

# Datenhygiene

Egal ob bei TKÜ, digitaler Forensik oder Hausdurchsuchungen: Es geht immer um Daten, aus denen euch potentiell ein Strick gedreht werden soll. Deshalb gehört es dazu, sich die Frage, welche Daten wirklich notwendig sind, regelmäßig zu stellen.

Natürlich bereitet das ein bisschen mehr Aufwand, Daten tatsächlich zu vernichten und erfordert vor allem Disziplin.

- Brauchen wir für dieses Treffen ein Protokoll?
- Muss das Handy mit auf die Aktion?/Habe ich vor das Handy für irgendwas zu benutzen?
- Muss ich Freund\*innen schreiben, welche coole Aktion ich gerade gemacht habe?
  - Selbstdarstellung ist schon vielen zum Verhängnis geworden
- Wenn alle beim Treffen waren, braucht es für manches vielleicht kein Protokoll

Wenn es keine Daten gibt, kommt auch niemand dran. Allerdings kann die Einschätzung einiger weniger, dass die Recherche-Unterlagen jetzt veraltet sind und vernichtet werden können, ein paar Jahre später schwer bereut werden. Der berühmte Aktenordner unter dem Bett wäre aber vielleicht zu riskant gewesen. Wie also Daten sicher aufbewahren? Auf Papier auf jeden Fall nur in den wenigsten Fällen!

Was aber, wenn "euch selbst belastendes Material" entstanden ist? Weg mit dem Mist. Den meisten dürfte jedoch bekannt sein, dass das einfache Löschen von Dateien keineswegs heißt, dass Daten unwiderruflich verschwunden sind. Noch nicht einmal wenn Windows euch warnt, dass mit dem leeren des Papierkorbs aber nun wirklich alles für immer in einem schwarzen Loch verschwindet.

## Daten sicher löschen

Um zu veranschaulichen was passiert, wenn Dateien "normal" gelöscht werden gibt es eine Metapher:

### Info

Das folgende Szenario gilt aus technischer Perspektive nur bedingt für gängige Arten von Speichern, bspw. für klassische HDD-Festplatten! Bei Flashspeichern wie bspw. SD-Karten, USB Sticks oder SSD's gibt es noch zusätzliche Dinge zu beachten. Mehr dazu unter "Besonderheiten" weiter unten.

# Anna & Arthur's WG

Anna & Arthur wohnen in einer WG. Ihre Namen und Adresse stehen im Adressbuch (anders als beim Telefonbuch ist hier alles nach Adresse geordnet).

Die Wohnung ist das Speichermedium/Datenträger (Festplatte, USB Stick, SD-Karte, etc) und Anna & Arthur sind die Daten auf dem Datenträger. Das Adressbuch ist die Adressverwaltung des Datenträgers.

Wollt ihr euch nun Arthur auf eurem Bildschirm anzeigen lassen, gebt ihr dem PC die Adresse von Arthur. Dieser geht für euch zu besagter Adresse, holt Arthur aus seiner Wohnung und präsentiert ihn auf dem Bildschirm.

Soweit der Normalbetrieb, wenn Daten im Speicher liegen und benutzt werden.

Leider ist Arthur aber bei der letzten Aktion der Schlauchschal unter die Nase gerutscht, er wurde erkannt und muss nun schnell weg. -> Daten müssen gelöscht werden.

Klickt ihr nun auf "löschen" wandert diese Datei in den Papierkorb. Im Papierkorb ist gar nichts gelöscht; seht das einfach als einen "Noch zu löschende Dateien"-Ordner.

Also leert ihr auch den Papierkorb. Was ist nun passiert? Ist Arthur verschwunden?

Nein, ihr habt lediglich Arthurs Namen aus dem Adressbuch gelöscht. Arthur selbst sitzt noch immer auf seiner Couch und wartet, dass etwas passiert. -> Die Daten liegen physisch noch immer auf dem Datenträger. Sie sind bloß nicht mehr im Adressverzeichnis des Speichers indexiert.

Schauen die Cops nun ins Adressbuch, werden sie Arthurs Namen nicht mehr finden. Doch wenn sie einfach Straße für Straße, Haustür für Haustür absuchen, stoßen sie irgendwann auf Anna & Arthurs WG, in der Arthur immer noch sitzt.

Das führt uns zum Überschreiben mit zufälligen Bits: Anna & Arthur brauchen random Nachmieter\*innen. Denn wenn ihre Genoss\*innen einziehen, oder eben alles nur mit Nullen überschrieben wird, könnte das Spuren hinterlassen.

Zusammengefasst: Daten sind erst richtig gelöscht, wenn die Adressen im Speicher, auf dem sie lagen, durch andere zufällige Daten überschrieben wurden. Dieser Vorgang ist jedoch in keinem gängigen Betriebssystem (egal ob PC oder Handy) Standard, denn diese löschen nur die Adresseinträge zu den Dateien. Das erfordert also extra Aktionen.

## Besonderheiten

- **Adressierung:** Bei Flashspeichern wie SD-Karten, USB Sticks oder SSDs weiß das Betriebssystem nicht genau, auf welchen exakten Bits die Daten eigentlich liegen. Eine eindeutige Verbindung zwischen physischen Bits und von außen adressierbaren Sektoradressen existiert so nicht. Deshalb können diese Bits auch nicht einfach überschrieben werden, weil gar nicht klar ist, welche denn überschrieben werden sollen.

- **Overprovisioning:** Noch dazu blockieren diese Arten von Speicher bestimmte Adressblöcke vor externem Schreibzugriff, sogenannte "Reserveblöcke". Dieses Overprovisioning hat drei Hauptfunktionen: Fehlerkorrektur, Optimierung von Schreibgeschwindigkeit und schont die Lebensdauer des Speichermediums.

### Technical Details - Overprovisioning

- Fehlerkorrektur: Wenn einzelne Speicherzellen fehlerhaft werden (zum bsp. durch Verschleiß), kann der Controller auf diese Reserve zurückgreifen, um zu vermeiden, dass die Daten "kaputt" abgelegt werden.
- Schreibgeschwindigkeit: Da die Reserveblöcke bereits "leer" zur Verfügung stehen, müssen nicht immer erst Zellen gelöscht werden, um sie neu zu beschreiben. Der Controller kann so direkt auf leere Zellen zurückgreifen und sie sofort beschreiben.
- Lebensdauer: Overprovisioning vermeidet durch Rotieren der Daten auf den Speicherzellen, dass einzelne Zellen über eine sehr lange Zeit im immer gleichen Zustand bleiben. Das führt klassischerweise dazu, dass diese Zellen bezüglich ihres "an"- und "aus"-Zustandes asymmetrisch werden. Sie tendieren also eher in die eine, oder die andere Richtung zu kippen. Bei Schreibvorgängen kommt es dann zu Fehlern, weil einem Transistor, der bspw. über Jahre "an" war, nun mit einem extrem kurzen Impuls gesagt wird, dass er nun mal "aus" werden soll. Das passiert aber eventuell nicht, weil er sich schon so lange an "an" gewöhnt hat.

Deshalb reicht es hier nicht aus, mit gängigen Methoden Speicherzellen mit random Bits zu überschreiben. Damit bleiben die Reserveblöcke unangetastet, aus denen aber im Zweifel alte Daten rekonstruiert werden können. Die ATA Spezifikation bietet dafür zwei Befehle: `SECURITY ERASE UNIT` und `ENHANCED SECURITY ERASE UNIT`. Ersteres überschreibt nur mit Nullen, zweiteres mit random Bytes. Werden diese Befehle auf eine SSD angewandt, werden auch besagte Reserveblöcke überschrieben. Sowohl unter Linux als auch unter Windows finden sich dafür Kommandozeilen-Tools, die jedoch etwas *hacky* sein können. Die meisten SSD Hersteller wie Samsung, Kingston, Western Digital und Co. liefern extra dafür eigene Tools mit, derer sich bedient werden kann.

Diese Tools machen im Prinzip nichts anderes als diese Befehle auf SSDs mit ihrer eigenen (proprietären) Firmware anzuwenden.

## Verschlüsselte Daten löschen

Eine effizientere Methode ist die Verschlüsselung. Das folgende gilt für sowohl für rotierende Platten (HDDs) als auch für SSDs:

Wird der Datenträger verschlüsselt, wird ein Key generiert, der im Header (~Kopfzeile) des Speichers abgelegt wird. Dabei werdet ihr aufgefordert ein Passwort für die Verschlüsselung

festzulegen. Mit diesem Passwort wiederum wird der im Header liegende Key verschlüsselt - nicht die Daten selbst.

Jede Datenlese- oder Schreiboperation der Daten wird symmetrisch mit dem Key ent-, oder verschlüsselt.

Die Bit-Zustände auf dem physischen Datenträger können auf Grund der mathematischen Eigenschaften moderner Verschlüsselungsalgorithmen nicht von random Bits unterschieden werden. Ein verschlüsselter Datenträger sieht also forensisch genau so aus wie ein zufällig beschriebener.

Um diese Daten nun wieder sicher zu löschen, muss daher nur der Key im Header des Datenträgers gelöscht und überschrieben werden. Das spart nicht nur enorm viel Zeit (dauert nur ein paar Minuten), das schont auch die Lebensdauer des Datenträgers. Ein vollständiges Überschreiben von einer 1TB HDD kann gut und gerne mal mehr als 5 Stunden dauern.

Detailliertere Infos findet ihr beispielsweise [hier](#).

### Kurzfassung

- Daten auf unverschlüsseltem Datenträger: gelöschte Daten lassen Spuren zurück, die wiederhergestellt werden können. Deshalb müssen Daten beim Löschen mit zufälligen (random) Bits überschrieben werden (am besten mehrfach).
- Daten auf verschlüsseltem Datenträger: Diese sind höchstens durch den Key in ihrem Header entschlüsselbar. Dieser Key ist mit einem Passwort gesichert. Wird nur dieser Key gelöscht und überschrieben, können Daten nicht mehr hergestellt werden.

---

Version #1

Erstellt: 14 Januar 2025 18:53:33 von ESC-IT Migration Bot

Zuletzt aktualisiert: 14 Januar 2025 18:53:33 von ESC-IT Migration Bot