IT Sicherheit für die Praxis

Eine Anleitung für Beginner

Betriebssystem:
Nutze nie die vorinstallierten Betriebssysteme wie Windows oder Mac OS, denn sie sind nur aufgrund kapitalistischer Prinzipien in diese Position gekommen und handeln mit deinen Daten immer im Gegenteil zu deinen Interessen.

Laptop und PC: Lass dir helfen, ein **Linux** Betriebssystem einzurichten! Dies ist viel sicherer als die Alternativen und bietet zahlreiche Tools und Anwendungen dafür an.

Regelmäßig **Updates** installieren!

Smartphones:
Sind vulnerabel, da sie laufend Informationen über dich senden und mit dem Telefonnetz in Verbindung stehen. Als Betriebssystem bietet sich z.B. „**Lineage OS**“ an. Das Betriebssystem „**Graphene OS**“ ist speziell für Google-Pixel Phones ist ein freies Betriebssystem, dass auf Privat- und Sicherheit ausgelegt ist.
Nutze **vorregistrierte Simkarten**, bei denen du dich nicht mit dem Ausweis anmelden musst und die dann nicht mit deinem Namen in Verbindung stehen (gibt es z.B. von Lyca an manchen Kiosks).

Wenn du Hilfe brauchst mit den Betriebssystemen wende dich an: … Anarch-IT Support (anarchitsupport.noblogs.org) in der Bambule35 (immer Dienstags 11 – 15 Uhr).

Standort Funktion ausschalten!

Gehe über den **Tor Browser** ins Internet, um keine Spuren zu hinterlassen. Es ist normal, dass der Tor Browser etwas langsamer ist.
Alternativ: Eine **VPN** (z.B. Proton VPN, kostenlos) einrichten. Eine VPN gibt vor, dass dein Gerät in einem anderen Land ist. Für die Nutzung musst du meist einen Account erstellen. Aktiviere die VPN bevor du mit Firefox o.ä. ins Internet gehst.

Nutze die Suchmaschine „**DuckDuckGo**“ statt Google. Sie speichert und verkauft deine Informationen nicht (stimmt das?)

Whatsapp und Telegramm sind beide unsichere Messenger. Telegramm hat im Gegensatz zu Whatsapp Zugriff auf die Inhalte der Chats und kooperiert mit der Polizei.

Grundsätze für die **Signal** Nutzung:
- Alias benutzen
- einstellen, dass die Nummer nicht angezeigt wird
- Synchronisierung mit den SIM Kontakten deaktivieren
- verschwindende Nachrichten einrichten
- Signal nutzen, um Paste Bins etc zu senden

Am besten nutze **Element** oder **Briar** als Messenger!

Metadaten-Reiniger oder „Metadata-Cleaner“

Anwendung für Linux (in der Anwendungsverwaltung herunterladen).
Entfernt die Metadaten von Dateien, die Informationen über dein Gerät enthalten, die zur

Rückverfolgung genutzt werden können. Bevor du Dateien irgendwo hochlädst, entferne zuerst die Metadaten.

Passwort Manager

Empfehlung: KeepassXC
Mit einem Hauptpasswort, das du dir merkst, öffnest du dieses Programm. Hier kannst du alle deine Passwörter sicher ablegen. Dies ist sicherer, als sie irgendwo aufzuschreiben!
Keepass hat auch die Funktion, sichere Passwörter zu generieren.
Keepass gibt es auch für Android. Unter Android heißt es KeepassDX

Grundsätzlich gilt für Passwörter:
Je länger ein Passwort, desto sicherer. Reihe mehrere zusammenhangslose Wörter, die nichts mit dir zu tun haben aneinander und baue dabei Sonderzeichen ein.
Immer verschiedene Passwörter benutzen! Für Accounts, die von mehreren Personen genutzt werden macht es Sinn, das Passwort gelegentlich zu ändern.

Passwörter nicht im Browser speichern! Mindestens unter Einstellungen → Passwörter → Einstellungen ein Hauptpasswort einrichten, das du dir merkst oder im Passwortmanager speicherst.

Verschlüsselte USB Sticks

→ wie das geht siehe Anleitung
Hier kannst du ein Backup von deinem Keepass oder anderen Daten aufbewahren, sowie Informationen an andere Person übertragen, ohne dass sie ins Internet gelangen.

Verschlüsselte Ordner („Container“)
→ siehe Anleitung
Hier kannst du deine Daten sicher ablegen, so wie es normal sein sollte!

Tails Stick nutzen
→ siehe Anleitung
Tails OS ist ein externes Betriebssystem für Aktivisti, das sich auf einem verschlüsselten USB Stick befindet. Einfach den Stick einhängen und Tails OS nutzen. Alles, was du damit recherchierst etc. hat nichts mit deinem Gerät zu tun und kann nicht nachvollzogen werden. Wenn du den Stick aushängst ist Reset.

Thunderbird nutzen
Thunderbird ist ein E-Mail Client, der mit einem Hauptpasswort geschützt ist und in dem du alle deine E-Mails gesammelt verwalten kannst. Die Nutzung ist handlicher und hinterlässt weniger Spuren als über den Browser. Thunderbird kann außerdem **PGP Schlüssel erstellen und verwalten**. PGP Schlüssel sind Passwörter für verschlüsselte E-Mails. Wenn du kannst, solltest du sie immer aktivieren.
→ siehe Anleitung oder komm zum Anarch-IT Support (anarchitsupport.noblogs.org)

Erstelle dir eine E-Mail Adresse/Account bei systemli.org, riseup.net oder disroot.org, da diese eine Vielzahl an zusätzlichen Diensten anbieten, wie **Paste Bins** oder **Cloud**.

Wegwerf-Emailadressen

Wenn du von einem Anbieter, dem du nicht vertraust, gezwungen wirst, eine Mailadresse anzugeben, kannst du AnonBox vom CCC benutzen. Generiere eine wegwerf E-mail, die eine Stunde lang aktiv ist. Hier die Webseite → https://www.anonbox.net/

Paste Bin
Eine Funktion, die z.B. von systemli.org angeboten wird. Wenn du einen Account hast, kannst du sie nutzen. Paste Bins sind temporäre Container, in denen du einmalig sensible Informationen senden kannst, wie z.B. Passwörter oder Treffpunkte. Du kannst einstellen, wann sie ablaufen.

Sicherheit für Aktivisti allgemein:

- lass deine Geräte bei Plena und Aktionen zu Hause!
- nutze konsequent ein Pseudonym im aktivistischen Kontext
- nutze Codewörter für sensible Themen oder politische Schlagwörter (z.B. Zumba Kurs für Aktionsplenum, alternative Verben, …). Werdet kreativ ;)
- gib den Cops keine Antwort und keine Informationen, wenn sie dich fragen. Du hast das Recht zu schweigen
- bereite dich mit deiner WG auf Hausdurchsuchungen vor