5. Dokumentation

Tipps zum Verfassen und Versenden von Schreiben

Grundsätzliches: Wählt nicht immer die gleiche Methode, falls ihr regelmäßig aktiv seid! Wenn es geht, vermeidet es, zu Hause zu arbeiten, denn dort gibt es überall Spuren von euch, Fasern, Fusseln, Haare etc.. Genaueres zum Thema Spuren findet ihr im 4. Kapitel „Spuren". Bewahrt nichts unnötig auf! Sicherheit geht vor Kosten.

„das gängige Modell: Computer":

Wenn ihr euch für diese Methode entscheidet, lest auf jeden Fall auch den nächsten Artikel „Sicher schreiben lernen am Computer"!

Und nun folgen die unplugged Versionen:

„auf die Schnelle":

Für kürzere Texte sind Schablonen aus dem Schreibwarenladen geeignet. Werft sie aber hinterher weg! Nicht alle Stifte eignen sich für eine Schablone, viele sind nicht spitz genug. Vermeidet das Durchdrücken auf eure Unterlage und kopiert den Text vor dem Versenden.

„kurz und knapp":

Für Kürzeres gibt es auch Klebebuchstaben im Schreibwarenladen. Löst die einzelnen Buchstaben mit einer Pinzette, kopiert den Text danach, entsorgt die Reste.

„old school":

Schreibmaschinen könnt ihr auf dem Trödelmarkt kaufen. Sie sollten vorher nicht von euch oder Bekannten benutzt worden sein. Vermeidet Durchdruck oder werft auch das Unterlagenpapier weg. Entsorgt die Maschine, verwendet sie nur einmal.

„der Klassiker":

Buchstaben oder Worte aus Zeitungen ausschneiden und aufkleben, dann kopieren und die Reste entsorgen. Verwendet keine speziellen Magazine, die den Autor_innenkreis besonders einengen.

„zu vermeiden":

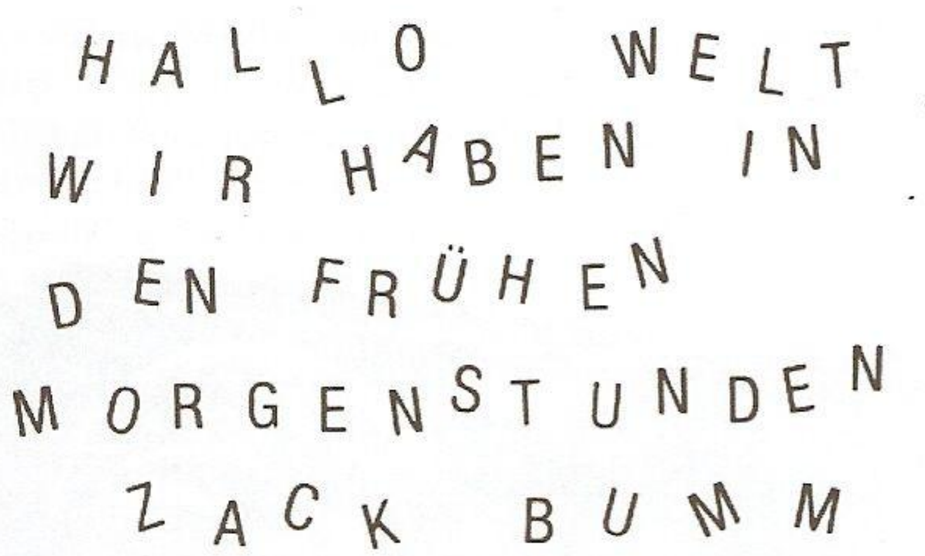
Eure Schrift verstellen oder mit links schreiben solltet ihr niemals! Texte von Schreibmaschinen, die ihr unbedingt aufheben wollt, könnt ihr nachschreiben oder übermalen, aber sicher ist das nicht.

Kopieren

Kopierer haben spezifische Merkmale, die wiedererkennbar sind. Einige moderne Farbkopierer und Laserdrucker drucken zudem eine hellgelbe, kaum sichtbare Identifikationsnummer auf jede Kopie. Geht daher nicht in Läden, die ihr regelmäßig aufsucht. Arbeitet (zumindest in warmen Jahreszeiten) nicht mit Handschuhen oder verhaltet euch anderweitig auffällig. Um die Originale zu verändern, könnt ihr zoomen (abwechselnd stark vergrößern und verkleinern) und Kopien von Kopien machen. Vergesst die Vorlagen nicht im Kopierer! Kopiert als erstes und letztes ein oder mehrere leere Blätter, damit ihr den Papierstapel mit den Fingern nehmen könnt, wenn ihr keine Handschuhe tragt. Steckt diesen Stapel dann in eine neue, saubere Mappe, die geschlossen ist und in der keine Spuren von euch auf den Blättern landen können.

Versenden

Kauft Umschläge und Briefmarken nur eingepackt - es gibt auch bereits frankierte, eingepackte Umschläge bei der Post. Ihr solltet diese Verpackungen und die Mappe mit den Kopien erst in einer Umgebung aufmachen, in der keine Spuren von euch herumfliegen: Geht in eine andere Wohnung und/oder legt dort Folie aus, wo ihr eintüten wollt. Kleidet euch dabei gut ein, z.B. mit einem Haarschutz und lasst nichts in die Umschläge fallen. Es ist empfehlenswert, die Umschläge mit einer Absende-Adresse zu versehen, allerdings nicht mit auffälligen Klebebuchstaben oder einer Schablone. Ihr könnt die Adressen irgendwo außerhalb ausdrucken und sie kopieren oder ihr schreibt mit einer Schreibmaschine, verkleinert das Geschriebene und klebt dann die Adressen und Absender auf. Es muss davon ausgegangen werden, dass die Post nach Aktionen an Zeitungen adressierte Umschläge, besonders solche ohne Absender_in, an die Bullen weiterleitet. Vielleicht ist absehbar, dass eure Schreiben von den bürgerlichen Medien sowieso unbeachtet bleiben. Dann kann es sinnvoll sein, nur an eure regionalen Blätter zu



senden, um unnötige Spuren zu vermeiden. Aber auch dort natürlich auf Fingerabdrücke achten.

Vermitteln auf andere Art

Schreiben oder Flugblätter vor Ort zu hinterlassen ist gut, aber auch ein Risiko. Auch Sprühen am Objekt oder in dessen Nähe kann den inhaltlichen Kontext erklären. Aber Vorsicht: Auch diese Schriftzüge sind wiedererkennbar. Direkt bei der Presse im Hausbriefkasten einwerfen solltet ihr nur unter Beachtung von möglichen Kameras.

Schreiben an wen?

Überlegt vor der Aktion gut, an wen sich eine Vermittlung der Hintergründe richten soll.

Welches Medium, welche Zeitschrift wäre dafür geeignet und würde eurem Text eventuell auch Beachtung schenken? Denkt auch an lokale Blättchen und an Fachzeitschriften. Generell erhöhen mehr Sendungen oder Hinterlassenschaften vor Ort die Chance auf Veröffentlichung und der Mehraufwand beim Postversand ist gering, aber die Spurenquellen nehmen dadurch zu. Deshalb kann weniger manchmal mehr sein.

Ist schlechte Presse besser als gar keine? Es ist manchmal einfacher bei der Boulevardpresse etwas zu veröffentlichen, aber dafür ist es wahrscheinlich, dass dort euer Anliegen verdreht oder absichtlich falsch eingeordnet wird. Aber vielleicht können sich schlaue Leser_innen trotzdem selbst ein Bild machen und bei manchen Objekten ist schon die Nennung des Objekts ausreichend, zum Beispiel bei Militärgerät.

Posteinwurf

Nehmt nicht den Briefkasten direkt vor der Tür und vergesst die Handschuhe beim Einwerfen nicht. Werft nicht alle Sendungen in denselben Kasten. Falls es zu einem Durchchecken durch die Bullen kommt, fallen die gleichartigen Briefe dann nicht sofort auf. Bei Aktionen in mehreren Orten oder Städten oder auf dem Land kann sich eine Reise an einen anderen Ort zum Einwerfen der Post lohnen. Zum Zeitpunkt des Verschickens: Ihr solltet die Texte über Nacht nicht zu Hause aufbewahren, sondern an einem sicheren Ort. Wartet bei koordinierten Aktionen die Rückmeldungen der anderen ab. Falls es zu Festnahmen kommt, kann ein gemeinsames Schreiben zu einem §129(a)-Verfahren führen. Manchmal kann es sinnvoll sein, den Text erst nach der Aktion zu verfassen, damit mögliche Effekte noch kommentiert werden können oder falls die Aktion nicht wie vorgesehen gelaufen ist.

Textaufbau

Für die bürgerliche Presse ist es meist sinnvoll, zu Anfang ein oder zwei prägnante Sätze zu formulieren, in denen alle wichtigen Informationen enthalten sind. Danach können Argumente und Hintergründe folgen. Macht eure Texte nicht länger als nötig (um es der Presse zu erleichtern und um so wenig Schreibstilspuren wie möglich zu hinterlassen), aber bringt Hintergrundinfos, wenn das Thema oder der Anlass neu und unbekannt sind.

Inhaltlich

Kennt ihr das? Mensch sitzt nach der Planung einer tollen Aktion zusammen und irgendwann taucht die Frage auf, wer einen erklärenden Text schreibt und was drinstehen soll. Ist es nicht eigentlich schade, dass wir die Gelegenheit selten dazu nutzen, mit der Gruppe mal wieder eine Diskussion zu vertiefen und so den Text gemeinsam zu entwickeln, anstatt die Aufgabe an eine Person zu delegieren, die unter Zeitdruck schnell etwas fabriziert, das die anderen nur abnicken? Oft wird, auch der Risiken wegen, dieser Aufwand gescheut, obwohl durch einen Text die Aktionen stärker wahrgenommen werden könnten. Gleichzeitig kann das eine Anregung sein, Diskussionen in der Szene weiterzuführen, Kampagnen aufzugreifen und selbst aktiv zu werden.

Namensgebung

In den letzten Jahren gab es u.a. in der Militanzdebatte Argumente pro und contra einer kontinuierlichen Namensgebung bei Erklärungen. Es gibt demnach vier Konzepte: Kontinuität des Namens; immer andere (fantasievolle) Namen; kein Gruppenname sondern Forderungen und Parolen oder ein allgemein gehaltener Name, unter dem sich diverse Gruppen, manchmal mit eigenen Zusätzen, erklären können (z.B. RZ und Autonome Gruppen).

Für einen kontinuierlichen Namen spricht:

- erhöhte mediale Aufmerksamkeit
- eine Auseinandersetzung mit der Politik der Gruppe wird ermöglicht, weil mehrere Texte vorliegen
- auch nicht-aktionsgebundene Texte erfahren Aufmerksamkeit in der Szene

Dagegen spricht:

- erhöhte Repressionsgefahr (euch kann alles, was unter Verwendung dieses Namens getan wird, angehängt werden)
- andere Aktionsgruppen werden weniger wichtig genommen
- es gibt mehr Rasterpunkte für euer Gruppenprofil
- durch die überhöhte Bedeutung kann es zu einem „Wegdelegieren" an diese Gruppe kommen oder ein sich darauf Ausruhen, da „die ja schon was tun"

Fotos von Aktionen

Nur ein paar kleine Tipps:
Wir raten dringend davon ab, Aktionsfotos zu machen, auf denen Menschen zu sehen sind! Auch vermummt können diese eventuell später identifiziert werden. Wenn ihr verpixelt, denkt daran: Personen können auch anhand von Körperbau und Kleidung identifiziert werden. Zudem sind nicht alle Verpixelungsverfahren sicher. Einige Verdrehungen etwa können von Polizeitechniker_innen einfach wieder zurückgedreht werden. Manche Fotoprogramme verwenden zudem einen Vorschaumodus, in dem die Daten unverpixelt gespeichert werden. Es gibt aber auch Programme, die diese Zusatzinformationen wieder entfernen. Wenn ihr digitale Fotos ins Netz stellt, denkt daran, dass die Bilddatei Daten eurer Kamera enthalten kann. Auch hierfür gibt es Programme, die diese Informationen löschen. Wir wissen nicht, wie sicher das ist. Außerdem ist es ja möglich, dass einer_m die Kamera abgenommen wird, bevor mensch die Fotos unkenntlich gemacht hat!

Sicher schreiben lernen am Computer

Zusammenfassung:

Egal, ob es um das Verfassen sensibler Flugblätter, Anleitungen, Zeitungen oder Bücher geht oder um die schriftliche Vermittlung einer illegalen Aktion – es gibt viele Umstände, welche das anonyme und spurenfreie Erstellen von Schreiben notwendig machen. Nur noch selten wird hierfür die Einweg-Schreibmaschine genutzt. Computernutzer_innen raten wir jedoch dringend vom nachträglichen Löschen wirklich heikler Daten durch vermeintlich sicheres Überschreiben (z.B. der Festplatte oder des Memorysticks) ab. Wir empfehlen und beschreiben eine Methode, mit der Datenspuren im Computer vermieden werden sollen, statt sie nachträglich zu entfernen/verwischen. Mit einem Betriebssystem auf CD gehen auch Nicht-Expert_innen auf Nummer Sicher: *Festplatte raus!* Das Betriebssystem, mit dem der Computer sonst arbeitet, bleibt davon vollkommen unberührt.

Wer nur eine Anleitung sucht und keine Lust auf eher technische Hintergrundinfos hat, die erläutern, warum wir eben diese Anleitung vorschlagen, kann die folgende Einleitung überspringen. Für alle anderen gilt: Nicht entmutigen lassen - die Problembeschreibung in der *Einleitung* ist deutlich komplizierter als der rezeptartige Ausweg in der *Anleitung*. Viele werden sich fragen, ob wir mit unseren vorgeschlagenen Vorsichtsmaßnahmen nicht reichlich paranoid sind. Das hoffen wir, denn wir orientieren uns an dem (uns bekannten, derzeit) technisch Machbaren. Wir wissen zu wenig darüber, welchen Aufwand zur Datenwiederherstellung welche Behörde tatsächlich betreibt. Dieser Artikel ist kein Beitrag zu einem verunsichernden „Finger-Weg!" vom Erstellen sensibler Dokumente, sondern eine Anleitung zu einem *bewussten* „Trau-Dich!".

Einleitung

Das Problem: Daten „sicher" loswerden

Zu diesem Thema kursieren leider ähnlich wie beim Umgang mit Mobiltelefonen viele (entschieden vorgetragene) „persönliche Einschätzungen" und leider neigen nicht wenige zur Unterschätzung des Problems. Die leichtfertige Selbstvergewisserung „Handy ausschalten reicht" ist ähnlich wie „x-maliges Überschreiben einer Datei reicht" eine unter Umständen folgenschwere Verharmlosung. Um unseren Ratschlag der Anleitung gleich vorwegzunehmen: Ähnlich dem „bei wichtigen Gesprächen: Handy-Akku raus!"[1] gilt „bei sensiblen Schreiben: Festplatte raus!". Und jetzt zum Warum.

Die meisten von uns wissen, dass ein normales Löschen von Dateien auf dem Computer (z.B. über den Papierkorb trotz anschließendem „Papierkorb leeren") nichts bringt – und zwar bei allen gängigen Dateisystemen, unabhängig vom verwendeten Betriebssystem (Windows, Linux, Mac, etc.). Tatsächlich bleibt der Inhalt der Datei vollständig erhalten. Der Speicherbereich, in dem sich die Datei befindet wird lediglich in einer Tabelle als „leer" markiert und für zukünftige (unter Umständen sehr viel spätere) Nutzung freigegeben. Auch beim Formatieren der Festplatte wird nur diese Dateizuordnungstabelle gelöscht – die Daten selbst bleiben unverändert erhalten.

Häufig greift mensch daher auf Hilfsprogramme zurück, die sensible Dateien, Verzeichnisse oder ganze Laufwerke auf der Fesplatte, dem Memorystick oder sonstigen Speichermedien mehrfach mit Nonsens überschreiben. Eine als

1 Besser noch: Handy zu Hause lassen, um der Gefahr manipulierter Handys (verwanzte Akkus, oder versteckte zusätzliche Batterie im Handy) zu entgehen

besonders gründlich angesehene Methode[2] überschreibt die Daten dabei mit bis zu 35 verschiedenen (statischen und zufälligen) Bit-Mustern, welche die ursprünglichen Daten für diverse Codierungsverfahren[3] „möglichst nachhaltig überbügeln". Diese Methode wird z.B. im Programm *srm* (secure remove) verwendet, das ebenfalls auf der nachher vorgestellten *Ubuntu Privacy Live-CD* verfügbar ist. Doch auch das derart gründliche Überschreiben einer zu löschenden Datei auf der Festplatte oder dem Memory-Stick ist nicht ausreichend, denn:

1. Textverarbeitungsprogramme (und andere) legen im Normalfall (temporäre) Sicherheitskopien ab. Diese werden in der Regel nur *unsicher gelöscht* – verbleiben also auf der Festplatte oder dem Memorystick.

2. Das Betriebssystem lagert aus Platzgründen eigenständig und für den Nutzer unbemerkt Datenblöcke aus dem Computerspeicher (RAM) auf die Festplatte in eine Auslagerungsdatei (SWAP) aus, um sie später wieder in den Speicher zu holen. Wenn die zu löschende Datei auf eurem Rechner erstellt oder bearbeitet wurde, liegt also in der Regel noch eine Kopie an irgendeiner Stelle innerhalb dieses recht großen SWAP-Bereichs auf der Festplatte.

Auch das ist vielen Computernutzer_innen bekannt. *Aber* - angenommen wir könnten 1) und 2) ausschließen, in dem wir nicht nur die Datei selbst, sondern alle freien Bereiche (des Memorysticks und) der Festplatte in einer stundenlangen Prozedur „sicher" überschreiben. Sind die so gesäuberten Speichermedien wirklich sauber in dem Sinne, dass die ursprüngliche Datei und ihre ungewollten Kopien *sicher* nicht mehr wiederherstellbar sind? - **NEIN!**

Rekonstruktion von Datenspuren auf Speichermedien:

a) magnetische Medien (Festplatten, Disketten)

Der Defense Security Service (DSS) des US-Verteidigungsministeriums weist in seinem Sicherheitsstandard von 2007[4] Software-Methoden zur Löschung von magnetischen Medien als unzureichend aus. Als „streng geheim" eingestufte magnetische Datenträger müssen physisch zerstört werden. Wir beschreiben im Folgenden einige Umstände, Effekte und Unsicherheiten beim Überschreiben von magnetischen Medien, die dieses klare Misstrauensvotum gegenüber vermeintlich sicheren Löschprogrammen nachvollziehbar machen.

Daten werden als Bitfolge, also als Folge von Nullen und Einsen gespeichert. Auf einem magnetischen Datenträger werden diese logischen Nullen und Einsen physikalisch als Wechsel der Ausrichtung winziger Minimagnete codiert. Ein lokales Magnetfeld richtet beim Schreiben viele dieser Minimagnete in der Nachbarschaft aus. Nach dem Schreiben verbleiben also Regionen unterschiedlicher *Magnetisierung* auf einer so genannten Spur der Festplatte/Diskette. Ein Lesekopf kann diese magnetischen Muster beim Überfliegen entlang einer solchen Spur mit einer gewissen Genauigkeit abtasten und damit die Daten lesen.

Störender Zwischenpuffer

Das Löschen von Daten auf Festplatten durch mehrfaches Überschreiben beruht darauf, dass möglichst viele dieser Minimagnete *mehrfach* gedreht werden, in dem mensch *nacheinander, verschiedene* Datenmuster an die Stelle der zu löschenden Daten schreibt. Der *Schreibcache* ist eine Art Zwischenpuffer der Festplatte. Durchschaut die Festplatte unser Vorhaben, verschiedene Daten nacheinander an die gleiche Stelle zu schreiben, „optimiert" sie diese Operation und schreibt (bei aktiviertem Schreibcache!) nur das letzte dieser Datenmuster. Die sensiblen Daten wären damit nur einfach überschrieben statt wie angenommen z.B. 35-fach und damit leicht wiederherstellbar. Löschprogramme versuchen daher diesen Schreibcache vor dem Überschreiben auszuschalten. Doch nicht alle Festplatten schalten den Schreib-Cache tatsächlich ab! Computernutzer_innen haben (abhängig von der Festplatte und des darauf verwendeten Dateisystems) keine unmittelbare Kontrolle darüber.

Defekte Sektoren

Moderne Festplatten kopieren Daten von Sektoren, die als fehlerhaft erkannt wurden, in andere Bereiche der Festplatte. Diese fehlerhafter Sektoren sind ab dann auch für Löschroutinen nicht mehr zugänglich. Damit werden nur die Daten an der neuen Stelle, nicht jedoch die ursprünglichen überschrieben. Die Computernutzerin bekommt davon nichts mit. Fällt die Festplatte (z.B. bei einer Hausdurchsuchung) in die Hände von engagierteren Schnüffelbehörden, könnten diese die Magnetscheibe der Festplatte entnehmen und (mit Aufwand) solche fehlerhaften Sektoren auslesen.

Wandernde Bits

Die Festplattenherstellung hat mit dem Effekt zu kämpfen, dass die Grenzen zwischen kleinsten Bezirken[5] mit unterschiedlicher Ausrichtung der oben beschriebenen Minimagnete mit der Zeit (mehrere Mikrometer) auf der Platte wandern können. Damit verschieben sich unter Umständen auch unsere (viel größeren) Regionen unterschiedlicher Magnetisierung, die für die Aufzeichnung der Daten verwendet werden. Festplatten sind so konstruiert, dass das Wandern solcher Bits, deren Magnetisierungsmuster sich im Laufe der Zeit ausdehnen oder verschieben, automatisch durch geringfügige Justierung von Schreib- und Leseköpfen kompensiert werden kann. Die Daten können also auch weiterhin noch gelesen werden. Dieses Nachführen der Köpfe kann allerdings dazu führen, dass die Muster der Daten, die *vor* einer solchen Positionskorrektur auf die Platte geschrieben wurden, von der Löschsoftware nicht mehr (vollständig) überschrieben werden. Ähnlich aussichtsreich (für Schnüffelbehörden) kann eine Analyse des Pufferbereichs zwischen den Spuren sein. Dieser Pufferbereich zwi-

2 Peter Gutman *Secure Deletion of Data from Magnetic and Solid-State Memory* (http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html)

3 physikalische Darstellung der logischen Bits (0 und 1) auf dem jeweiligen Speichermedium

4 Standard des Department of Defense: DoD 5220.22-M

5 Weißsche Bezirke. In einem Magnetfeld haben die Minimagnete (atomare magnetische Momente) die Möglichkeiten, sich parallel oder anti-parallel dazu auszurichten. Diejenigen Bezirke, die bereits eine energetisch günstige Orientierung haben, wachsen auf Kosten der anderen, und die Grenzschichten zwischen ihnen, die so genannten Bloch-Wände wandern.=

schen den Spuren dient dazu, magnetische Beeinflussung zwischen den Mustern der Spuren zu vermeiden. Im Laufe der Zeit greifen die Magnetmuster der Spuren, ähnlich wie beim bekannten Durchkopiereffekt von alten Kassettenbändern, auf den Pufferbereich über. Die Rekonstruktion dieser Muster und damit der vermeintlich überschriebenen Daten ist mit Hilfe von Magnetkraftmikroskopen unter erhöhtem Aufwand möglich. Solche Mikroskope lassen sich beim forensischen „Lesen" der Festplatte viel genauer positionieren als ein normaler Lesekopf. Diese Analyse ist aber nur auf der Originalfestplatte möglich, nicht auf einer Kopie.

Zerstörung mit Tücken

Magnetische Materialien verlieren oberhalb einer gewissen Temperatur (Curie-Temperatur) schlagartig ihre magnetischen Eigenschaften. Alle Daten sind dann unwiderruflich weg. Die Curie-Temperaturen der dünnen magnetischen Schicht des Datenträgers (Eisenoxid oder Kobalt-Legierungen) liegen bei etwa 800°-1000°C. Diese Materialien schmelzen erst bei noch höheren 1500°C. Die Magnetschicht ist **bei Festplatten** auf eine starre Scheibe aus Aluminium *(Schmelzpunkt, 660°C)* oder Glas *(kein Schmelzpunkt – aber zähflüssig oberhalb 1000°C)* aufgebracht. Diese Temperaturen erreicht mensch in der Regel nicht in einem normalen Holz- oder Kohleofen und leider auch nicht ohne weiteres mit einer Campinggas-Lötlampe. Denn obwohl letztere eine maximale Flammentemperatur von 1800°C besitzt, erreicht das Material, was mensch erhitzen will, (wegen Wärmeabfuhr) häufig weniger als 700°C. In unserem Test reichte die Wärmeleistung der Billiglötlampe gerade aus, um eine ausgebaute Festplatten-Scheibe (in kleine Stücke zersplittert) zum Glühen zu bringen und zu deformieren. Hier sind heißere Flammen von Brennern zum Schweißen/Hartlöten gefragt. Bei einer (aus der Mode gekommenen) **Diskette** hingegen lässt sich die rechteckige Kunststoffhülle entfernen. Der eigentliche Datenträger (die dünne flexible Scheibe) brennt gut, wenn auch ungesund.

Magnetische Materialien können ebenfalls durch (extrem hohe) Magnetfelder unlesbar gemacht werden. Dafür nötige typische Feldstärken von z.B. 2.5 Tesla erreichen jedoch nur außergewöhnliche Kernspintomographen oder teure so genannte *Degaußer*. Handelsübliche Magnete sind dazu viel zu schwach.

Fazit:

Festplatten sind nicht leicht (billig) unlesbar zu machen. Mensch sollte sich nicht auf das Zersplittern der Scheiben in viele kleine Stücke verlassen. Selbst kleinste Stücke können unter dem Magnetkraft-Mikroskop mehrere Megabyte an Daten preisgeben. Die überzeugendste Strategie ist, sensible Daten von der Festplatte fern zu halten!

b) Flash-Speicher (Speicherkarten, USB-Sticks)

Zu diesem Typ Speicher gehören alle Speicherkarten, USB-Sticks, SD Karten, Multi-Media Karten (MMC), Mini und Micro SD Karten, CompactFlash-Karten (CF), Smart Media (SM) und auch die neueren SSD-Festplatten. Diese Solid-State-Disks setzen zum Speichern nicht wie herkömmliche Festplatten auf das magnetische Prinzip, sondern bestehen ebenfalls aus Flash-Speicherchips, die ihren Inhalt auch ohne Stromversorgung behalten. Für diese Speicherchips gilt leider ähnliches wie für magnetische Festplatten. Einem sicheren Löschen per Überschreibsoftware steht insbesondere folgender Effekt im Weg: Wegen der (immer noch) hohen Fehleranfälligkeit der verwendeten Speicherzellen werden Speicherbereiche, auf die häufig zugegriffen wurde, vorsorglich an andere Stellen umkopiert, um den Speicherzugriff gleichmäßiger zu verteilen. Damit können auch unsere sensiblen Daten mehrfach z.B. auf dem USB-Stick existieren. Beim mehrmaligen Überschreiben der Datei z.B. mit dem Programm *srm* (secure remove) erwischen wir unter Umständen nur eine von mehreren Kopien.

Speicherchips sind ziemlich robust. Die physikalische Zerstörung im Feuer gelingt in der Regel nur unvollständig. Nur wenige von uns haben Zugang zu einem Industrie-Schredder.

Falls wir also zur Zwischenspeicherung sensibler Daten USB-Sticks benutzen, müssen wir darauf achten, dass wir a) möglichst nur verschlüsselte Dateien abspeichern und b) die Sticks spurenfrei lagern und entsorgen.

c) Speicher des Computers (RAM)

Selbst im Hauptspeicher des Computers sind die als „flüchtig" geltenden Daten nach dem Unterbrechen der Spannungsversorgung (beim Ausschalten des Rechners) nicht sofort weg! Sowohl bei den Halbleiterbauelementen im *statischen* Speicher (SRAM) als auch bei denen des so genannten *dynamischen* Speichers (DRAM) bleiben Veränderungen in Abhängigkeit der ehemals gespeicherten Daten feststellbar[6].

Darüber hinaus lassen sich die zuletzt im Speicher befindlichen Daten kurz nach dem Ausschalten des Rechners vollständig wiederherstellen. Und dies um so länger, je niedriger die Temperatur der Speicherbausteine ist. Während bei Raumtemperatur der Speicherinhalt nur wenige Sekunden verlustfrei rekonstruierbar bleibt, lassen sich stark gekühlte Chips noch Stunden bzw. Tage später lesen[7]. Schnüffelbehörden können dies nutzen, wenn sie einen Computer vorfinden, der bei der Beschlagnahmung noch angeschaltet ist, oder kurz zuvor heruntergefahren wird.

Anders als bei allen anderen Speichermedien, lässt sich die Nutzung des internen Computerspeichers allerdings nicht vermeiden. Wir müssen ihn also anschließend säubern.

Beim Überschreiben von RAM ist (anders als bei magnetischen Datenträgern) nicht der häufige Musterwechsel sondern die *Speicher-Dauer* entscheidend - je länger ein Datum gespeichert bleibt, desto tiefer hat es sich „eingebrannt". Das berücksichtigen wir in unserer Anleitung beim „Überschreiben" des RAM nach Abschluss der Textarbeit.

6 P. Gutmann, *Data remanence in semiconductor devices*, Proc. 2001 USENIX Security Symposium

7 J. Haldermann, *Cold boot attacks on encryption keys*, Proc. 2008 USENIX Security Symposium

d) optische Medien (CD, DVD)

Bei CDs und DVDs (egal ob wieder beschreibbar oder nicht) fällt uns kein sinnvoller Grund ein, über andere Methoden zur Löschung als die vollständige Zerstörung nachzudenken. Eine CD/DVD in wenige Stücke zu brechen, reicht dazu definitv nicht![8] Aber Feuer hilft: Das Trägermaterial dieser optischen Medien (Polycarbonat) schmilzt bei 220-230°C. Die Zersetzung beginnt ab 350-400°C und bei 520°C entflammt es. Die billigste Campinggas-Lötlampe reicht aus, um die Scheibe aus Polycarbonat, einer dünnen Aluminiumschicht und der Schutzschicht aus Lack zu einem Klumpen zu schmelzen bzw. zu verbrennen. Nur wer viel Geduld hat, kann die Flamme einer Kerze verwenden. Bei der Verbrennung entstehen unangenehme Dämpfe – Atemschutz! Wegen eben dieser Dämpfe raten wir vom (durchaus wirksamen, wenige Sekunden dauernden) „Toasten" der CD/DVD in einer Mikrowelle ab.

Auf der Basis der oben beschriebenen Schwierigkeiten, Daten von verschiedenen Speichermedien RESTLOS verschwinden zu lassen, schlagen wir folgende Anleitung zur Erstellung sensibler Texte (oder allgemein zur Bearbeitung sensibler Daten) vor.

Anleitung

Der Ausweg: Arbeiten ohne Festplatte

Ziel ist es, sensible Texte in einer „sicheren" Computerumgebung zu bearbeiten und Datenspuren zu vermeiden, statt sie nachträglich zu entfernen/verwischen. Dazu benötigen wir ein sogenanntes Live-Betriebssystem auf CD oder DVD. Der populärste Vertreter solcher Live-Systeme ist Knoppix (www.knoppix.org). Knoppix bietet viele Möglichkeiten und arbeitet bestens mit verschiedenster Computer-Hardware zusammen. Wir empfehlen allerdings ein stärker abgeschottetes Live-Linux namens Ubuntu Privacy Remix (www.privacy-cd.org). Dieses Betriebssystem unterbindet jegliche Verbindung zum Internet und zu den gängigen Festplatten-Typen. Beide Distributionen werden regelmäßig aktualisiert und können unter den angegebenen Internetadressen frei heruntergeladen und anschließend auf CD oder DVD gebrannt werden. Windows-gewöhnte Computernutzer_innen werden nach kurzer Orientierung keine Probleme mit der sehr ähnlichen Oberfläche haben.

8 Auf einem 1cm2 großen Bruchstück einer einfach beschriebenen DVD sind etwa 45 MB gespeichert.

Das Sicherheitskonzept:

1. Keine Festplatte

Das ist der entscheidende Punkt, um sicher gehen zu können, dass auf dem Computer nach unserer Textarbeit keine Spuren zurückbleiben. Und weil das so zentral ist, vertrauen wir nur unserer Handarbeit und entfernen die Festplatte physikalisch.

2. Kein Netzwerk

Alle Schotten dicht. *Ubuntu Privacy Remix* deaktiviert den Zugang sowohl zu „wireless" als auch zu kabelgebundenen Netzwerken. Natürlich machen wir auch hier zusätzlich alles, was unter unserer unmittelbaren Kontrolle steht und ziehen das Internetkabel (Ethernet, oder LAN) von unserem Rechner ab.

3. Das Betriebssystem ist unveränderbar (da auf CD oder DVD).

Das heißt unser Betriebssystem kann von außen nicht bleibend verändert werden, also es kann auch keine Schnüffelsoftware dauerhaft installiert werden. Selbst wenn ein Schädling z.B. durch das Lesen eines USB-Sticks in das System gelangen sollte, ist er nach dem Ausschalten des Computers wieder weg.

4. Verwendung von Verschlüsselungssoftware

Um Texte später weiterverarbeiten zu können, kann es notwendig sein, sie auf einem neuen USB-Stick (ohne Fingerspuren) zwischenzuspeichern. Dies sollte allerdings aus Sicherheitsgründen nur verschlüsselt geschehen. Auf den Live-CDs ist dazu verwendbare Software (*Truecrypt, pgp*) enthalten.

Die Live-CD von *Ubuntu Privacy Remix* verhindert zwar, dass der Computer übliche Festplatten vom Typ ATA oder S-ATA aktiviert (weder schreiben noch lesen), allerdings gilt dies nicht für (eher selten gewordene) SCSI-Festplatten. Andere Live-CDs, wie z.B. *knoppix* erlauben der_m Nutzer_in, per Hand Festplatten einzubinden und nutzen diese standardmäßig sogar für das Anlegen von Auslagerungsdateien (SWAP), sofern dies beim Start nicht explizit mit der Option *noswap* unterbunden wird.

An diesem sensiblen Punkt vertrauen wir weder der Dokumentation hoch komplexer Betriebssysteme, noch unserem Halbwissen in deren Anwendung. Deswegen vermeiden wir das (fehleranfällige) Setzen von Lese- und Schreibrechten für Festplattenpartitionen und verbieten dem Rechner, jegliche Daten auf die Festplatte(n) auszulagern, indem wir alle Festplatten vor dem Einschalten des Computers physikalisch abziehen. Bei Laptops lässt sich die Festplatte in der Regel nach dem Lösen weniger Sicherungsschrauben einfach heraus nehmen. Bei Desktop-Computern müssen wir das Gehäuse öffnen und bei jeder(!) Festplatte das Datenkabel oder ihr Verbindungskabel zum Netzgerät – also die Stromzufuhr abziehen[9].

9 Wer im Zuge der Bedrohung durch Online-Durchsuchung seinen Computer sowieso mit verschiedenen (niemals zeitgleich betriebenen!) Festplatten versehen will, kann auch gleich einen kleinen Schalter am Spannungskabel einer jeden Festplatte einbauen.

Grundlegende Voraussetzung dafür: Der Computer muss in der Lage sein, (ohne angeschlossene Festplatte) von CD oder DVD aus zu starten. Die meisten Rechner können dies auf Anhieb, bei anderen muss mensch die Einstellungen im BIOS (eine Art Basis-Betriebssystem, in der die Grundkonfiguration des Computers festgelegt wird) so einstellen, dass der Rechner das CD-Laufwerk zum „booten" (hochfahren) verwendet. In das BIOS gelangt mensch bei den meisten Computern durch Drücken der Taste *F1* oder *F2* beim Bootvorgang (bei machen Rechnern kann das auch die *Esc* oder *Entf* Taste sein). Dann erscheint eine Liste von Bootmedien zur Auswahl.

Die Kurzanleitung:

Wir beschreiben die einzelnen Schritte für Computerunerfahrene etwas ausführlicher anhand der *Ubuntu Privacy Remix* Live-CD. Da sich die Linux-basierten Live-CDs stark ähneln, lässt sich die Anleitung leicht auf *Knoppix* und andere Distributionen übertragen. Lest die Anleitung vorab vollständig durch - nicht nur Schritt für Schritt. Nehmt euch Zeit. Überlegt vorab: Wo kaufe ich welchen (neuen!) Drucker? Gibt es dafür einen Druckertreiber auf der Live-CD? Probiert dann die Schritte in einem „Probelauf" aus.

1. **Festplatte ausbauen** oder abklemmen, Internetverbindung abziehen, Drucker mit Computer verbinden.
Beachtet beim Aufbau: Abhängig vom Druckertyp sind nach Benutzung im Druckerspeicher ebenfalls sensible Daten enthalten!!! Daher dürfen keine Fingerspuren auf dem Drucker sein. Ein Druckkopf kann mit seinen minimalen Abweichungen vom Typ-spezifischen Standard einem Ausdruck zugeordnet werden. Deshalb sollte insbesondere der Druckkopf frei von Fingerspuren sein und hinterher getrennt entsorgt werden.

2. Computer mit Live-CD im Laufwerk starten (warten bis fertig hochgefahren)
Wundert euch nicht, dass sich das System etwas träge „anfühlt". Alle Funktionen und Programme werden im Bedarfsfall von der CD/DVD geladen. Das dauert länger als ihr es von eurem Betriebssystem auf der Festplatte gewohnt seid. Wer einen Rechner mit ausreichend Speicher (mehr als 1,5 GB RAM) hat, kann die Startoption F4 - „copy to ram" nutzen. Dann wird das Betriebssystem komplett in den Speicher geladen. Ab jetzt arbeitet es sich viel schneller mit dem Computer und ihr könnt CDs brennen, da die Live-CD nach dem Hochfahren heraus genommen werden kann.

3. Drucker einschalten und einrichten
In der Regel wird der Drucker automatisch erkannt. Ihr könnt dies unter System//Systemverwaltung//Drucken überprüfen. Auf den dort erscheinenden Drucker klicken und dann eine Testseite ausdrucken. Funktioniert alles, dann könnt ihr noch unter Druckeroptionen die zu verwendende Patrone (sw/farbe), die Auflösung, ... einstellen. Wenn euer Drucker nicht automatisch oder falsch erkannt wurde, könnt ihr ebenfalls unter System//Systemverwaltung//Drucken unter Neu einen Drucker manuell einrichten. Taucht euer Druckermodell nicht in der Liste der angebotenen Treiber auf, könnt ihr so genannte generische Treiber oder Treiber älterer Modelle der gleichen Serie probieren. Wer Schwierigkeiten hat, kann unter Anwendungen//Hilfe eine Einrichtungsanleitung finden.

4. Testschreiben anfertigen und ausdrucken
Um sicher zu gehen, dass die Textverarbeitung (z.B. OpenOffice), das Desktop Publishing Programm (z.B. Scribus) oder die Bildbearbeitung (z.B. gimp) einwandfrei mit dem Drucker zusammenarbeiten und das Ergebnis brauchbar ist, sollte ein Probeausdruck angefertigt werden, bevor die eigentliche Schreibarbeit startet.

5. Schreiben
Beachtet, dass euer Text unwiderruflich weg ist, wenn ihr nachher den Rechner ausschaltet. Also überlegt bei längeren Texten, an denen ihr mehrere Tage schreibt, wo und wie ihr die Texte bis zur Fertigstellung speichern wollt. Wir empfehlen die Text-Datei verschlüsselt (z.B. mit *Truecrypt* oder *pgp*) auf einem spurenfreien Memory-Stick außerhalb eurer Wohnung aufzubewahren. Macht IMMER eine Sicherheitskopie der verschlüsselten Datei auf einem zweiten, ebenfalls spurenfreien Stick (oder auf einer CD). Gerade billige USB-Sticks sind leider recht fehleranfällig.

6. Drucken
Wenn es sich bei dem Ausdruck um das finale Schriftstück handeln soll, dann ist neben der Spurenfreiheit des Druckers und seines Standortes auch die Spurenfreiheit des Papiers und der Hülle, in der der Ausdruck transportiert werden soll, sicherzustellen. In diesem Fall sollte die Arbeit nicht bei euch zu Hause stattfinden und ihr keine bereits getragenen Klamotten in der äußeren Schicht anhaben.

7. Runterfahren (Ausschalten)
Rechts-oben klicken, warten bis das System heruntergefahren ist und den Computer ausschalten, falls er es nicht selbständig tut.

8. Endreinigung: Spuren im Speicher des Computers entfernen
Bei einem erneuten Start mit der Live-CD im Laufwerk wählen wir *„Arbeitsspeicher tèsten"*[10]. Damit wird anstelle des Betriebssystems auf der Live-CD das Programm *„memtest"*[11] gestartet, welches zur Überprüfung der korrekten Funktionsweise des Speichers verschiedene Bit-Muster in das RAM schreibt. Genau das hilft uns Datenreste loszuwerden. Zehn verschiedene Tests laufen in einer Endlosschleife ab, bis wir dies mit der Taste *„Esc"* stoppen, dann startet der Computer neu. Insbesondere Test 9 „Bit Fade Test" erscheint geeignet (wähle „c" für configuration, „1" für Testauswahl, „4" für Bit Fade Test und „0" für Continue), da er ein festes Muster für je 90 Minuten in den Arbeitsspeicher schreibt. Diesen Test lassen wir einige Stunden laufen, bevor wir mit *„Esc"* den Endlostest abbrechen und den Rechner ausschalten.

10 Unter Knoppix wählt mensch die Option „memtest".
11 Infos zu den Testalgorithmen unter www.memtest.org

9. Entsorgung
Testseite und Probeausdruck sollten verbrannt werden; Druckkopf und Drucker ohne Druckkopf sollten getrennt voneinander und spurenfrei entsorgt werden.

10. eventuelles Vervielfältigen
Falls der so erstellte Text vervielfältigt werden soll, beachtet dabei, dass fast alle Kopierläden mittlerweile digitale Kopierer verwenden, auf deren Festplatten die (eingescannten) Kopien aller Kund_innen Platz in der Größenordnung von Gigabytes finden, bevor sie überschrieben werden. Also verwendet keinen Kopierladen, in dem ihr häufiger seid. Macht zumindest Kopien von den Kopien um Charakteristika des von euch verwendeten Druckkopfes stärker zu verschleiern. Stufenlose Vergrößerungen und anschließende Verkleinerungen helfen ebenfalls. Wenn es zu auffällig ist in eine (nur außen angefasste, ansonsten saubere) Zeitung „hinein" zu kopieren, dann nutzt abgezählte Zusatzkopien vor und nach den verwendbaren Kopien zum Anfassen des Papier-Stapels.

Anmerkungen zur Sicherheit:

Um sicher zu gehen, dass das von euch verwendete Live-Betriebssystem auch tatsächlich das ist, wofür ihr es haltet, könnt ihr anhand „signierter Prüfsummen" überprüfen, ob eure CD oder DVD tatsächlich exakt (und nur) das gewünschte Betriebssystem enthält. Wie das geht, ist auf der Webseite (www.privacy-cd.org) beschrieben.

Das Ausbauen der Festplatte und die Verwendung des Betriebssystems auf der *Ubuntu Privacy Remix* CD bieten guten Schutz davor, dass 1) während des Bearbeitens Daten über irgendeine (wireless-LAN) Netzwerkverbindung nach draußen gelangen können und 2) Daten auf dem Rechner zurückbleiben. Es gibt aber *Angriffe, vor denen diese Anleitung keinen Schutz bietet:*

- **Abhören der elektromagnetischen Abstrahlung**

Computerbildschirme können auch auf größere Distanz (über 100m) abgehört werden. Funktastaturen (mit in der Regel simplen Verschlüsselungsverfahren) auch; kabelgebundene Tastaturen sind bisher nur eingeschränkt abhörbar.

- **Manipulierte Computerhardware**

Hierzu ist in der Regel physischer Zugriff der Schnüffler_innen auf den Computer notwendig. Keylogger (mit oder ohne Funk-Übertragung) getarnt als kleine Steckverbindungen am Tastaturkabel zeichnen alle Tastaturanschläge auf.

- **Innenraumüberwachung**

Überwachungsmethoden außerhalb des Computers (z.B. eine auf Bildschirm oder Tastatur gerichtete Kamera) können unsere Arbeit am Rechner aufzeichnen und uns zuordnen. Auch hierzu müssen Schnüffler_innen mindestens einmal in unserer Wohnung/Nachbarwohnung gewesen sein.

Was tun? - Bei diesen Sicherheitsbedenken ist zu empfehlen, für das Schreiben sensibler Texte keinen Rechner zu verwenden, der euch zugeordnet werden kann. Also lieber einen Rechner, der a) nicht von euch gekauft wurde, b) nie im Internet war und c) nicht in eurer sondern in einer völlig unverdächtigen Wohnung lagert. Eure Textarbeit solltet ihr dann ebenfalls lieber in anderen Räumlichkeiten (außerhalb eurer Wohnung) machen.

Weitere Anmerkungen:

- **Fotos** (z.B. von einem USB-Stick) bearbeiten und in eure Texte einfügen: Kein Problem. Wer schon mal mit Photoshop gearbeitet hat, wird auch in *gimp* die Werkzeuge zur grafischen Nachbearbeitung finden. Denkt daran, dass in Bilddateien von Fotos digitaler Kameras (ohne Nachbearbeitung) versteckte Metadaten zur Herkunft des Fotos enthalten sind.
- Auf der Live-CD ist auch ein Programm zum **Scannen** vorhanden, mit dem viele gängige Scanner betrieben werden können. Beachtet aber, dass je nach Scannertyp Daten der gescannten Dokumente im Scanner-Speicher wiederzufinden sind. Daher solltet ihr im Anschluss zumindest einige Nonsens-Dokumente in hoher Auflösung einscannen, damit der Scanner-Speicher wenigstens mit anderen Daten überschrieben wird.
- Was tun, wenn eine **Datei auf CD- oder DVD** vorliegt, die für das Schreiben verwendet werden soll. Leider ist das (einzige) Laufwerk durch die Betriebssystem-CD belegt, sofern ihr nicht genügend RAM für das vollständige Laden der Live-CD habt. Der Ausweg: Das Betriebssystem auf USB speichern, sofern der Computer in der Lage ist, von USB zu starten. Wie das geht, ist auf der Webseite zu eurem Live-Betriebssystem beschrieben. Achtung: Ein USB-Stick kann generell ungewollt mit anderen Daten beschrieben werden. Hier solltet ihr daher unbedingt einen *USB-Stick mit mechanischem Schreibschutzschalter* verwenden! Zum Zwischenspeichern eures Textes muss ein zweiter Stick benutzt werden.

Viel Erfolg!