Daten löschen

Hier erfährst du:

- Warum Daten löschen oft komplizierter ist als gedacht.
- Warum Verschlüsselung die bessere Alternative zum Löschen ist.
- Konkrete Anleitungen und Programme zum sicheren Löschen von Daten.
- Wie du dein Smartphone wirklich zurücksetzt und löscht.

Es ist leider etwas kompliziert einmal erstellte Daten “sicher” zu löschen. Wenn du Dateien einfach normal löscht, sind die Daten meist noch vollständig da. Wenn du Dateien in den “Papierkorb” schiebst, sind sie noch nicht gelöscht – auch nicht wenn du den “Papierkorb” löscht/leerst! Ihr Name wird lediglich aus der Liste verfügbarer Dateien auf diesem Datenträger ausgetragen. Der Verweis auf die Daten wird so quasi nur aus dem Inhaltsverzeichnis gelöscht, die Daten selbst bleiben aber enthalten. Der belegte Platz wird freigegeben, aber nicht überschrieben. Das heißt, mit der richtigen Software können die Daten meist recht einfach wiederhergestellt werden. Daten sicher löschen, heißt daher die Daten gezielt zu überschreiben.

Auch allein durch die Verwendung des Computers fallen unbewusst recht viele ‘einfach’ gelöschte “Temporäre Dateien” an, zB beim erstellen eines Textdokuments werden – für die User:in unbewusst – viele Versionen zwischengespeichert. Auch beim Besuchen von Websiten werden oft Daten auf dem Computer zwischengespeichert. Diese Daten können ebenfalls sehr viel über dich verraten. Hier ist es unmöglich den Überblick zu bewahren: Ein verschlüsselter Computer ist die einzige zufriedenstellende Lösung für dieses Problem.

Verschlüsselung als bester Schutz!
Generell ist der beste Schutz deiner Daten verschlüsselte Datenträger zu verwenden. Auch dein Computer sollte unbedingt verschlüsselt sein, nur dann kannst du sicher sein, dass deine Daten auch nicht ausgelesen werden können.
Vorschlag: Die sicherste Variante wäre Daten nur (temporär) im Arbeitsspeicher des Computers zu halten. Hierfür empfehlen wir das Betriebssystem auf dem USB-Stick: Tails

Daten sicher löschen

Um Daten sicher, also möglichst nicht wiederherstellbar, zu löschen, werden sie meist mit Zufallszahlen überschrieben (wipe). Es gibt verschiedene Einschätzungen, wie oft die Daten dafür überschrieben werden sollen. Klar ist, je öfter die Daten überschreiben werden, desto besser. Oft wird empfohlen Daten mindestens sieben mal zu überschreiben. Mit bestimmten Programmen kannst du einzelne Dateien sicher löschen oder auch den gesamte Speicherplatz, der als “frei” markiert ist. Dann sollten Daten, die du auf diese Weise gelöscht hast, auch nicht mehr wiederherstellbar sein.

Einschränkungen
“Sicheres Löschen” funktioniert aber nicht immer! Zum Beispiel, können Sektoren auf einem Speichermedium nicht erreicht werden, wenn sie als defekt markiert sind. In einem Forensik-Labor könnten die darauf gespeicherten Daten jedoch wiederhergestellt werden. Bei sogenannten Flash-Speichermedien, wie USB-Sticks, SD-Karten und die neueren SSD-Festplatten (Solid-State-Disks), werden Daten intern noch häufiger umgespeichert, wodurch das “sichere Löschen” womöglich nicht

alle Kopien erwischt. Deswegen gilt das “sicher Löschen” also vor allem auf Flash-Speichern (USB-Sticks, SSD,…) als nicht zuverlässig. **Daher empfehlen wir jedenfalls eine komplette Verschlüsselung deines Datenträgers.** Im Folgenden geben wir aber dennoch Tipps zum “sicheren Löschen” von Daten.

Anleitungen

Wir empfehlen trotz der Möglichkeit Daten sicher zu löschen, alle Datenträger nach Möglichkeit zu verschlüsseln!

Verschlüsselung als sichere Datenvernichtung

Wenn ihr einen ganzen Datenträger löschen wollt, könnt ihr den Datenträger auch verschlüsseln. Das macht ihr zum Bespiel mit dem Verschlüsselungsprogramm VeraCrypt – eine Anleitung dafür findest du im Wiki.

Wenn ihr den Datenträger nun neu formatiert, ist er wieder voll verwendbar und die alten Daten nicht mehr wiederherstellbar. Einen Datenträger formatieren ist sehr einfach:
In **Linux** gibt es dafür eigene Tools, hier findet ihr eine einfache Anleitung zum Formatieren unter Ubunutu.

Unter **Windows** ist es ebenfalls einfach: Ihr klickt im File-Explorer (Dateibrowser) mit der rechten Maustaste auf den zu formatierenden Datenträger und wählt “Formatieren”. Du wirst dann nach der Auswahl deines Dateiensystems gefragt: NTFS: Wenn ihr das Windows-eigene Dateiformat “NTFS” verwendet, kann der Datenträger von allen Betriebssystemen gelesen werden sowie von Linux und Windows auch beschrieben werden. FAT32: Falls ihr auch unter MacOS darauf etwas speichern wollt, empfehlen wir euch das ältere und langsamere “FAT32” auszuwählen. Hier kannst du auch nichts falsch machen, den im schlimmsten Fall sind deine Daten weg. Was hier ja sowieso so gedacht war.

Linux und sicher Daten löschen

Löschen mit BleachBit (Linux)

BleachBit ist eine FOSS (Freie Software) Software und mit ihr lassen sich Daten einfach löschen. Sie kann sowohl auf Linux, als auch auf Windows verwendet werden. Bei *Surveillance Self Defence* findest du eine ausführliche Anleitung zur Installation und Verwendung von BleachBit with Linux [english] .

Löschen mit shred (Linux)

Das Programm *shred* ist unter den meisten Linux-Varianten (Ubuntu, Debian,…) bereits vorinstalliert. Allerdings hat es keine graphische Obfläche, sondern muss im Programm Terminal über Texteingabe ausgeführt werden.

Sicheres Löschen von Daten mit shred:

⇒ Klicke im Dateimanager im Ordner in dem die Datei liegt die du löschen möchtest mit der rechten

Maustaste ins „Leere“. Wähle *In Terminal öffnen* aus.
⇒ Folgenden Textbefehl eintippen:
`shred -fuz DATEINAME`
⇒ Die Datei wird überschrieben gelöscht und anschließend nochmal mit Nullen überschrieben um den Löschvorgang zu verschleiern. Die Datei ist nach ausführen des Befehls verschwunden.

Mit *shred* können auch Festplatten überschrieben werden. Weitere Funktionen und Befehle findest du im Wiki von Ubuntu.

Windows und sicher Daten löschen

Löschen mit BleachBit (Windows)

BleachBit ist eine FOSS (Freie Software) Software und mit ihr lassen sich Daten einfach löschen. Sie kann sowohl auf Linux, als auch auf Windows verwendet werden. Hier ist eine recht ausführliche Anleitung zur Installation und Verwendung von Bleachbit unter Windows.

Löschen mit SDelete (Windows)

Wenn du mit der Kommandozeile zurecht kommst, kannst du auch „SDelete“ von Microsoft verwenden.

⇒SDelete installieren
⇒In der CMD zum Speicherort navigieren
⇒„sdelete DATEINAME“
⇒Warten bis Datei verschwunden ist

macOS und sicher Daten löschen

Wie du unter macOS Daten mit internen Tools sicher löschen kannst, findest du hier.

Smartphone richtig zurücksetzen

Ihr habt ein neues Smartphone und wisst nicht, was ihr mit dem alten machen sollt? Die Dateien sind auch schon auf einem verschlüsselten Backup, aber was nun? Das Smartphone auf Werkeinstellungen zurücksetzen, reicht nicht aus. Leider ist es nicht sehr einfach alle Daten ganzheitlich zu löschen, so dass sie nicht mehr wiederherstellbar sind. Hier empfehlen wir euch am besten euer Smartphone zu verschlüsseln. Wählt ein sicheres Passwort für den Schlüssel. Das Passwort müsst ihr euch auch nicht merken. Danach setzt ihr es auf die Werkeinstellungen (in den Einstellungen zu finden) zurück. Am Besten ist es, wenn euer Smartphone von Beginn an verschlüsselt und mit einem guten Passwort geschützt ist.

Zum Weiterlesen

Destroy sensitive information [english] by Security in a Box
Daten löschen by beschlagnahmt.org
Ratgeber Daten vom Mobilgerät löschen by mobilsicher.de