Gruppensicherheit

Hier findest du:

- Informationen zum Thema Sicherheitskonzepte für Gruppen und Aktivist:innen.
- Hintergrundinformationen und einen Leitfaden für die Erstellung eines für dich und deine Gruppe passendes Sicherheitskonzept.
- Workshopideen für deine Gruppe.

Zur Notwendingkeit von Sicherheitskonzepten für Gruppen

„Ich sitze in einer Runde mit Freund:innen und erzähle ihnen ein Geheimnis. Das ist möglich, weil ich ihnen vertraue. Ich sitze in einer Runde mit einem Rechtshilfekollektiv und erzähle über einen Repressionsfall bei dem ich betroffen bin. Das ist möglich, weil ich ihnen vertraue.“

Das Teilen von sensiblen Inhalten erfordert auf der einen Seite Vertrauen und auf der anderen die Verantwortung mit diesem geschenkten Vertrauen umzugehen. Es ist ein wechselseitiges Verhältnis.

Im direkten Gespräch mit meiner Gruppe muss ich meinen Gegenübern vertrauen, dass sie verantwortungsvoll mit den anvertrauten Informationen umgehen. Auch muss ich darauf vertrauen können, dass niemand zuhört und mithört: Darum spreche ich über Dinge, die nur für unsere Ohren bestimmt sind, nicht im Café oder im Nahverkehrsbus.

Wenn ich mich aber nicht persönlich treffe, sondern mit Hilfe von digitaler Kommunikation - Textnachrichten, Emails, Telefonie, Online-Portalen, Online-Pad, etc. - austausche, dann brauche ich auch Vertrauen darauf, dass alle mit denen ich kommuniziere auch verantwortungsvoll mit diesen Kommunikationsmitteln umgehen und auch umgehen können - nicht nur was verschlüsselte Kommunikation selbst angeht, sondern auch was die Aufbewahrung, Speicherung und Löschung von anvertrauten Informationen betrifft.

Das trifft insbesondere dann verstärkt zu, wenn Repressionsbehörden unsere Sicherheit bedrohen. Daher muss eine politisch arbeitende Gruppe notwendiger Weise Platz für die Thematisierung von Repression allgemein und klugen Strategien zu digitaler Selbstverteidigung im Konkreten bieten. Mit der Thematisierung geht auch einher im Kollektiv Sicherheitsstandards zu entwickeln.

Warum wir uns alle mit digitaler Sicherheit auseinandersetzen müssen erklären wir auch in unserem Eingangsstatement

Entwickeln und Etablieren eures Sicherheitskonzeptes

Schritt 1: Bestandsaufnahme - Analyse der Situation

Bei der Entwicklung von Sicherheitsstandards dreht sich zunächst alles um die Fragen: Vor was wollen wir uns schützen und wie wird die gesamte Gruppe geschützt? Dabei übernimmt jede:r die

Verantwortung mit Vertrauen im entsprechenden Maß umzugehen. Damit wir in der Gruppe alle vom Gleichen reden und ein gemeinsames Bild von notwendigen Sicherheitsmaßnahmen entwickeln können, empfehlen wir das gemeinsame Gespräch.

Wir haben einige Fragen zur Auseinandersetzung in der Gruppe vorbereitet. Dabei sollte im Mittelpunkt stehen, dass alle in der Gruppe sich dazu äußern können und sollen wie es ihnen persönlich damit geht. Der Austausch ist ein vertrauensvoller, wir wollen ja dass alle sich mit Selbstvertrauen der digitalen Selbstverteidung annehmen!

Bestandsaufnahme

Wie kommunizieren wir in der Gruppe miteinander? Sammelt eure Kommunikationsmittel

- *Messenger, E-Mails, Forum, Plenum,...*

Wie werden die Daten geschützt? Verschlüsseln wir unsere Datenträger?

- *Computer, Handies, USB-Sticks, externe Festplatten*

Welche gemeinsam verwalteten Accounts nutzen wir?

- *Wer hat Zugang zu den Accounts?*
- *Wie werden die Passwörter weitergegeben?*
- *Wann werden Passwörter gewechselt?*
- *Verwenden wir Anonymisierungtools für den Zugriff auf diese Accounts (wie den Tor Browser)?*

Wie gehen wir in der Kommunikation mit sensiblen Gruppeninfos um?

- *Aktionen und Projekte in Chats*
- *Wo werden Protokolle gespeichert und wie haben alle darauf Zugriff*
- *Verwenden wir unsere Namen in Chats, Foren, Emails, Protokollen,...*

Auf welche Sicherheitsstandards achten wir bei etwaigen Außenauftritt?

- *Verwenden wir Gruppenhandies, Gruppenlaptops?*
- *E-Mail Konten und Emailverkehr*
- *Social-Media Konten (Metadaten von Bildern, Verpixelung von Gesichern,..)*

Workshopidee Teil 1: Ein gemeinsames Bild als Gruppe bekommen

Alle diese Fragen auf einmal zu beantworten, wird wohl ein wenig überfordernd sein. Nehmt euch ein Thema nach dem anderen vor, vielleicht bereitet jemand aus der Gruppe kleine Workshopeinheiten vor. Wenn wer etwas vorbereitet könnt ihr auch gut überlegen, welche Fragen für euer Konzept wichtig sind und ihr könnt obige Fragen auf eure Bedürfnisse anpassen.</color>

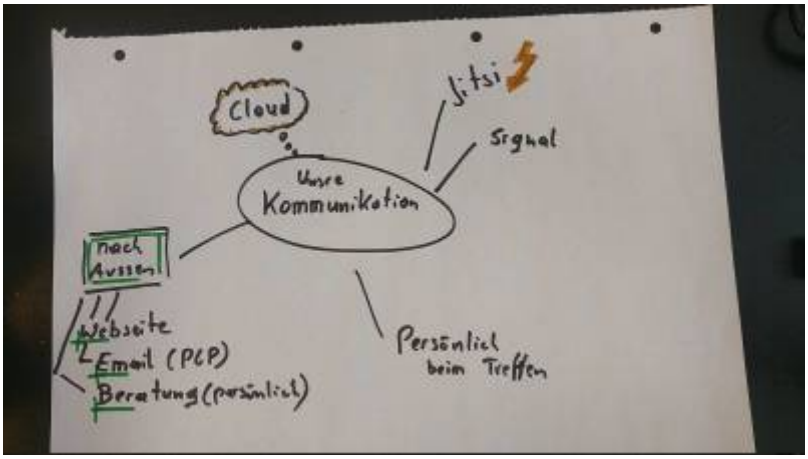
Ihr könnt in das Thema einsteigen, indem ihr euch über eure persönlichen Zugänge zum Thema Digitale Sicherheit austauscht.
Für den Austausch geht ihr in Dreiergruppen zusammengehen und könnt euch so in kleinem Rahmen zu folgenden Fragen austauschen:

```
◊ Wie schützt du dein Smartphone?
◊ Wie sicher sind deine Passworte?
◊ Was denkst du ist die größte Sicherheitslücke in deiner Nutzung?
```

Erzählt euch gegenseitig eure individuellen Antworten auf die Fragen. Das Zeitlimit kann etwa 30 Minuten sein. Anschließend kommt ihr wieder als gesamte Gruppe zusammen und fasst Erkenntnisse aus diesen > Gesprächen zusammen.

In einem nächsten Schritt könnt ihr gemeinsam auf einem Flipchart-Papier sammeln mit welchen Mitteln ihr miteinander kommuniziert.

Das kann so aussehen:



Anschließend tauscht ihr euch wieder über eure Eindrücke zu den gesammelten Kommunikationsmitteln aus:

```
◊ Wissen alle Gruppenmitglieder von diesen Kommunikationsmitteln?
◊ Seid ihr Zufrieden wie diese Kommunikationmittel verwendet werden?
◊ Braucht es vielleicht ein Kommunikationskanal den ihr noch nicht habt?
```

Mit diesem oder ähnlichen Vorgehen, könnt ihr euch Schritt für Schritt ein gemeinsames Bild erarbeiten was für Herausforderungen für die Gruppe zu bewältigen sind, den gemeinsamen Prozess starten.

Beachtet dabei drei Grundlagen:
◊ In diesem ersten Schritt geht es darum ein gemeinsames Bild zu bekommen - noch NICHT um Lösungen.
◊ Nehmt euch bewältigbare Stückchen vor. Ein Sicherheitskonzept wird nicht auf einem einzelnen Treffen entstehen.
◊ Nehmt euch gegenseitig mögliche Ängste: Schafft ein Gesprächsklima in dem alle sich äußern mögen.

Schritt 2: Wissen und Unterstützung für Alle

Leider ist es so, dass das Wissen darüber was wichtig ist bei Sicherheit auf der digitalen Ebene, nicht weit und gerecht verteilt ist. Im besten Fall hat man in der Gruppe mindestens eine Person, die sich

dabei etwas besser auskennt und bereit ist, diese Fähigkeiten weiterzugeben in Form eines Workshops zum Beispiel. Die Bereitschaft das eigene Wissen und Können auch zur Verfügung zu stellen, soll im Sinne der Selbstorganisierung gedacht werden und nicht etwa den Charakter einer Serviceleistung einnehmen.

Findet sich dieses Wissen nicht im Mindestmaß innerhalb der Gruppe, gibt es die Möglichkeit um Hilfe bei der Erstellung des eigenen Sicherheitskonzeptes bei anderen linken Gruppen anzufragen, welche sich intensiver mit solchen Fragen beschäftigen.

Um innerhalb der Gruppe zu gewährleisten, dass der Umgang um Wissen mit digitaler Sicherheit transparent und ansprechbar bleibt, soll dem Thema auch bewusst Raum gewidmet werden. Sicherheit geht vor Bequemlichkeit! Macht euch Gedanken darüber wie ihr im stetigen Austausch über Unsicherheiten und Neuigkeiten in diesem Bereich bleibt.

Workshopidee Teil 2: Notwendige Änderungen besprechen

Nachdem ihr etwa in Schritt 1 eine gemeinsame Bestandsaufnahme gemacht habt könnt ihr euch als Gruppe über Änderungen und Überarbeitungen unterhalten:

```
◊ Bei welchem Thema oder Tool müssen wir als Gruppe nachsteuern?
◊ Welche Tools oder welches Nutzungsverhalten wollen wir über Bord werfen?
◊ Wo brauchen wir eine andere Lösung?
◊ Wer benötigt in der Gruppe Unterstützung bei der Verwendung?
```

Schritt 3: Anregungen zum Standards entwicklen

Jede Person sollte sich mit ihren eigenen Sicherheitsstandards beschäftigen

- Tipps für deinen persönlichen Sicherheitsplan findest du hier im Wiki.

o Passwortsicherheit

- Verwendet unbedingt sichere Passworte! Diese sollten auch sicher aufbewahrt werden und wenn sie weitergegeben werden: auf sicherem Weg kommuniziert werden.

o Verschlüsselung von Daten und Endgeräten

- Alles was die Gruppe betrifft soll nur auf verschlüsselten Geräten benutzt und gespeichert werden.

o Anonymität

- Wenn ihr anonym im Internet auf Webseiten zugreifen wollt, empfehlen wir den Tor-Browser.
- Für umfassendere Anonymität (auch für Kommunikation) empfehlen wir das portable Betriebsystem Tails als bequeme und sichere Lösung.

o Gruppenaccounts

- Wenn möglich solltet ihr einzelne User anlegen mit individuellen Passworten, die sicher aufbewahrt werden.
- Wenn es ein „Gruppenpasswort“ geben muss/soll: Wer hat den Überblick darüber? Regelmäßige Passwortwechsel an definierten Passwortwechseltagen helfen auch hier, die Sicherheit zu stärken.
- Stellt euch die Frage: Ist es eventuell sinnvoll, dass auf den Account ausschließlich anonym zugegriffen wird?

o Aufbewahrung von Unterlagen, Löschen von Daten, Datenvermeidung und Vernichten von Unterlagen

- Achtet darauf, dass Daten nur verschlüsselt aufbewahrt werden. Am besten alle Datenträger verschlüsseln.
- Wie ihr Daten sicher löschen könnt, findet ihr hier im Wiki
- Nicht alles was ihr besprecht und verschriftlicht, muss auch auf Dauer aufbewahrt werden. Löscht alte Archive und Dokumente.
- Achtet auch außerhalb des Computers auf eure Daten und lasst sie nicht einfach rumliegen, ein Schredder/Aktenvernichter kann hier sehr hilfreich sein.

o Austausch von Daten

- Eine einfache und sichere Möglichkeit ist die Übergabe eines verschlüsselten USB-Stick.
- Auch verschlüsselte E-mails sind eine gute Option.
- Ihr könnt verschlüsselte Ordner über eine Cloud teilen. Achtet jedoch auf einen vertrauenswürdigen Anbieter, *Nextcloud* über das linke Technikkollektiv Systemli wäre eine Option

o Gemeinsames Arbeiten an Dokumenten

- Ob Pads, Forum oder Wiki: Achtet auch hier darauf wie und wo eure Daten gespeichert werden.

o Sichere digitale Kommunikaton

- Achtet darauf nur verschlüsselt zu kommunizieren, mehr dazu hier im Wiki.
- Je nach Organisierung und Themen sind vielleicht unterschiedliche Arten der Kommunikation angebracht. Stellt euch die Frage: Soll eine langfristige Organisierung wirklich hauptsächlich über einen „instant messenger“ (z.B. Signal) ablaufen oder benötigt ihr dafür auch andere Technologien wie Email oder ein Forum?
- Anonyme Arten der Kommunikation wären z.B. Emails verschicken über Tails oder die Android App Briar
- Datenvermeidung: Nicht jede Kommunikation sollte für immer gespeichert werden - was nicht da ist, kann dir auch nicht zum Verhängnis werden. Ihr könnt das in den meisten Programmen einstellen, dass alte Nachrichten automatisch gelöscht werden. Oder ihr müsst eben von Zeit zu Zeit aufräumen.
- Manche Dinge sollten überhaupt lieber von Angesicht zu Angesicht an einem sicheren Ort besprochen werden.

o Gruppenemail

- Erstellt euch einen Email-Account bei einem vertrauenswürdigen Anbieter z. B. Systemli
- Wer soll Zugriff auf den Account haben und wie werden die Zugangsdaten sicher weitergegeben.
- Wenn es anonym sein soll → Verwendet das Betriebssystem Tails

- schreibt verschlüsselte Mails

o Protokolle

- Worauf schreibt ihr Protokolle? Verwendet z.B. einen verschlüsselten Computer oder das portable Betriebssystem Tails
- Wo speichert ihr, oder wie verschickt ihr eure Protokolle?
- Achtet auch darauf, dass Protokolle nicht irgendwo liegen gelassen werden, ob digital oder ausgedruckt.

o Aussenauftritte - Fotos, Texte, Videos

- Bevor ihr Fotos, Dokumente,.. hochladet bereinigt sie von Metadaten
- Vor einer Veröffentlichung sollten ihr auf Bildern und Videos Gesichter unkenntlich gemacht werden. Wie ihr Gesichter und Fototeile verpixelt findet ihr hier im Wiki.

o Social Media Sicherheit

- Macht euch mit den Sicherheits- und Datenschutzeinstellungen der Socialmedia-Plattformen bekannt und achtet darauf was ihr postet Tipps zu Privacy-Einstellungen in Webkonten
- Sollen wir anonym auf die Plattform zugreifen?
- Was stellen wir hoch und was legen wir dadurch über uns und andere offen?
- Veröffentlicht keine Namen und Gesichter.
- Achtet auch gerade dann auf Anonymität auf wenn ihr etwa Videos oder Fotos von Übergriffen der Polizei online stellt: Das kann üble Anzeigen und Gerichtsprozesse aufgrund des Schutzes des Persönlichkeitsrechtes einzelner Polizist:innen nach sich ziehen.

o Sichere Gespräche und Räume von Angesicht zu Angesicht

- Mit wem rede ich?
- Ist das Handy mit im Raum? Vergesst nicht: Das Telefon ist ein wandelndes Mikrofon immer mit dem Internet und dem Telefonnetz verbunden.
- Wo rede ich über was? Nicht jedes Thema gehört in den Bus oder das Cafe

Schritt 4: Am Laufenden bleiben - Plädoyer für regelmäßige Sicherheits-Treffen

Wir plädieren dafür Raum und Zeit zu schaffen um Sicherheitskonzepte zu etablieren! Dazu kann auch gehören, dass ein Teil eines Treffens auch diesem Thema gewidmet ist - nicht nur in der Erstellung des Konzeptes sondern gerade auch im Alltag.

Sicherheitsstunde: Warum nicht immer die letzte Stunde des ersten Treffens im Monat mit Passwörtern, Programmen und Sicherheit verbringen: Die *„Sicherheitsstunde“* dient der praktischen Hilfestellung bei der ihr euch gegenseitig unterstützt.

o Passwörter ändern

Bei kritischen Passwörtern in eurer Gruppe solltet ihr diese regelmäßig wechseln. Dazu ergibt es Sinn das gemeinsam zu machen: Oft geht dieser wichtige Schritt im Alltag sonst unter. Zum Beispiel bei jedem ersten Gruppentreffen im Monat.

o Programme aktualisieren

Programme gehören aktualisiert und manchmal erneuert - ob sie verwendet werden oder nicht. Gerade bei Problemen bei Verschlüsselung oder Unklarheiten kann es helfen, das in einem regelmäßigen gemeinsamen Treffen anzugehen, damit verhindert ihr, dass es im Alltag untergeht oder jemand von einem Problem überfordert ist.

o Neue Leute in das Sicherheitskonzept einbinden

Ein Sicherheitskonzept will gelebt werden und nicht nur einmal erklärt sein. Daher brauchen neu zur Gruppe gestoßene Leute manchmal besondere Unterstützung.

o Fragen klären

Bei der Nutzung von Programmen und Technologien tun sich immer wieder Fragen auf. Spätestens beim nächsten Versionsupdate. Schafft euch den Raum und die Zeit, wo diese Fragen gestellt und beantwortet werden können.