Eine kurze Einführung zu

Security Culture

*diese Kurzinfo hat keinen Anspruch einen vollständigen Überblick über das Thema zu geben
[Vgl. ignite! Workshopkollektiv: https://ignite.blackblogs.org]

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.

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.

Die drei Dimensionen der Security Culture:

1. Soziale Sicherheit

☆ „Don‘t ask, don‘t tell“ Prinzip

*Beispiel 1: Es reicht Freund*innen zu sagen ihr geht zu einem Plenum, ihr braucht nicht zu sagen von welcher Gruppe oder wo es stattfindet.*
Beispiel 2: Wenn Menschen letzte Nacht in schwarzer Kleidung spät nach Hause kamen, muss mensch nicht nachfragen, was sie gemacht haben.

☆ Nur so viel Wissen wie nötig

Fragt euch bei jeder Info, die ihr weitergebt, muss die andere Person das wissen. Nicht nur Informationen, wer was genau macht, sondern auch wer eine Aktion organisiert, die Netzwerke dahinter, etc. sind für Repression sehr relevant.

Wichtig: Gilt auch nach Aktionen, Aktionsgemacker gefährdet uns alle!

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

☆ Seid ihr auf Hausdurchsuchungen vorbereitet?

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? Ist bei euch aufgeräumt? Kalender, unverschlüsselte Sticks/ Handys/ Laptops sind bei eine Hausdurchsuchung

das größte Geschenk für die Repressionsbehörden.

☆ Welche Spuren hinterlasst ihr?

z.B. Fingerabdrücke, bezahlen mit EC-Karte, Video-Aufnahmen, Hausmüll, Flyer, SMS, Metadaten…

☆ Welche Räume haben ein besonders hohes Repressionsrisiko? Sollten dort dann Treffpunkte für Aktionen sein?

Repressions-Beispiel: In Tübingen wurden mehrere Hausprojekte im Jahr 2016 Video überwacht. In Hamburg wurde der Infoladen Schwarzmarkt und das Hausprojekt darüber videoüberwacht. Die KTS wurde 2014 videoüberwacht und 2017 durchsucht.

☆ Welche Kleidung auf Aktionen 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.

3. Kommunikation und digitale Sicherheit

☆ Umfasst u.a.: Briefe, Telefone, Email, Chat/Messenger, „Soziale"-Netzwerke, digitale Informationen (Daten auf 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.

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 haben.

☆ Bedenke, dass unverschlüsselte Kommunikation (Mails, SMS, http statt https) unglaublich einfach zu überwachen ist.

☆ Mache vor einem Treffen/ einer Aktion niemals dein Handy aus!

Lege es entweder angelassen beiseite oder lass es Zuhause. Wenn 10 Leute gleichzeitig ihr Handy ausmachen lässt sich daraus schließen, dass sie sich treffen und nicht belauscht werden wollen. Repressionsbehörden lieben solche Metadaten und kommen (sogar im Nachhinhein) problemlos an sie heran.

☆ Welche Daten verbreitest du im Internet, speziell sozialen Medien?

Repressions-Beispiel: Immer häufiger werden Bilder aus „Sozialen"-Medien von den Verfolgungsbehörden zur Identifizierung von Beschuldigten genutzt.

Im Allgemeinen gilt: Sicherheitsbewusstsein statt Paranoia!

<u>Damit eine Sicherheitsstrategie funktionieren kann, muss Handlungsfähigkeit erhalten bleiben:</u>

☆ 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 nutzen 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 dasselbe wie impraktikabel!