Sicheres Löschen

Daten endgültig zu löschen ist schwieriger als man denkt, denn Löschen ist nicht gleich Löschen. Die sicherste Lösung – die physische Zerstörung des Datenträgers – ist meist nicht praxistauglich. Doch es gibt Alternativen.

Daten löschen Sie sicher, indem Sie...

- die freigegebenen Datenbereiche auf magnetischen Festplatten oder Datenbändern mit Hilfe von Tools (mehrfach) überschreiben.
- den gesamten Speicherbereich von elektronischen Datenträgern wie USB-Sticks, SD-Karten oder SSD-Festplatten mit Hilfe von Tools einmalig überschreiben.
- ein Smartphone oder Tablet bei aktivierter Geräte-Verschlüsselung auf die Werkseinstellungen zurücksetzen.
- optische Datenträger wie CD-R/RW oder DVD-R/RW physisch zerstören.
- den gesamten Speicherbereich oder sensitive Inhalte von Datenträgern aller Art verschlüsseln und das Schlüsselmaterial vernichten.
- den Datenträger physisch zerstören.

Dateien, die ohne besondere Vorkehrungen gelöscht wurden, können mit entsprechenden Programmen häufig wiederhergestellt werden. Dies liegt daran, dass Daten gar nicht gelöscht, sondern nur mit anderen Daten überschrieben werden können. Die Schwierigkeit liegt allerdings darin, alle Ablageorte zu erwischen.

Um vertrauliche Daten endgültig und unwiederbringlich zu löschen, benötigen Sie deshalb spezielle Tools und ein der Art des verwendeten Datenträgers angepasstes Vorgehen.

Magnetische Datenträger wie Festplatten oder Datenbänder

Spezielle Programme überschreiben den Bereich der Festplatte oder des Datenbands, in welchem sich die zu löschenden Daten befanden mit (sinnlosen) Datenmustern – meist mehrmals. Durch diesen Vorgang sind die Daten unwiderruflich gelöscht.

Auf dem Markt finden sich diverse kommerzielle Programme sowie auch freie Produkte, z.B.:

Windows

- **Eraser**: Download: eraser.heidi.ie (https://eraser.heidi.ie)
- **Secure Eraser**: Eine gute Anleitung (https://www.computerbild.de/artikel/cb-Downloads-Tuning-System-Secure-Eraser-Tipps-Anleitung-5697825.html) finden Sie auf der Internetseite der Zeitschrift Computerbild. Download: www.secure-eraser.com (http://www.secure-eraser.com)

macOS

- **Permanent Eraser**: Download: www.edenwaith.com (http://www.edenwaith.com)

Elektronische Datenträger wie SSD-Festplatten, USB-Sticks oder SD-Karten

Einzelne Dateien auf elektronischen Datenträgern wie USB-Sticks, SD-Karten oder SSD-Festplatten können mit den oben genannten Programmen technisch bedingt nicht zuverlässig gelöscht werden.

Eine Möglichkeit besteht darin, den Datenträger komplett zu überschreiben. Dabei gehen aber sämtliche Inhalte verloren. Alternativ können die Daten verschlüsselt werden (siehe unten).

Smartphones und Tablets

Um in Smartphones und Tablets eingebaute Datenträger endgültig zu löschen, kann das Gerät bei aktivierter Geräte-Verschlüsselung auf Werkseinstellungen zurückgesetzt werden. Doch Vorsicht: Dabei gehen sämtliche Benutzer-Daten verloren!

Android

1. Aktivieren Sie unter **Einstellungen / Sicherheit** die Verschlüsselung des Gerätes und warten Sie deren Fertigstellung ab (kann u.U. lange dauern!)
2. Setzen Sie das Gerät unter **Einstellungen / System / Optionen zum Zurücksetzen** auf Werkseinstellung zurück

iOS

1. Bei aktuellen iOS-Geräten ist die Verschlüsselung standardmässig aktiviert und kann nicht ausgeschaltet werden.
2. Über die Apple-ID bleibt das Gerät auch nach dem Löschen an Sie gebunden. Falls Sie das Gerät weitergeben möchten, müssen Sie daher (vor der Löschung der Inhalte) unter **Einstellungen / Abmelden / Deaktivieren** die Verbindung zu Ihrer Apple-ID löschen.
3. Setzen Sie das Gerät unter **Einstellungen / Allgemein / Zurücksetzen / Alle Inhalte & Einstellungen löschen** zurück.

Eine weitere einfache Möglichkeit, um zumindest den Foto- und Videobereich sicher zu löschen, ist, nach der manuellen Löschung der unerwünschten Inhalte mit der Kamera-App eine «leere» Videoaufnahme mit z.B. auf die Tischplatte gerichteter Kamera zu machen, bis der Speicher voll ist. (Achtung: Der Ton wird dabei auch aufgezeichnet und einzelne Speicherbereiche, wie z.B. Nachrichten werden dadurch u.U. nicht gelöscht, resp. Überschrieben.)

Optische Datenträger wie CD-R/RW oder DVD-R/RW

Optischen Datenträgern wie CD-R/RW oder DVD-R/RW wird hinsichtlich der Datenlöschung oft zu wenig Beachtung geschenkt. Häufig landen sie nach der Benutzung, und mit ihnen auch sensitive Daten, unbesehen im

Abfall.

Eine sichere Datenlöschung ist hierbei technisch oft nicht möglich (CD-R / DVD-R) oder aufgrund des geringen Werts der Datenträger unverhältnismässig (CD-RW / DVD-RW).

Hier ist die physische Zerstörung des Datenträgers zugleich eine sichere wie praxistaugliche Methode.

Physische Zerstörung des Datenträgers

Für Datenträger aller Art stellt die physische Zerstörung eine sichere Methode dar. Zum Beispiel, indem in eine Festplatte ein Loch gebohrt oder ein USB-Stick mit einem Hammer zerschlagen wird, um dessen Speicherchip zu zertrümmern. Eine professionellere und garantierte Abwicklung nach DIN-Norm 66399 wird von kommerziellen Firmen angeboten.

Mit der physischen Vernichtung des Datenträgers wird selbstredend auch der damit zusammenhängende Wert vernichtet. Gerade bei teureren Datenträgern wie grösseren SSD-Festplatten oder bei Geräten mit fest verbauten Datenträgern wie Smartphones oder Tablets ist diese Lösung im Allgemeinen nicht praxistauglich. In solchen Fällen stellt die Datenverschlüsselung eine gute Alternative dar.

Schutz durch Verschlüsselung

Die sicherste und zugleich flexibelste Alternative zu sämtlichen Formen der Datenlöschung besteht darin, schützenswerte Daten zu verschlüsseln und vertrauliche Inhalte damit für Dritte unlesbar zu machen. Im Gegensatz zur Datenlöschung wirkt dieser Schutz während des gesamten Lebenszyklus der Daten und sogar darüber hinaus. Mit der Löschung des Schlüsselmaterials sind nämlich die Daten unwiederbringlich verloren.

Um sicher zu gehen, dass zu keinem Zeitpunkt ungeschützte Inhalte auf einem Datenträger abgelegt werden, sollte der gesamte Datenträger bereits bei der Inbetriebnahme verschlüsselt werden. Auch hierfür existieren verschiedene Programme:

Windows

- **BitLocker** ist eine in den Windows Ultimate / Pro / Enterprise Versionen verfügbare Funktion zur Verschlüsselung ganzer Datenträger.
- **EFS** ist eine standardmässig in Windows eingebaute Funktion des Dateisystems NTFS. Damit lassen sich benutzerspezifisch einzelne Dateien oder Ordner verschlüsseln.
- **VeraCrypt** ist kostenlos, mächtig und einfach zu bedienen. Download: www.veracrypt.fr (https://www.veracrypt.fr)

macOS

- **FileVault** ist eine standardmässig in macOS eingebaute Funktion zur Verschlüsselung von Dateien sowie ganzen Festplatten.
- **VeraCrypt** ist kostenlos, mächtig und einfach zu bedienen. Download: www.veracrypt.fr (https://www.veracrypt.fr)

Eine unwiderrufliche Datenvernichtung erfolgt durch die physische Zerstörung des Datenträgers. Praxistauglicher ist das «Löschen durch Überschreiben» mittels spezieller Programme. Eine Alternative dazu, welche über den gesamten Lebenszyklus der Daten und darüber hinaus wirksam ist, ist deren Schutz mittels Verschlüsselung.

Weiterführende Informationen für Interessierte

Löschen über den Papierkorb oder Formatieren reicht nicht

Bei Computern wird eine Datei beim Löschen normalerweise zuerst in den Papierkorb verschoben. Von dort kann diese Datei bei Bedarf wiederhergestellt oder durch Leeren des Papierkorbes scheinbar definitiv gelöscht werden. Letzteres «löscht» jedoch nicht die eigentlichen Daten, sondern lediglich den Verweis auf die Datei im Verzeichnis. Dadurch wird die Datei für den Benutzer «unsichtbar», und die Bereiche der Festplatte, auf denen sich die zu löschende Datei befindet, zum Überschreiben freigegeben. Die Daten bleiben auf diese Weise also solange bestehen, bis eine andere Datei in den freigegebenen Bereich geschrieben wird.

Ähnlich verhält es sich mit dem Formatieren von Datenträgern. Bei der Schnellformatierung (Quick Format) werden die Verweise auf sämtliche Dateien aus dem Verzeichnis gelöscht. Die Inhalte der Dateien bleiben aber auch bei diesem Vorgang erhalten – wenn auch verwaist.

Effektiver ist die vollständige Formatierung. Hierbei werden bei modernen Betriebssystemen die Speicherbereiche vollständig mit Nullen überschrieben. Damit ist eine Wiederherstellung von Dateien mit vertretbaren Mitteln faktisch ausgeschlossen.

Aus diesem Grund ist es möglich, gelöschte Dateien, welche noch nicht überschrieben wurden, wiederherzustellen. Dies kann sehr hilfreich sein, wenn Sie aus Versehen eine Datei gelöscht haben, die Sie noch benötigen. Aus Sicherheitsgründen, z. B. wenn Sie eine vertrauliche Datei unwiederbringlich löschen möchten, ist dies jedoch nicht erwünscht.

Um eine einzelne Datei oder einen kompletten Datenträger unwiderruflich zu löschen, benötigen Sie unter Umständen spezielle Programme. Der Vorgang hängt dabei von der Art des verwendeten Datenträgers bzw. des darin verwendeten Aufzeichnungsverfahrens ab:

Magnetische Festplatten

Auf magnetischen Datenträgern ist der Ablageort einer Datei genau festgelegt. Spezielle Programme können daher gezielt diesen Bereich der Festplatte ausfindig machen und überschreiben – zur Sicherheit meist gar mehrmals. Durch diesen Vorgang sind die Daten unwiderruflich gelöscht.

Wenn Sie Ihren alten Computer entsorgen oder verkaufen, sollten Sie entweder die Datenträger daraus entfernen oder zumindest vorgängig die Daten auf der Festplatte löschen. Schliesslich möchten Sie nicht, dass der Käufer Ihres Geräts Ihre sensiblen Daten wiederherstellen kann. Am einfachsten benützen Sie hierfür eine bootfähige CD mit entsprechenden Tools, welche die komplette Festplatte überschreiben, z.B. DBAN (https://www.dban.org/) für Windows.

USB-Sticks und SD-Karten

Auf sogenannten Flash-Speichermedien wie USB-Sticks oder SD-Speicherkarten kann ein- und derselbe Inhalt technisch bedingt an mehreren Ablageorten abgelegt sein. Es entstehen dadurch von selbst Kopien. Beim Löschen per Überschreiben wird nur die zuletzt verwendete Kopie gelöscht – die anderen blieben bestehen.

Beachten Sie deshalb, dass eine Datei auf einem Flash-Speicher nur sicher gelöscht werden kann, indem Sie das gesamte Medium unwiderruflich löschen. Einzelne Dateien können auf USB-Sticks und SD-Karten grundsätzlich nicht sicher gelöscht werden.

SSD-Festplatten

Die Dateien auf den in neueren Computern verbauten SSD-Festplatten können mit den genannten Programmen nicht zuverlässig gelöscht werden. Dies ist technisch bedingt: Um eine gleichmässige Abnutzung der Speicher-

zellen zu erreichen, werden die gespeicherten Inhalte von der Festplatte periodisch automatisch umorganisiert. Dadurch entstehen «verlorene» Kopien der Daten, welche nicht gezielt überschrieben werden können. Ein zuverlässiges Löschen durch Überschreiben von Daten ist daher nicht möglich.

Einige Hersteller von SSD-Festplatten bieten eingebaute Funktionen, welche diese verlorenen Daten auf dem Datenträger aufspüren und angeblich endgültig löschen. Die Funktionsweise und Verlässlichkeit dieser Funktionen lassen sich allerdings kaum überprüfen.

Nebst der physikalischen Zerstörung des Datenträgers gilt auch in diesem Fall, dass die sichere Löschung einer Datei nur über das Löschen des gesamten Speicherbereichs des Datenträgers erfolgen kann.

Eine weitere sichere Alternative besteht darin, einzelne heikle Dateien oder gleich den gesamten Speicherbereich des Datenträgers zu verschlüsseln. Ohne Schlüsselmaterial sind vertrauliche Inhalte damit für Dritte unlesbar. Dies hat zudem den Vorteil, dass Ihre sensiblen Daten selbst dann geschützt sind, wenn Ihr Gerät (z.B. Laptop) verloren geht oder gestohlen wird – ohne Schlüssel kein Zugriff!

Optische Speichermedien
Bei beschreibbaren optischen Speichermedien werden die Daten mittels eines Lasers als Lochmuster in eine reflektierende Schicht eingraviert. Je nach Beschaffenheit dieser Schicht lässt sich dieser Vorgang nur einmalig (R) oder mehrmalig (RW) durchführen.

Aufgrund der technischen Schwierigkeit und des geringen Werts der Datenträger ist hierbei die physische Zerstörung des Datenträgers die praxistauglichste Lösung der Datenlöschung.

Magnetische Datenbänder
Magnetische Datenbänder werden häufig für Backups ganzer Datensammlungen verwendet und oftmals über längere Zeiträume aufbewahrt. Sie ermöglichen damit einen «Blick in die Vergangenheit» - auch auf längst verschollen geglaubte Daten.

Magnetische Datenbänder zeichnen die zu sichernden Inhalte sequentiell in Datensets auf. Diese bilden im Allgemeinen eine unveränderliche, mit Integritätsschutz versehene Einheit. Einzelne Dateien lassen sich daraus nicht entfernen. Vielmehr muss bei der Datenlöschung das ganze Datenset vernichtet werden.