Security Culture & Digitale Selbstverteidigung

Eine kurze Einführung

* Diese Einführung ist nur eine Informationssammlung mit kurzen Einführungen und Links mit mehr Informationen. Sie hat nicht den Anspruch einen vollständigen Überblick über das Thema zu geben, sie ist vielmehr eine Materialsammlung. Öffnet am besten die Links im Tor Browser*

Um unsere Strukturen zu schützen und Repression und Überwachung durch Staat, Konzerne, Faschist*innen und andere abzuwehren, wurde das Konzept der Security Culture entwickelt. Es geht dabei nicht nur darum Geräte und Emails zu verschlüsseln, sondern Sicherheit als ein ganzheitliches Konzept zu erkennen, dass neben digitaler Sicherheit auch soziale und physische Aspekte betrachtet. Sicherheit ist viel mehr als Verschlüsselung und kann nicht einfach eingekauft werden, egal was Euch Anbieter alles versprechen.

> *Beispiel 1: Wenn Euer Computer toll verschlüsselt ist, ihr aber zu viel Leuten von der nächsten Aktion erzählt habt, kann es trotzdem bei den falschen Leuten landen.*
>
> *Beispiel 2: Ihr verschlüsselt Kommunikation und nur wer davon wissen muss, weiß von der nächsten Aktion, aber das Aktionsmaterial steht offen in eurem Zimmer rum und die Haustür ist offen.*

Dabei ist es auch essentiell zu verstehen, dass Sicherheit nie eine individuelle Entscheidung ist. Es geht genauso um die Sicherheit eures Umfeldes und unserer Strukturen bei der Frage, wie unsere Sicherheitsstandards sind. Insofern kann der Versuch uns und unsere Strukturen zu schützen nur kollektiv funktionieren.
Im folgenden einige wichtige Punkte zu Security Culture und danach mehr Lesematerial nach Themen sortiert.

Einige Fragen und Ideen zu den drei Bereiche von Security Culture:

1. Soziale Sicherheit:

- “Don’t ask, don’t tell” Prinzip

  Beispiel 1: Wenn Menschen letzte Nacht in schwarzer Kleidung spät nach Hause kamen, muss mensch nicht nachfragen, was sie denn so gemacht haben

  *Beispiel 2: Es reicht Freund*innen zu sagen ihr geht jetzt zu einem Plenum, ihr braucht nicht zu sagen von welcher Gruppe oder wo es stattfindet.*
- Nur so viel Wissen wie nötig

- Fragt Euch bei jeder Info die ihr weitergebt, muss die andere Person das wissen. Nicht nur die Information, wer was genau macht, sondern auch wer eine Aktion organisiert, die Netzwerke dahinter, etc. sind für Repression sehr relevant.
  Beispiel: Der Staat versucht koordinierte Aktionen mit gezielter Repression zu verhindern. Dazu gibt es den Konstrukt der Mittäterschaft. Alle bei einer Aktion sollen damit für alles was passiert Mitschuld tragen.
  Repressions-Beispiel: So wurde einer Kletteraktivistin auch das Bauen einer Barrikade bei der A5 Blockade im Rahmen der No Border Action Days zur Last gelegt. Bei den G20 Rondenbarg und den Basel18 Prozessen wurde gar nicht versucht einzelne Straftaten einzelnen Personen zuzuordnen.
- Gilt auch nach Aktionen, Aktionsgemacker gefährdet uns alle
  Beispiel: Wenn ihr andere zu einer Aktion einladen wollt, fragt erst mal, ob mensch überhaupt Zeit und Lust auf eine Aktion hat, bevor ihr mensch konkrete Details nennt.

- Niemensch vertrauen müssen
  Beispiel: Emails bei linken Techkollektiven haben und online PGP Verschlüsselung nutzen (z.B. bei Posteo, immerda) heißt, dass eure Sicherheit komplett von der Sicherheit des Servers abhängt. Wenn ihr aber mit Thunderbird und Enigmail auf eurem eigenen Computer verschlüsselt, kann der Server gehackt werden und eure Emails trotzdem nicht entschlüsselt werden.
  Repressions-Beispiel: Der Emailanbieter Posteo wird vom Staat zum Rausgeben von Nutzerdaten gezwungen. Wer Tor und PGP benutzt bleibt trotzdem anonym und die Nachrichten verschlüsselt, da Posteo keine IP-Adresse und keine Klartextemails rausgeben kann. (zB Transparenzbericht Posteo) Das selbe gilt auch für Riseup! (Canary 2017, Zwiebelfreunde Razzia)
- Verschiedene Aktionsbereiche und -level trennen
  Beispiel: Bei einer offenen Plattform können auf Treffen gut neue Leute gewonnen werden, Themen breiter diskutiert werden, etc. - es ist aber der falsche Ort, um Leute für die nächste militante Aktion zu mobilisieren.

2. Physische Sicherheit

- Wer hat Zugang zu was?
  Beispiel 1: Ist eure Haustüre offen? Wer hat alles einen Schlüssel?

Beispiel 2: Der Raum in dem ihr eure Aktionsmaterialien lagert im AZ, ist er abgeschlossen, wer kann dort alles rein?

- Seid ihr auf Hausdurchsuchungen vorbereitet?

  Beispiel: Habt ihr ein Plakat Checkliste Hausdurchsuchung an die Tür gehängt? Eine Handynummer einer Anwält_in? Habt ihr in der WG schon mal geredet, wie ihr mit so einer Situation umgehen wollt?
- Welche Spuren hinterlasst ihr? (z.B. Fingerabdrücke, bezahlen mit EC-Karte, Video-Aufnahmen, Hausmüll, Flyer, …)
- Welche Räume haben ein besonders hohes Repressionsrisiko? Sollte dort dann Treffpunkte für Aktionen sein?

  Repressions-Beispiel: In Tübingen wurden mehrere Hausprojekte im Jahr 2016 Video überwacht. (siehe Meldestelle) In Hamburg wurde der Infoladen Schwarzmarkt und das Hausprojekt darüber videoüberwacht (Schwarzmarkt Blog)
- Welche Kleidung auf Aktion tragen? Welche Kleidung und Dinge solltet ihr nach Aktionen loswerden?

  Repressions-Beispiel: Sehr häufig werden Kleidungsstücke als Beweise vor Gericht verwendet und bei Hausdurchsuchungen gezielt danach gesucht. (Samba Turnschuhe im Balu Prozess)

3. Kommunikations und digitale Sicherheit

- Umfasst unter anderem: Briefe, Telefon, Email, Chat / Messenger, “Soziale” Netzwerke, digitale Informationen (Daten auf eurem Computer, Cloud, ...), Funk, …
- Bereiche, die wir schützen wollen:
  - Inhalt unserer Nachrichten und Daten
  - Metadaten – z.B. wer redet mit wem, mit welcher Kamera wurde das Bild gemacht, etc.

  Beispiel 1: Ihr benutzt verschlüsselte Messenger, aber der Staat sieht, dass ihr zu Beginn einer Räumung Euch alle gegenseitig kontaktiert → das Netzwerk ist offen gelegt.

  Beispiel 2: Löscht ihr die Metadaten von Bildern und anderen Dokumenten vor dem Hochladen auf Blogs, indymedia, etc.?

  Repressions-Beispiel: In Basel wurden Leute vor Gericht gezerrt für eine Scherben-Sponti, nur weil sie am Tag der Sponti mit anderen Beschuldigten SMS geschrieben hatten. Sie wurden freigesprochen, das stressige Verfahren und die Kosten sind trotzdem entstanden. (siehe Basel18 Verfahren)

- Code-Wörter und Signale: Sind für bestimmte Gegenstände, Orte, Rollen, etc. Code-Wörter und Signale sinnvoll? Wie kommuniziert ihr vor und während Aktionen?
- Welche Daten von Euch finden sich im Internet, speziell sozialen Medien?

  Repressions-Beispiel: Immer häufiger werden Bilder aus “Sozialen” Medien von den Verfolgungsbehörden genutzt. Schon 2011 wurden Facebook Profilbilder zur Identifizierung von Beschuldigten genutzt.

Viele weitere Informationen und Tipps zum Thema Security Culture findet ihr hier:

- *Informationssicherheit für Aktivist*innen* *Broschüre* des ABC Dresden
- *What is security culture?* von Crimethinc
- *Audiozine Security Culture* des ABC AA
- *Eine kurze Anleitung zur digitalen Selbstverteidigung* der WOZ
- Earth First! *Direct Action Manual*
- *Warrior. Crowd control & riot manual*
- Workshops der Gruppe Zucker im Tank, https://zuckerimtank.net
- Anti-Repressions Flyer der Roten Hilfe

Im allgemeinen gilt: Sicherheitsbewusstsein statt Paranoia

Damit ein Sicherheitsstrategie funktionieren kann muss Handlungsfähigkeit erhalten bleiben:

- Ein Sicherheitsstandard der dich handlungsunfähig macht ist eine Vorverlagerung der Repression
- So sicher Arbeiten wie möglich und trotzdem praktikabel bleiben
- In Gruppen darf ein Sicherheitsstandard Menschen nicht ausschließen, stattdessen Skillshare und Workshops bis alle es benutzen können. Aber auch ein zu niedriger Sicherheitsstandard schließt Menschen aus
- Nur kollektive Sicherheitsstandards erreichen Schutz für uns und unsere Strukturen
- Repression trifft uns nicht alle gleich. Aufenthaltsstatus, potenzielle Berufsverbote und Bewährung können zu sehr unterschiedlichen Risiken für Einzelne führen.
- Faulheit ist nicht das selbe wie impraktikabel!

Risikoanalysen

Um nicht unsere Strategie durch Paranoia oder Faulheit zu bestimmen, brauchen wir eine Risikoanalyse und ein daran angepasstes Sicherheitslevel.

Das ist aber keine einmalige Sache, sondern ein dauerhafter Prozess, der auf verschiedenen Ebenen stattfinden muss: individuell, nach Gruppe, nach Thema, nach Aktionsform, …

Erstellung einer Risikoanalyse:

- Wer sind meine Gegner_innen?
- Welche Mittel haben sie und was werden sie voraussichtlich davon einsetzen?
- Was habe ich zu beschützen?
- Was passiert wenn dies nicht gelingt?
- Welche Mittel habe ich zur (digitalen) Selbstverteidigung?
- Was bringt maximalen Schutz vor zu erwartenden Angriffen ohne meine Handlungsfähigkeit zu verlieren?

Ergebnis der Risikoanalyse:

- Sicherheitsstandard aufbauen und zur Routine machen
  - Individuell
  - Situationsbedingt (Gruppe, Aktionslevel, …)
- Technische Mittel besorgen und benutzen lernen
- Sicherheitsbewusstsein etablieren
- Sicherheitsstandard ohne Kompromisse einhalten
- Wenn nicht möglich, überlegen ob zu hoch angesetzt
- Offener Umgang mit Fehlern
- Solidarische Unterstützung und Kritik

Anleitung zur Erstellung einer Risikoanalyse zum Beispiel von der Electronic Frontier Foundation

Beispiele für Sicherheitslevel

Um das ganze nun ein wenig zu konkretisieren, folgt nun eine beispielhafte Einordnung verschiedener Sicherheitslevel. Passt sie jeweils an eure konkreten Umständen an!

Wer soll dabei sein?

1. Es besteht ein sehr hohes Repressionsrisiko und die Aktion ist gut in einer kleinen geschlossenen Gruppe umsetzbar. Nur die, die direkt an der Aktion beteiligt sind, werden informiert. Es wird bei Vor- und Nachbereitung, sowie am Tag der Aktion darauf geachtet, dass Unbeteiligte von dem Ganzen nichts mitbekommen.

2. Es besteht ein erhöhtes Repressionsrisiko und die Aktion braucht nur eine überschaubar große Gruppe an Menschen. Vertraute Unterstützer*innen werden mit einbezogen, aber alle in der Gruppe entscheiden gemeinsam, wer das sein soll. Nur die, die direkt an der Aktion Beteiligten, sowie die ausgewählten Unterstützer*innen, werden informiert. Es wird bei Vor- und Nachbereitung, sowie am Tag der Aktion darauf geachtet, dass Unbeteiligte von dem Ganzen nichts mitbekommen.

3. Teilnehmenden steht es frei andere zur Aktion einzuladen, aber dabei soll klar kommuniziert werden, das nur in vertrauten Kreisen über die Aktion gesprochen werden soll. Die Teilnehmenden organisieren sich in Bezugsgruppen.

4. Gerüchte über die Aktion können weit in der Szene gestreut werden. Aber dabei sollen keine Details erwähnt werden und niemand soll wissen, wer die Aktion organisiert.

5. Die Aktion wird mit sämtlichen Details öffentlich angekündigt.

Wie und über welche Wege soll kommuniziert werden?

1. Es wird nur persönlich über die Aktion geredet und auch nur dann, wenn das absolut notwendig ist. Zu den Treffen nimmt niemensch ein Handy mit und diese finden in Überwachungs-freieren Räumen wie Wäldern, Parks oder beim Spaziergang außerhalb der Stadt statt. Nicht sicher sind deine WG, dein Auto, das Café wo du Stammkundin bist, dein lokaler Infoshop oder das autonome Zentrum.

2. Diskussionen werde ohne Handy in halbwegs Überwachungs-armen Räumen geführt und außerhalb der WG der Beteiligten. Per verschlüsselter Mail (kein online PGP) kann über den Termin von Treffen, aber nicht über den Inhalt der Aktion, kommuniziert werden. Die Beteiligten nutzen verschlüsselte Computer mit open-source Software (nicht Windows, Mac, ..) oder Tails, keine Smartphones zur Kommunikation.

3. Diskussionen können in Wgs stattfinden, in denen akute Überwachung unwahrscheinlich ist. Auch hierbei sind keine Handys oder andere Geräte mit Internet im Raum. Teilnehmende können über verschlüsselte Mails kommunizieren.

4. Teilnehmende können über die Aktion per Handy und Mail reden, auch unverschlüsselt, aber es dürfen keine Details wie “wer, wann und wo” erwähnt werden.

5. Alle Details können öffentlich geteilt werden, entweder persönlich, per Handy oder Mail.

Spitzel

Spitzel sind eine Realität, überlegter und informierter Umgang mit dem Thema sind daher wichtig. Keine unüberlegten Vorwürfe oder Gerüchte = Bullen die Arbeit abnehmen!

Es ist dabei wichtig sich über aktuelle Enttarnungen informieren und Gesichter merken. Und allgemein dieses Thema das Ursache für viel Unsicherheit ist, in den eignen Strukturen thematisieren und einen guten Umgang gemeinsam finden.

Repressions-Beispiel: Im Umfeld der Roten Flora in Hamburg wurden bereits vier Spitzel enttarnt. (Übersicht auf dem Enttarnung Blog*) Der bereits 2015 als Spitzel geoutete Marcel Göbel, versucht immer wieder Zugang zu linken Räumen zu bekommen, zuletzt 2019 beim Hambi-Camp während des Skillshares. (*indymedia*)*
*Auch scheinbar "harmlose" / "uninteressant" scheinende Politikfelder wurden schon von Spitzeln infiltriert, wie sich am Beispiel Simon Bromma zeigt, der in Heidelberger Studikreisen unterwegs war. (*Spitzelklage Blog*)*

Wenn ihr euch gerne mehr zum Thema informieren wollt:

- *Schöner Leben ohne Spitzel, ein Ratgeber* der Antifaschistischen Linken Berlin
- *Was my friend a Spycop?* der Undercover Research Group
- *Anti-Repressions Flyer Anquatschversuche* der Roten Hilfe

Wichtige Fragen, die ihr vor jeder Aktion klären solltet

- Wie öffentlich soll eine Aktion sein?
- Welche Menschen sollen eingeladen werden?
- Welche (technologischen) Kommunikationswege werden für welche Informationen genutzt?
- Kurz: WER soll WAS WANN auf welchem WEG wissen?

Denkt daran: Das Sicherheits-Level kann später noch gesenkt werden, aber umgekehrt ist das schwierig! Wägt dabei auch ab, ob ihr mit dem gewählten Sicherheits-Level noch vernünftig arbeitsfähig seid.

Weiteres Material

- Repression
  - *Wege durch die Wüste. Ein Antirepressions-Handbuch für die politische Praxis* des Autor*innenkollektivs erschienen im Verlag edition assemblage
  - *In Bewegung. Praxishandbuch für linke Aktivist_innen bezogen auf die Rechtslage in der Schweiz* des Verein AntiRep Bern (Hg.) erschienen im unrast Verlag
  - *Maßnahmen gegen Observation* von Luchs.
  - *Der Hunger des Staats nach Feinden. §129* der Roten Hilfe
  - *Broschüre Aussageverweigerung* der Roten Hilfe
  - Tipps vom EA Berlin
  - Trouble #4 No Justice, just us Video von sub.media

- Digitale Selbstverteidigung
  - Sicherheitstipps des Riseup Tech-Kollektivs
  - *Tails Heft* des Capulcu Kollektivs
  - *Anleitungen zu Verschlüsselung und Computer-*Sicherheit des Mtmedia Tech-Kollektivs
  - *D*u kannst alles hacken, du darfst dich nur nicht erwischen lassen Talk von Linus Neumann und Thorsten Schröder
  - *Verhalten bei Hausdurchsuchungen* Talk von Kristin Pietrzyk
  - *Android Smartphones Google-frei einrichte*n von Systemli

Danke an Earth First! für das Direct Action Manual und ABC Dresden für die Broschüre Informationssicherheit für Aktivist*innen auf denen diese Sammlung aufgebaut ist.