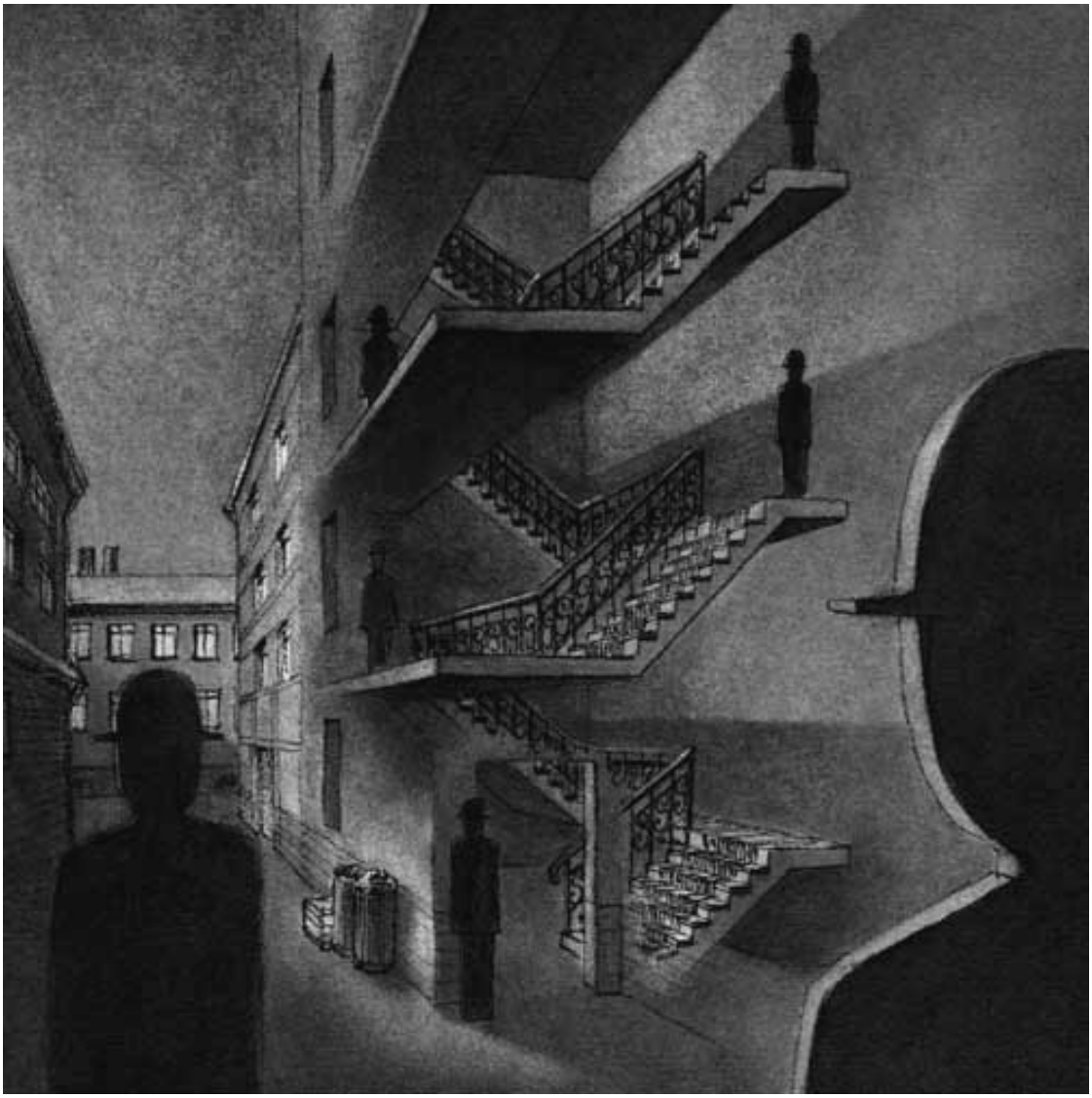
Security Guidelines

Von Sicherheitsmassnahmen zum Sicherheitsbewusstsein

– Ein kleines Handbuch gegen Repression –



Ein Projekt des Antirep-Kollektivs ALARM, 2010

www.antirep-alarm.tk

Inhaltsverzeichnis

1. Einleitung

Staatliche Repression hat zum Ziel, unliebsame Bewegungen zu entkräften. Ein Aspekt davon ist die individuelle Verfolgung und Bestrafung sowie die Spaltung einer ganzen Bewegung. An Einzelpersonen werden Exempel statuiert, um damit eine generelle Angst vor politischem Engagement zu verbreiten. Staatliche Repression kann viele Formen annehmen, von Personenkontrollen, Wegweisungen, strengen Demonstrationsauflagen oder gar -verboten, physischer Gewalt über Überwachung (inkl. dem Einsatz verdeckter Ermittler_innen), Festnahmen und Hausdurchsuchungen bis hin zu unbezahlbar hohen Geldschulden und jahrelangen Haftstrafen. Am Ende stehen meist demotivierte und eingeschüchterte Aktivist_innen. Vor diesem Hintergrund ist es unerlässlich, sich im Vorfeld über Repression Gedanken zu machen – jede und jeden kann es treffen!

Dazu gehört, gewisse Sicherheitsmassnahmen im Alltag konsequent anzuwenden, um die Effektivität von Repression zu minimieren. Das Besprechen gemeinsamer Sicherheitsstandards in der Gruppe ist dabei ebenso gefragt wie die individuelle Abwägung, wie viel Zeit und Energie in Sicherheit investiert wird. Am wichtigsten ist jedoch, dass Menschen und Gruppen sich mit der Thematik auseinandersetzen, um dadurch ein generelles Sicherheitsbewusstsein zu entwickeln.

»Wieso Sicherheitsmassnahmen? Ich habe doch nichts zu verbergen!«

Ein oft gehörter, vermeintlicher Einwand gegen «paranoides Sicherheitsdenken» − er reduziert Repression jedoch auf «legitime» staatliche Strafverfolgung und Kriminalitätsbekämpfung. Er impliziert, dass nur die »kriminellen» Menschen vom Staat bekämpft werden und dass diejenigen, welche sich an die Regeln halten, nichts zu befürchten haben. Abgesehen davon, dass legal keineswegs mit legitim gleichgesetzt werden kann, dient Repression vor allem dazu, Menschen mundtot zu machen, um den Status Quo aufrecht zu erhalten.

Emanzipatorische Bewegungen fordern eine grundlegende Änderung des Bestehenden, was früher oder später an die Schmerzensgrenze der staatlichen «Meinungsfreiheit» und des «demokratischen Pluralismus» stösst. Die «Radikalen», in den Medien gerne als Chaot_innen oder gar Terrorist_innen bezeichnet, werden zur Bedrohung (für die öffentliche Sicherheit, unsere Demokratie usw.) und emanzipatorischer Aktivismus per se zum tendenziell kriminellen Akt. Eine Demonstration wird schnell zum Landfriedensbruch, das Verteilen von Flyern zur Störung der öffentlichen Ordnung. Menschen, die sich politisch legal engagieren und daher angeblich «nichts zu verbergen haben», können so schnell zu potentiellen Extremist_innen stilisiert werden, was wiederum polizei- und geheimdienstliche Massnahmen wie Telefon-, E-Mail- und Videoüberwachung, Beschattung oder andere Formen der Fichierung legitimiert.

Einem eigentlichen Strafverfahren geht, abhängig vom angeblichen «Gefahrenpotential», meist eine lange Phase der Informationsbeschaffung (Überwachung und/oder Infiltration) durch Staatsschutz oder Strafverfolgungsbehörden voraus. Auch der DAP (Dienst für Analyse und Prävention; Staatsschutz) interessiert sich für den so genannten »gewalttätigen Tierschutz». Wie sich im Rechenschaftsbericht des Bundesamts für Polizei[1] nachlesen lässt, befassten sich 2008 im Bereich Extremismus 10 Prozent der Aufträge des DAP mit gewalttätigen Tierschützer_innen (2007 waren es 16 Prozent). Für den Staatsschutz interessant ist das Analysieren der Struktur und der Vernetzung der Tierrechtsbewegung. Wer verkehrt mit wem, wer organisiert was, wer taucht an welchen Anlässen auf, wer äussert sich positiv zu Tierbefreiung etc. Gerne versucht der Staatsschutz dabei auch vermeintliche Rädelsführer_innen auszumachen, so lächerlich diese Vermutung für uns auch scheint.

Gewisse Sicherheitsmassnahmen im Hinblick auf mögliche Repression können helfen, den Schaden sowohl individuell als auch kollektiv zu begrenzen. Je mehr wir uns bewusst sind, mit welchen Mitteln wir ausspioniert werden können, desto mehr können wir diese umgehen, um uns und andere zu schützen. Damit sind simple Verhaltensweisen wie bspw. der Verzicht auf Handys, verschlüsselte Kommunikation oder das sichere Entsorgen politischer Dokumente und Zettel gemeint – denn dadurch können die Überwachungsbemühungen massiv erschwert werden. Sicherheitsmassnahmen können als konsequente Aussageverweigerung verstanden werden: Wenn du den Behörden in Verhören nichts sagen willst, warum dann indirekt durch unverschlüsselte E-

Mails, ungehemmtes Plaudern am Telefon und sonstige Unvorsichtigkeiten? Solltest du einmal von Überwachungsmassnahmen und Repression betroffen sein, bist du froh, einige Massnahmen im Hinblick darauf getroffen zu haben.

1 http://www.ejpd.admin.ch/etc/medialib/data/sicherheit/reberi_fedpol.Par.0010.File.tmp/reberi-2008-d.pdf

---

Beispiele: Grossbritannien, USA, Österreich

SHAC UK 9

Im März 2007 wurden in Grossbritannien, Belgien und den Niederlanden synchronisierte Polizeirazzien durchgeführt – mit über 700 beteiligten Polizist_innen und über 30 Verhafteten. Mit der Zeit wurden einige Anklagen fallen gelassen bzw. einige Angeklagte freigesprochen, bis im Januar 2009 wurden 7 SHAC-Aktivist_innen zu Haftstrafen zwischen 4 und 11 Jahren verurteilt. Ferner wurde ihnen verboten, jemals wieder öffentlich gegen Tierversuche zu protestieren oder Kampagnen zu führen. Vorgeworfen wurde den Verurteilten das «verschwörerische Agieren um HLS zu erpressen».

Mehr Infos: http://www.myspace.com/shacukprisonersupport/

SHAC 7 (USA)

Im Oktober 2006 wurden in den USA 6 Aktivist_innen der Kampagne SHAC zu mehrjährigen Haftstrafen verurteilt. Das den Aktivist_innen zur Last gelegte Verhalten war das Betreiben der SHAC Homepage in den USA, auf welcher sie unter anderem Aktionsberichte der SHAC-Kampagne veröffentlichten. Das Bestrafen einer völlig normalen Sache wurde möglich durch das «Animal Enterprise Terrorism»-Gesetz, welches das Ausüben von Zwang, Gewalt oder Bedrohung als Mittel zur Beeinträchtigung von tierausbeutenden Firmen unter Strafe stellt. Das Wort «Terrorismus» ist bewusst weit gefasst, um legale Proteste (Meinungsfreiheit) einzuschliessen.

Mehr Infos: http://www.shac7.com/

Kriminelle Organisation in Österreich

Im Mai 2008 wurden in ganz Österreich über 20 Wohnungen und Geschäftsräume gestürmt, 10 Personen in Untersuchungshaft genommen «Grund» dafür war der Vorwurf der Bildung einer kriminellen Organisation, welcher die Betroffenen laut den Behörden angeblich angehörten. Die 10 inhaftierten Tierschutz- und Tierbefreiungsaktivist_innen waren über 3 Monate in Untersuchungshaft. Das Ausmass der ganzen Aktion wurde erst nach und nach bekannt. Über Jahre hinweg wurden bestimmte Personen überwacht, abgehört und verfolgt. Trotz aufwändiger Überwachung konnte keinem/keiner Angeklagten irgendeinen konkreten, strafbegründenden Vorwurf gemacht werden. Dennoch müssen sich die 10 Angeklagten seit März 2010 vor Gericht für das Konstrukt einer «kriminellen Organisation» verantworten.

Mehr Infos: http://www.antirep2008.org/

Weitere Verfahren mit dem Vorwurf der “Bildung einer terroristischen/kriminellen Organisation“:

- Tarnac9 (Frankreich): http://tarnac9.noblogs.org/
- October 15th Solidarity (Neuseeland): http://october15thsolidarity.info/
- militante gruppe (Deutschland): http://einstellung.so36.net/de/militante_gruppe/

Das Konstrukt der «kriminellen Organisation» als Bedrohung für politisch Aktive

Eine Repressionswelle, wie sie in Österreich noch immer andauert, ist auch in der Schweiz denkbar. Auch hier gibt es einen ähnlichen Artikel – Art. 260ter im Strafgesetzbuch –, der die Mitgliedschaft in einer kriminellen Organisation unter Strafe stellt:

> «Wer sich an einer Organisation beteiligt, die ihren Aufbau und ihre personelle Zusammensetzung geheim hält und die den Zweck verfolgt, Gewaltverbrechen zu begehen oder sich mit verbrecherischen Mitteln zu bereichern, wer eine solche Organisation in ihrer verbrecherischen Tätigkeit unterstützt, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.»

Aus einer politischen Gruppe lässt sich in der Schweiz also genauso eine kriminelle Organisation konstruieren, die masslose Überwachungsmassnahmen und Verhaftungen/Bestrafungen legitimiert. So «rechtfertigt» der blosse Verdacht auf Mitgliedschaft in einer «kriminellen Organisation» bspw. die Überwachung der Kommunikation (Art. 3 Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs). Weitere mögliche Überwachungsmassnahmen: Observation, Beschattung, Einsatz verdeckter Ermittler_innen, Verwanzung von Wohnungen, Fahrzeugen und Geräten, Installation von Kameras vor Hauseingängen oder in Räumen und allg. (Bewegungs-)Profilerstellung mit allen verfügbaren Daten (öffentliches Auftreten, Telefongespräche, Kontakt mit Behörden, besuchte Webseiten etc.).

Die Gefahr für politisch Aktive (Gruppen oder Einzelne) ist absehbar und immens: Politisch Gleichgesinnte können vom Staat mehr oder weniger willkürlich als «kriminelle Organisation» zusammengefasst und somit kriminalisiert werden. Die Existenz und innere Struktur dieser konstruierten «kriminellen Organisation» wird dann mittels tiefgreifender Überwachung, Beschattung und Infiltration zu belegen versucht. Im Falle einer Verurteilung drohen bis zu 5 Jahre Knast und meistens nahezu unbezahlbare Prozesskosten.

---

2. Individuelles und kollektives Verhalten

Sowohl als Einzelperson als auch in der Gruppe und als Gruppe sollten Sicherheitsmassnahmen beachtet werden. Am besten ist es, wenn Sicherheit als Thema offen angesprochen und diskutiert wird, sodass sich ein generelles Sicherheitsbewusstsein herausbildet. Sicherheit sollte Normalität werden und immer wieder Thema sein, wobei auch Ängste und Kritik nicht tabuisiert werden dürfen. In einem Klima des Vertrauens sollte mensch nicht davor zurückschrecken, auch Freund_innen explizit zu konfrontieren, ohne dass dies als persönlicher Angriff gedeutet wird.

Demos & sonstige Aktionen

Nur kurz: Überlegt euch, was für eine Aktion unbedingt nötig ist. Agendas, Adressbücher, Handies und allg. persönliche Gegenstände sollten zu Hause bleiben. Unerlässlich hingegen sind ein amtlicher Ausweis, etwas Geld und ein klarer Kopf.

Ein ausführlicherer Ratgeber findet sich auf der Homepage der Roten Hilfe Schweiz: http://www.aufbau.org/images/stories/flugis/AntiRep_Broschuere_Keine_Panik_2003.pdf

Exkurs: Aussageverweigerung

Die Aussageverweigerung ist ein fundamentales Recht und wichtig, solltest du mal in ein Strafverfahren verwickelt sein. Grundsätzlich sollte mensch sich bewusst sein, dass Angeschuldigte sich nicht entlasten müssen, sondern dass die Strafverfolgungsbehörden belasten, also die Schuld beweisen müssen. Gelingt dies nicht, gilt mensch als unschuldig. Deshalb sind Polizei und Staatsanwaltschaft auf die Aussagen von Beschuldigten und Zeug_innen angewiesen, umso mehr beim Fehlen anderer Beweise.

Jede Aussage, die du machst, wird grundsätzlich gegen dich und/oder andere verwendet werden. Es ist weitaus sicherer, in einer Extremsituation wie in einem Verhör die Aussage zu verweigern, als zu versuchen, sich zu entlasten. Die verhörende Person ist darauf trainiert, an relevante Informationen zu gelangen und die verhörte Person in Widersprüche zu verwickeln oder zu manipulieren. Alle gemachten Aussagen können unvorteilhaft interpretiert werden und liefern dem Staat darüber hinaus Aufschluss über dein politisches Engagement und dein soziales und politisches Umfeld. Auch kannst du ungewollt weitere Personen belasten und Informationen über sie bekanntgeben.

Selbst wenn in Verhören keine Aussage gemacht wird, ist es immer noch möglich, sich vor Gericht zu äussern. Dies sollte jedoch grundsätzlich mit einem Anwalt oder einer Anwältin abgesprochen werden. Zusammengefasst heisst das, dass die Verweigerung

jeglicher Aussagen nur Vorteile bringt und das nicht nur auf individueller, sondern auch auf kollektiver Ebene.

Als Angeschuldigte_r musst du nicht mehr sagen als deinen Namen, Geburtsdatum, Adresse, Wohnsitz und ungefähre Angabe des Berufs. Zudem bist du nicht verpflichtet, Dokumente (Protokolle etc.) zu unterschreiben. Als Auskunftsperson kommen dir im Prinzip dieselben Rechte zu wie als Angeschuldigte_r. Wirst du als Zeugin verhört, musst du dir bewusst sein, dass dir nur ein eingeschränktes Recht auf Aussageverweigerung zusteht (bspw. als nahe Angehörige des Beschuldigten). Grundsätzlich sind Zeug_innen zur Aussage und Wahrheit verpflichtet und können bei Verweigerung bestraft werden, Beugehaft gibt es hingegen keine.

Beachte: Sowohl Vorladungen der Polizei als auch der Staatsanwaltschaft muss als Angeschuldigte_r unbedingt Folge geleistet werden.

Gespräche

Nicht jeder Ort eignet sich dazu, über politische Themen zu sprechen bzw. Aktionen zu planen. Bei geschlossenen Räumen sollte immer die Möglichkeit in Betracht gezogen werden, dass sie abgehört werden. Auch in der Öffentlichkeit (ÖV, Restaurants, Bars, öffentliche Plätze etc.) können Gespräche – auch ohne technische Hilfsmittel – mitgehört werden. Je sensibler das Gesprächsthema, desto mehr sollte auf die Umgebung geachtet werden.

Protokolle

Protokolle sollten, wenn möglich, keine echten Namen enthalten und auf einem komplett verschlüsselten Computer geschrieben und aufbewahrt werden. Dokumente sollten allgemein nur verschlüsselt verschickt werden.

Papiere/Zettel

Diese sollten nach Gebrauch verbrannt oder geschreddert werden. Der Müll ist ein beliebter Ort für die Behörden, um nach Informationen zu suchen. Deswegen: Ob im eigenen Lokal oder zu Hause, nichts mit politisch relevantem Inhalt in den Müll!

Backups und dezentrales Lagern

Wichtige Dokumente sollten auf mehreren komplett verschlüsselten Computern gespeichert werden (als Backup, falls ein Computer kaputt geht oder beschlagnahmt wird). Ferner sollten auch nicht alle Gruppenbelange über eine Person laufen, d.h. nicht alles sollte bei derselben Person gelagert werden, um im Falle einer Hausdurchsuchung nicht alles zu verlieren und preiszugeben.

Verdeckte Ermittler_innen

Ob von Privatfirmen (z.B. Securitas) oder von der Polizei oder vom Staatsschutz – die Möglichkeit der Infiltrierung einer Gruppe ist real und sollte der Gruppe und den einzelnen Aktivist_innen auch bewusst sein. Generell sollte mensch darauf achten, mit wem was besprochen wird. Je sensibler der Inhalt, desto mehr sollte auf das Vertrauen untereinander geachtet werden.

Ein aktuelles Beispiel aus der Schweiz: Fanny Decreuze alias Shanti Muller, eine Securitas-Spitzelin, spionierte über mehrere Jahre hinweg die autonome Szene aus und war sogar bei einer Antirep-Gruppe in Lausanne aktiv. Unklar ist, ob die Securitas vom Staatsschutz beauftragt wurde.[1]

1 http://www.woz.ch/artikel/rss/16834.html

3. Computer- und Kommunikationssicherheit

Generell gilt: Alles, was über's Internet gesendet oder empfangen wird, kann einfach abgefangen und gelesen werden, insbesondere durch staatliche Behörden (gesetzliche Befugnisse). Deshalb sollte grundsätzlich jede Form der Internet-Kommunikation wie Surfen, Email und Instant Messaging (ICQ, MSN usw.) verschlüsselt werden, um den Inhalt vor fremden Augen zu schützen. Seit dem 1. August 2009 werden auch in der Schweiz alle via Telefon oder Internet übermittelten Daten für sechs Monate gespeichert und auf Abruf verfügbar gemacht (**Vorratsdatenspeicherung!**[1]). Dies ermöglicht eine noch lückenlosere Überwachung – auch rückwirkend.
Ausserdem sind auch auf dem eigenen Computer gespeicherte Daten ein gefundenes Fressen für neugierige Behörden, bspw. durch eingeschleuste Trojaner oder bei einer Hausdurchsuchung (offiziell oder heimlich). Grundsätzlich ist die Verwendung von Windows aus Sicherheitsgründen zu überdenken. So ist z.B. der Programmcode nicht einsehbar, Viren- und andere Schadsoftware weit verbreitet und die Grundeinstellungen des Systems sind unsicher. Sicherere und zudem kostenlose Alternativen bieten Linux-Distributionen wie Ubuntu[2] oder openSUSE[3].
Die folgenden Kapitel sind bewusst minimalistisch gehalten, da sämtliche Informationen und Anleitungen bereits zigfach im Internet verfügbar sind. Die Texte in den von uns gewählten Links sind sehr ausführlich, sodass es allen möglich sein sollte, diese zu verstehen und sich das Wissen anzueignen.

1 http://www.woz.ch/artikel/2009/nr29/schweiz/18143.html

2 http://www.ubuntu.com/

3 http://www.opensuse.org/

Achtung: Keine Verschlüsselung ist unknackbar; die Sicherheit hängt wesentlich von der Wahl des Passworts und vom Verhalten des Individuums ab.
Sichere Passwörter finden sich nicht in Wörterbüchern, sind nirgends aufgeschrieben, haben eine Länge von mind. 25 Zeichen und bestehen aus einer Mischung aus Gross-/Kleinbuchstaben, Zahlen und Sonderzeichen.

Email-Verschlüsselung mit PGP / GPG

Emails sind wie Postkarten. Selbst wenn die Verbindung zum eigenen Email-Konto verschlüsselt erfolgt, ist es für die Behörden ein Leichtes, über den Anbieter (z.B. GMX) Zugang zum Konto und damit zu den empfangenen bzw. verschickten Emails zu erhalten. Daher ist es unabdingbar, den Inhalt der Email-Kommunikation zu verschlüsseln. Hierfür hat sich das Programm GPG, der Ableger von PGP (Pretty Good Privacy), bewährt.
Die einfachste Lösung zur Nutzung von GPG unter Windows bietet das Programmpaket Gpg4win[1]. Die Installation und Einrichtung werden im Handbuch zu Gpg4Win[2] sehr ausführlich mit Bildern erklärt.

Im Folgenden eine Kurzanleitung (Handbuch benutzen!):

1. Download und Installation von Gpg4Win.
2. Schlüsselpaar (öffentlich/privat) erzeugen.
3. Öffentliche Schlüssel austauschen.

> Die Herkunft eines Schlüssels sollte grundsätzlich immer überprüft werden! Dies ermöglicht der «Fingerprint», eine eindeutige Prüfsumme des Schlüssels, die über einen «sicheren Kanal» (persönliches Gespräch, Telefonat u.ä.) kommuniziert und verglichen werden sollte. Den «Fingerprint» findet mensch in den Eigenschaften des betreffenden Schlüssels.

4. Verschlüsseln/Entschlüsseln von Mails.

> Im Handbuch wird das Vorgehen mit «WinPT» beschrieben, in neueren Versionen von Gpg4Win wird «Kleopatra» verwendet – die Funktionsweise ist allerdings identisch.
> E-Mails können wesentlich komfortabler durch den Einsatz eines E-Mail-Clients wie Mozilla Thunderbird verschlüsselt werden.

Thunderbird und GPG

1. Download und Installation von Thunderbird[3], Einrichtung des Email-Kontos.
2. Download und Installation des Enigmail-Plugins.[4]

> Wenn eine neue Mail verfasst wird, kann über das Schlosssymbol «OpenPGP» die Verschlüsselung aktiviert werden. Natürlich muss dafür der öffentliche Schlüssel des/der Empfängers/Empfängerin vorhanden sein.

Bei den meisten Linux-Distributionen ist GPG standardmässig enthalten (mit unterschiedlichen grafischen Oberflächen, z.B. GPA, seahorse etc.). Für Benutzer_innen von Mac OS X existiert eine detaillierte Anleitung[5].

1 http://gpg4win.de/

2 http://gpg4win.de/handbuecher/einsteiger.html

3 http://www.mozilla-europe.org/de/products/thunderbird/

4 https://addons.mozilla.org/de/thunderbird/addon/71/ Enigmail-Plugin
http://www.thunderbird-mail.de/wiki/Enigmail_OpenPGP/ Installationsanleitung

5 http://fiatlux.zeitform.info/anleitungen/pgp_macosx.html

Komplettverschlüsselung

Truecrypt (Windows)

Truecrypt[1] eignet sich hervorragend, um Festplatten vollständig zu verschlüsseln - das gesamte Betriebssystem inbegriffen. Ein Hochfahren des PCs ist danach nur noch nach Eingabe des korrekten Passwortes möglich und sämtliche persönlichen Daten sind nach dem Abschalten des Computers sicher verwahrt. Einzige Voraussetzung ist der Besitz eines CD-Brenners.

Eine sehr gute bebilderte Anleitung zum Vorgehen findet sich unter:
http://www.fixmbr.de/truecrypt-anleitung-verschlsselung-der-systempartition/
oder im Privacy-Handbuch des German Privacy Foundation e.V.[2].

LUKS/dm-crypt (Linux)

Viele Linux-Distributionen, etwa Ubuntu[3] oder openSUSE[4], bieten bereits bei der Installation die Möglichkeit einer Komplettverschlüsselung des Systems an.

FileVault (Mac)

Eine Komplettverschlüsselung unter Mac OS X ist bisher nicht verfügbar, allerdings kann zumindest der Home-Ordner mit dem Programm FileVault verschlüsselt werden[5]. Letzteres steht jedoch wegen einiger Schwachstellen in der Kritik[6].

1 http://www.truecrypt.org/
2 https://www.awxcnx.de/handbuch.htm
3 http://www.ubuntu.com/getubuntu/downloadmirrors#alternate/
4 http://www.opensuse.org
5 http://docs.info.apple.com/article.html?path=Mac/10.4/de/mh1906.html
6 http://en.wikipedia.org/wiki/FileVault#Criticism

Internet - Surfen

Das Internet hat viele Tücken. Besonders wichtig ist es, beim Surfen statt des Microsoft Internet Explorers einen sicheren Browser zu verwenden, etwa Mozilla Firefox[1]. Dieser kann mittels Plugins/Addons beliebig erweitert und angepasst werden (Menü «Extras/Addons»). Um die Sicherheit des Browsers zu verbessern und die Sammlung personenbezogener Daten durch Dienste wie Google, Amazon etc. einzuschränken, gibt es noch weitere Verbesserungsmöglichkeiten. Die vollständige Anonymisierung des Surfens ist ebenfalls möglich.

Skripte einschränken mit NoScript

Mit dem Firefox-Addon NoScript[2] kann generell das Ausführen von Skripten (kurze Programmroutinen) durch Internetseiten unterbunden werden. Dadurch wird verhindert, dass Schadsoftware durch den Aufruf einer Seite automatisch ausgeführt werden kann. Da viele Seiten für ihre Anzeige z.B. JavaScript benötigen, kann im jeweiligen

Fall deren Ausführen für eine spezifische (vertrauenswürdige) Seite – und nur diese – wieder erlaubt werden. Somit erlaubt NoScript dem User, selbst zu bestimmen, was auf welcher Seite ausgeführt werden darf und was nicht.

Cookies einschränken mit CookieSafe

Das Firefox-Addon CookieSafe[3] ermöglicht es, die Kontrolle über die Speicherung von Cookies[4] durch Websites zu übernehmen. So kann die Speicherung eines Cookies auf Seiten eingeschränkt werden, für die es unbedingt nötig ist, etwa für den Login beim Email-Provider oder beim Einkaufen in einem Webshop (eBay, Amazon usw.).

Den Referrer manipulieren mit RefControl

Ein Referrer ist die Internetadresse der Webseite, von der der/die Benutzer_in durch Anklicken eines Links zu der aktuellen Seite gekommen ist. Mit dem Firefox-Addon RefControl[5] kann der Referrer auf verschiedene Weise verändert oder unterdrückt werden.

Surfverhalten anonymisieren mittels TOR

Mit dem Programm TOR[6] kann das gesamte Surfverhalten anonymisiert werden. Eine einfach verständliche Erklärung des Funktionsprinzips[7] und der Installation[8] findet sich auf der Seite der Entwickler_innen.

Mit dem Firefox-Addon Torbutton[9] lässt sich per Knopfdruck zwischen dem normalen und dem mittels TOR anonymisierten Surfen komfortabel umschalten.

Ob alles korrekt funktioniert, kann auf der Website https://torcheck.xenobite.eu getestet werden.

1 http://www.mozilla.com/de/

2 https://addons.mozilla.org/de/firefox/addon/722/

3 https://addons.mozilla.org/de/firefox/addon/2497/

4 https://secure.wikimedia.org/wikipedia/de/wiki/HTTP-Cookie/

5 https://addons.mozilla.org/de/firefox/addon/953/

6 http://www.torproject.org/easy-download.html.de

7 http://www.torproject.org/overview.html.de

8 http://www.torproject.org/documentation.html.de

9 https://addons.mozilla.org/de/firefox/addon/2275/

Internet – Web 2.0

Profilerstellung mittels Facebook, StudiVZ, MySpace & Co.

Auf eigenen Websites besteht die Möglichkeit, Fotos hochzuladen, Beiträge zu schreiben, sich mit anderen Menschen und Gruppen zu vernetzen etc. Dadurch entsteht eine Fülle an Informationen über die eigene Person, welche für alle (insbesondere auch für staatliche Organe) leicht einsehbar und sehr interessant sein kann. Wer dies nicht möchte, sollte auf die Profilierung im Internet verzichten.

Mensch sollte sich auch bewusst sein, dass im Internet publizierte Artikel, Texte, Beiträge etc., in denen der eigene Name vorkommt, noch lange im Internet verfügbar sein können. Dies wird dann zum Nachteil, wenn sich bspw. ein_e potentielle_r Arbeitgeber_in über eine_n Bewerber_in informieren will.

Chatten

Die verbreiteten Instantmessenger wie ICQ, MSN, GoogleTalk etc. sind weder anonym noch verschlüsselt. Private Unterhaltungen können daher leicht mitgelesen/mitgehört werden. Auch die verschlüsselten Dienste von Skype müssen als unsicher eingestuft werden, da nicht transparent ist, was das Programm eigentlich macht und von einer Kooperation zwischen Skype und der Polizei auszugehen ist.

Alternativ kann zum Chatten Jabber verwendet werden und/oder eine Verschlüsselung der Kommunikation mittels GPG/PGP oder dem OTR-Plugin (Off-The-Record Messaging[1]). Hierfür gibt es eine Vielzahl geeigneter Programme, z.B. Pidgin (Windows, Linux), Miranda (Windows), Adium (Mac) etc.

Eine gute Übersicht bietet https://secure.wikimedia.org/wikipedia/de/wiki/Multi-Protokoll-Client/.

1 http://www.cypherpunks.ca/otr/ OTR für Pidgin

http://wasistjabber.tagkaffee.de/konfigurationv.pidginotr.html Anleitung für OTR

Festnetz- und Mobiltelefone

Ebenso wie alles andere können auch Telefone aller Art abgehört werden. Dies kann sowohl aktiv (beim Telefonieren) als auch passiv (Telefon als Wanze) geschehen. Darüber hinaus kann der Standort von Handys bestimmt und Bewegungsprofile erstellt werden.

Es empfiehlt sich, die Verwendung von Handys zu minimieren bzw. diese beim politischen Engagement generell zu Hause zu lassen. Notfalls kann immer noch der Akku entfernt werden, um die Überwachung zu vermeiden. Dabei ist zu beachten, dass es bei einer laufenden Überwachung verdächtig ist, wenn mehrere Personen ihre Handys zur gleichen Zeit ausstellen bzw. den Akku entfernen und so gesehen gleichzeitig vom «Radar» verschwinden.

Hinweis

Die Security Guidelines erheben keinen Anspruch auf Vollständigkeit. Sie sollen allerdings beständig ergänzt und erweitert werden.

Kritik und Verbesserungsvorschläge bitte an alarmail@immerda.ch.

---

4. Weiterführende Links

Antirep-Gruppen

- Rote Hilfe International http://rote-hilfe.de/
- Anarchist Black Cross (Berlin) http://www.abc-berlin.net/

Computer-/Kommunikationssicherheit

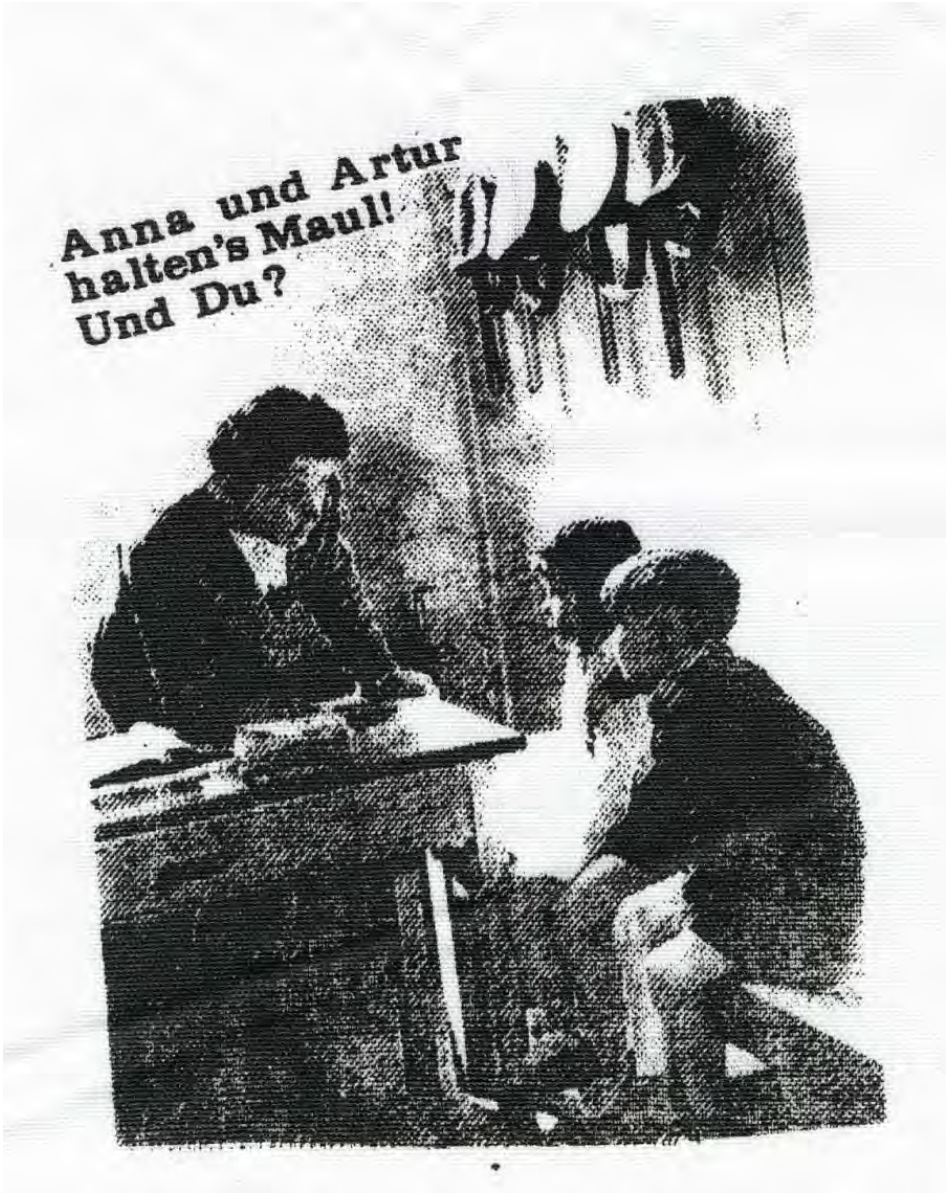
- German Privacy Foundation https://www.awxcnx.de/
- CryptoCD http://cryptocd.org/

Hilfreiche Broschüren

- Flyer zu Hausdurchsuchungen http://gipfelsoli.org/static/Media/Repression/hausdurchsuchungsflyer_carambolage.pdf
- Aussageverweigerung und Verhörmethoden http://aussageverweigerung.info/Aussageverweigerung.pdf
- viele weitere: http://gipfelsoli.org/Antirepression/436.html/

Buchtipp

Wege durch die Wüste – Ein Antirepressionshandbuch für die politische Praxis
Was tun, wenn die Repression uns in Form von Ermittlungen, Platzverweisen, Festnahmen, Überwachung, Durchsuchungen, Vorladungen ... trifft? Grundlegend überarbeitet bietet der Ratgeber nicht nur einen schnellen Überblick. Er vermittelt zu allen Themen auch die weitergehenden Zusammenhänge, verweist auf Erfahrungen aus der politischen Praxis und Diskussionen, die für einen Umgang mit Repression unverzichtbar sind.
Zu bestellen unter http://www.unrast-verlag.de/unrast,2,56,7.html/.



www.al-hallmarks.net

animal liberation
hallmarks

for human emancipation
and animal liberation