bestimmt und auch die Kopien sicher gelöscht werden können. Es ist deshalb nur für versierte Nutzer zu empfehlen.

➤ Überschreiben Sie die zu löschenden Daten mindestens einmal mit Zufallszahlen! Besonders sensible Daten sollten mehrfach mit Zufallszahlen überschrieben werden!

Die Wiederherstellung der Originaldaten mit Software zur Datenrettung ist meist schon nach einmaligem Überschreiben mit Zufallszahlen nicht mehr möglich. Gegen ausführliche Analysen in Speziallaboren mit aufwändiger Technik hilft, die Anzahl der Überschreibvorgänge auf mindestens 7 zu erhöhen.

Noch häufigeres Überschreiben kann sinnvoll sein, um Datenträger mit besonderen Aufzeichnungsverfahren zu löschen. Bei normalen, modernen Festplatten ist es in der Regel jedoch nicht erforderlich.

Welche Programme eignen sich zum Löschen durch Überschreiben?

Für das Löschen durch Überschreiben gibt es eine Reihe frei verfügbarer oder kostengünstiger Löschmodulare. Zwei Beispiele der ersten Gruppe sind:

- **Eraser** (www.heidi.ie/eraser/): überschreibt unter Windows 95 bis XP einzelne Dateien oder Verzeichnisse, temporäre Dateien, Auslagerungsbereiche und den ungenutzten Platz auf der Festplatte. Das separate Programm DBAN löscht ganze Partitionen oder Festplatten.
- **Wipe** (wipe.sourceforge.net): arbeitet unter Linux und kann sowohl einzelne Dateien oder Verzeichnisse als auch ganze Partitionen oder Festplatten überschreiben. Über Programmschalter lässt sich das Verhalten flexibel konfigurieren.

Weitere Programme können der unten angeführten Literatur entnommen werden.

Besser als das nachträgliche Löschen und deshalb in jedem Fall vorzuziehen ist es, wenn persönliche Daten gar nicht erst im Klartext auf der Festplatte abgespeichert werden. Diese Maßnahme schützt auch bei einem Diebstahl des Computers oder der Festplatte vor dem Missbrauch der Daten.

➤ Speichern Sie Ihre persönlichen Daten von Anfang an nur verschlüsselt! Verwenden Sie hierfür verschlüsselte Dateisysteme!

Es sollten mindestens die Verzeichnisse für eigene Dateien, aber auch für temporäre Daten oder Sicherheitskopien verschlüsselt werden. Die aktuellen Versionen der Betriebssysteme Windows und Linux enthalten bereits die erforderlichen Hilfsmittel.

Weiterführende Informationen

- Grunwald: Blitzblank – Sicheres Löschen von Speichermedien. Zeitschrift iX 05/2003, S. 72-78. (www.heise.de/ix/artikel/2003/05/072/)
- Akman, Beier, Brauch: Aber sicher – Verschlüsselung für Windows, Linux und MacOS. Zeitschrift c't 16/2004, S. 176-181.

Haben Sie Fragen oder Hinweise? Schreiben Sie uns oder rufen Sie an!

Der Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon: 033203 / 356 - 0
Fax: 033203 / 356 - 49
E-Mail: Poststelle@LDA.Brandenburg.de
Internet: <http://www.lida.brandenburg.de>

Der Landesbeauftragte
für den Datenschutz
und für das Recht
auf Akteneinsicht



Verräterische Spuren auf Festplatten



Hinweise zum sicheren Löschen von Daten