Die 10 goldenen Sicherheitsregeln

Die 10 goldenen Sicherheitsregeln

Aktivist*innen haben oft Angst vor Staatstrojanern. In der Praxis bekommt die Polizei aber die meisten Informationen über beschlagnahmte Geräte. Mit den folgenden Regeln machst du es der Polizei sehr schwer, an deine Daten zu kommen. Gleichzeitig bleibst du arbeitsfähig, wenn sie dir deine Geräte abnehmen.

> Vielleicht überfordert dich dieser Artikel mit seinen vielen Ratschlägen. Fang einfach da an, wo es für dich passt und sehe es als langfristiges Projekt. Jede umgesetzte Maßnahme verbessert deine Situation, auch wenn du noch nicht alle Regeln umgesetzt hast. {.is-info}

1) Verschlüssele alle deine Datenträger

- Aktiviere die Festplattenverschlüsselung auf deinem Laptop/PC. Prüfe, ob wirklich alle Partitionen verschlüsselt sind. Eine Einschätzung zur Windows-Festpattenverschlüsselung findest du hier.
- Wenn du die Verschlüsselung von Windows (BitLocker) nutzt, aktiviere unbedingt Pre-Boot Authentication.
- Entsperre deinen Laptop (Benutzer*innen-Account) nicht mit deinem Fingerabdruck, sondern nutze dafür ein Passwort.

- Verschlüssele alle externen Festplatten und USB-Sticks (mit Veracrypt oder unter Linux mit LUKS).

Wenn dein Laptop verschlüsselt ist, kann die Polizei nicht an deine Daten kommen. Das Gleiche gilt für externen Festplatten, die mit einem guten Passwort verschlüsselt sind. Bei Smartphones sieht das leider etwas anders aus. Smartphones sind heutzutage zwar standardmäßig verschlüsselt, die Polizei bekommt die meisten aber trotzdem auf (insbesondere Android-Geräte und generell ältere Geräte).

2) Steig auf GrapheneOS um

Was ist GrapheneOS? GrapheneOS ist ...

- ein Android-Betriebssystem, das auf Sicherheit ausgelegt ist.
- das Betriebssystem, das die Polizei nicht aufbekommt.
- in der Bedienung genauso wie ein normales Android. Du merkst keinen Unterschied. Du kannst selbst entscheiden, ob du es mit oder ohne Google-Dienste/Account nutzen möchtest.
- von Haus aus sehr sicher, du musst nichts besonderes einstellen. Du solltest das Gerät allerdings nicht nur mit deinem Fingerabdruck entsperren.

Wie kann ich GrapheneOS nutzen?

- GrapheneOS kann man nur auf Google Pixel Smartphones nutzen.
- Hole dir ein gebrauchtes Google Pixel über Kleinanzeigen (Übersicht Geräte und Preise, nutze den Käuferschutz!).
- Alternativ kannst du beim ProxyStore in Leipzig (oder im Online-Shop) Google Pixels mit vorinstalliertem GrapheneOS kaufen (etwas teurer).
- Du musst GrapheneOS selbst installieren (Installationsanleitung GrapheneOS). Alternativ gibt es vom ProxyStore auch einen Installationsservice, falls du schon ein Google Pixel ohne GrapheneOS hast.

Was mache ich, wenn ich kein GrapheneOS habe?

- Gehe davon aus, dass die Polizei dein Telefon auslesen kann und achte auf Datensparsamkeit
- Beachte die Hinweise zu Punkt 3 (Aktionstelefone) und Punkt 10 (datensparsam leben)
- Aktiviere den Lockdown Mode (Blockiermodus) in iOS.
- Aktiviere den erweiterten Sicherheitsmodus (Android Advanced Protection Mode) und die Einbruchsprotokollierung in Android.

3) Nutze für Aktionen ein separates Telefon

Überlege dir gut, ob du überhaupt ein Telefon mit in die Aktion nehmen musst. Wenn ja, dann gehe auf keinen Fall mit deinem privaten Telefon in Aktion. Nutze stattdessen dafür ein separates Telefon. Setze das Telefon vorher zurück (Werkseinstellungen/factory reset), um alle Daten zu löschen. Für Aktionstelefone sind Google Pixel-Geräte mit GrapheneOS meist zu teuer. In der Regel sind das ältere Android-Geräte. Gehe daher davon aus, dass die Polizei das Telefon auslesen kann, wenn sie es in die Hände bekommt. Um zu verhindern, dass die Polizei an deine Daten gelangt, kannst du Apps mit zusätzlicher Verschlüsselung nutzen oder dafür sorgen, dass sich das Telefon im Falle einer Beschlagnahmung automatisch löscht.

Einen ausführlichen Artikel mit App-Empfehlungen für Aktionselefone (Android) findest du hier im Wiki. Hier ist eine Zusammenfassung der Empfehlungen:

- Wenn du Signal nutzt: Verwende Molly anstelle der offiziellen Signal-App. Molly bietet eine zusätzliche Verschlüsselung an, mit der deine Signal-Nachrichten verschlüsselt werden.
- Es muss auch nicht immer Signal sein. Gerade für einzelne Aktionen kann sich Delta Chat lohnen. Der Messenger bietet ebenfalls eine Ende-zu-Ende-Verschlüsselung, erfordert aber keine Telefonnummer für die Registrierung.
- Aktiviere "Verschwindende Nachrichten" (Disappearing Messages) und setze die Ablaufzeit auf einen geringen Wert.
- Mit FMD (Find My Device) (F-Droid, Projekt) kannst du dein Telefon aus der Ferne orten oder löschen, ohne einen Account zu benötigen.
- Mit Oblivion kann das Telefon auch aus der Ferne gelöscht werden. Es bietet zusätzlich die Möglichkeit, mit zwei Klicks das Telefon zu löschen.
- Oblivian v2 bietet mehrere Möglichkeiten, um das Telefon automatisch zu löschen: zu einer bestimmten Uhrzeit, nach Eingabe einer bestimmten PIN (Duress PIN) oder wenn das Telefon über einen bestimmten Zeitraum nicht entsperrt wurde.
- Nicht ganz einfach einzurichten aber trotzdem cool: Cryptocam. Mit dieser App kannst du Fotos und Videos aufnehmen, die verschlüsselt auf dem Telefon gespeichert werden. Weder du noch die Polizei können die Dateien anschauen. Das Backoffice kann die Dateien aber entschlüsseln und verwenden. Wie das funktioniert wird hier beschrieben.

Wichtig: Wenn du im Alltag ein älteres Android-Gerät nutzt, ist es wichtig, dass du die empfohlenen Apps auch im Alltag verwendest.

4) Aktiviere "Verschwindende Nachrichten"

Egal wie sicher deine Geräte oder deine Passwörter sind: Informationen, die gar nicht erst vorhanden sind, können auch nicht von der Polizei ausgelesen werden. Aktiviere deshalb die Funktion "Verschwindende Nachrichten" (Disappearing Messages) in all deinen Messengern (Signal, Telegram, Delta Chat, ...).
Bei vielen Messengern kannst du "Verschwindende Nachrichten" als Standard einstellen. Dann verschwinden Nachrichten in neuen Chats automatisch (Signal, WhatsApp, usw.). Bei Element, das das Matrix-Protokoll nutzt, hängt es vom Server bzw. der installierten Anwendung ab, ob du "Verschwindende Nachrichten" nutzen kannst.

In der Vergangenheit kam es aufgrund von Zufallsfunden in ausgelesenen Telefonen bereits zu neuen Ermittlungsverfahren. Für die Polizei sind Chats äußerst wertvoll.

5) Kommuniziere ausschließlich mit Ende-zu-Ende-Verschlüsselung

Bei größeren Verfahren wie den kriminelle Vereinigungs-Verfahren (§ 129 StGB) kann die Polizei eine Telekommunikationsüberwachung (TKÜ) gegen dich einsetzen. Im Jahr 2024 wurde die TKÜ 13.779 Mal in 5.538 Strafverfahren richterlich angeordnet. Eine Anordnung beschränkt sich immer auf einen bestimmten Zeitraum (maximal drei Monate), der jedoch verlängert werden kann.

Im Rahmen einer TKÜ geben Telekommunikationsanbieter eine Kopie deiner Daten an die Polizei weiter:

- Dein Mobilfunkanbieter gibt der Polizei deine Telefongespräche in Form von MP3-Dateien weiter. Zusätzlich erhält sie deine empfangenen und gesendeten SMS sowie eine Kopie deines gesamten Internetverkehrs.
- Dein E-Mail-Anbieter leitet neue ein- und ausgehende E-Mails direkt an die Polizei weiter.

Dagegen kannst du dich relativ einfach schützen, indem du überall Ende-zu-Ende-Verschlüsslung einsetzt:

- Nutze für die Kommunikation (Anrufe, Chats, Sprachnachrichten) ausschließlich verschlüsselte Messenger (Signal, Delta Chat, Matrix ...). Verzichte auf das unverschlüsselte Mobilfunknetz zum Telefonieren - auch für die Familie.

- Nutze E-Mail-Verschlüsselung (PGP) oder verzichte bei politischer Arbeit auf E-Mails. Wenn du doch mal eine Mail schreiben musst kannst du mit https://secret.raz-ev.org/ Einmallinks generieren, um sensible Informationen nur einmal aufrufbar zu machen. Alternativ kannst du E-Mail-Provider nutzen, die deine Daten nicht an die Polizei weitergeben (Riseup, Systemli).
- Mit einem VPN kannst du deinen gesamten Internetverkehr verschlüsseln. Ohne VPN kann die Polizei sehen, wann du welche Webseiten besuchst (nur den Domainnamen, also z. B. wiki.raz-ev.org, aber nicht die genaue Unterseite, die du besuchst, oder ob du eingeloggt bist). Mit VPN sieht sie nichts außer "da nutzt wer einen VPN" und deinen VPN-Anbieter.

6) Sicherer Umgang mit Passwörter

- Verwende einen Passwort-Manager (z. B. Bitwarden oder Keepass)
  - Bitwarden ist Open Source-Software, du brauchst noch wen, der eine Instanz betreibt:
    - offizielle Instanz: https://vault.bitwarden.eu/ (die kostenlose Variante hat ein paar kleinere Einschränkungen)
    - Letzte Generation: https://vaultwarden.itsnow.biz/ (wird langfristig betrieben)
    - Systemli: https://passwords.systemli.org/ (braucht eine Systemli E-Mail-Adresse)
    - Es gibt für alle Plattformen Apps (Google PlayStore, F-Droid, App Store, Browser-Erweiterung, Desktop-Anwendung).
  - Achte darauf, dass du auch ohne deine Geräte auf deinen Passwort-Manager zugreifen kannst. Bei Bitwarden kannst du dich einfach im Browser einloggen.
- Verschicke niemals Passwörter unverschlüsselt und ohne ablaufende Nachrichten
  - Wenn du sicher gehen willst erstelle Einmallinks mit https://secret.raz-ev.org/
  - Alternativ: Setze den Timer für verschwindende Nachrichten herunter
  - Verschicke niemals Passwörter in E-Mails
- Verwende sichere Passwörter
  - Lass dir für Accounts im Internet ein Passwort von deinem Passwort-Manager generieren. Du musst es dir nicht merken
  - Für Passwörter, die du dir merken musst: Verwende eine Passphrase (aneinander gereihte zufällige Wörter, z. B. "urwald bellen byte kante nervig")

7) Erstelle regelmäßig verschlüsselte Backups

Langfristig gesehen werden all deine Geräte irgendwann kaputtgehen. Bei einer Hausdurchsuchung können dir sogar alle Geräte auf einmal weggenommen werden. Überlege dir deshalb, welche wichtigen Daten du auf deinem Telefon oder Laptop gespeichert hast, von denen du ein Backup brauchst.

Ein Backup ist letztlich nichts anderes als eine Kopie deiner Dateien. Im einfachsten Fall kopierst du einfach deine Dateien auf einen USB-Stick.

Vergewissere dich, dass all deine Datenträger verschlüsselt sind! Ein verschlüsselter Laptop nützt nichts, wenn die Backups unverschlüsselt neben dem Laptop auf der externen Festplatte liegen.

Hier ist ein Vorschlag zum Backup machen:

- Kopiere regelmäßig wichtige Dateien von deinem Telefon auf deinen Laptop. Das kannst du manuell mit dem USB-Kabel oder mit der App Syncthing erledigen.
- Besorge dir einen großen USB-Stick oder eine externe Festplatte.
- Verschlüssele deinen externen Datenträger (mit Veracrypt oder unter Linux mit LUKS).
- Erstelle regelmäßig ein Backup deines Laptops auf dem externen Datenträger (Backups erstellen unter Linux/MacOS mit Vorta erstellen).
- Im besten Fall lagerst du die Backups bei einer Person in deiner Nähe. So kannst du auch nach einer Hausdurchsuchung noch auf deine Daten zugreifen.

Hier noch ein paar Tipps:

- Wenn du Signal nutzt: Aktiviere das verschlüsselte Cloud-Backup (kostenlos und einfach zu aktivieren).
- Wenn du Delta Chat nutzt: Exportiere dein Profil in eine Datei und kopiere sie auf den Laptop.
- Wenn du deine Überweisungen mit dem Telefon bestätigst: Du kannst zusätzlich zur Banking-App auch noch einen TAN-Generator nutzen.
- Wenn du dein Telefon zur 2-Faktor-Authentifizierung nutzt: Was passiert, wenn dein Telefon weg ist?
- Wenn du PGP (E-Mail-Verschlüsselung) in Thunderbird nutzt: Exportiere den geheimen und öffentlichen Schlüssel in eine Datei.

8) Halte deine Software und Hardware aktuell

Es klingt langweilig, aber es ist wichtig: Installiere Software-Updates, sobald sie verfügbar sind. Denn Software-Updates beheben Sicherheitslücken, die dann nicht mehr von der Polizei ausgenutzt werden könnten. Daher ist es wichtig, dass deine Geräte noch Updates erhalten.

Suche in den Einstellungen deines Telefons nach "Updates". Wenn dein Gerät keine Updates mehr erhält, solltest du zu einem wechseln, das noch Updates bekommt.

Du kannst das alte Telefon aber weiterhin für Aktionen nutzen, sofern du datensparsam mit deinen Daten umgehst (siehe den Punkt zu den Aktionshandys). Die Google Pixel Smartphones bekommen sieben Jahre lang Updates.

Die Situation bei Windows 10/11 Als Mindestvorraussetzung für Windows 11 wird ein Sicherheitschip (TPM 2.0) vorausgesetzt. Dadurch sind sehr viele Geräte, auf denen Windows 10 läuft, nicht mehr mit Windows 11 kompatibel.

Ursprünglich sollte Windows 10 Updates bis Oktober 2025 erhalten. Nach großer Kritik gibt es nun doch längere Sicherheitsupdates für Windows 10, allerdings nur wenn man seinen Laptop mit einem Microsoft-Konto verbindet. Das ist kostenlos, aus Datenschutzgründen jedoch unschön. Ursprünglich waren die erweiterten Sicherheitsupdates bis Oktober 2026 angekündigt, dann wurden sie bis Oktober 2027 verlängert.

Zusammenfassung:

- Finde heraus, welche Windows Version du nutzt.
- Du nutzt Windows 11? Dann bekommst du in den nächsten Jahren Updates.
- Du nutzt Windows 10 und dein Laptop besitzt einen Sicherheitschip (falls nicht siehst du das bei den Windows-Updates)? Dann kannst du auf Windows 11 upgraden und erhältst die nächsten Jahre Updates.
- Du nutzt Windows 10 und dein Laptop hat keinen Sicherheitschip?
  - Dann steige auf Linux um, zum Beispiel auf Linux Mint.
  - Oder verbinde deinen Laptop mit einem Microsoft-Account, dann bekommst bis Oktober 2027 noch Sicherheitsupdates.

9) Verabschiede dich von Big-Tech

In Ermittlungsverfahren werden regelmäßig Telefone beschlagnahmt. Dass die Polizei jedoch direkt bei Google oder Microsoft auf deine Daten zugreift, kommt dagegen relativ selten vor. In den

129er-Verfahren der Letzten Generation wurden jedoch Google-Konten gesperrt und Google Docs an die Polizei herausgegeben.

Unabhängig davon gibt es zahlreiche Argumente, Trump und den US-Konzernen den Rücken zu kehren. Zuletzt gab es immer wieder Sanktionen gegen die Zivilgesellschaft:

- Nicolas Guillou wurde von den USA als Richter des Internationalen Strafgerichtshofs mit Sanktionen belegt. Alle seine Online-Konten und Kreditkarten wurden gesperrt.
- Nach der Einstufung "der Antifa" in den USA als Terrororganisation wurden Bankkonten von linken Organisationen wie der Roten Hilfe in Deutschland gesperrt. Außerdem wurden mehrere Instagram-Accounts gesperrt, darunter der "Antifa-Ost-Komplex".
- Menschen von HateAid wurden unter dem Vorwand von Anti-Zensur-Maßnahmen sanktioniert und dürfen nicht mehr in die USA einreisen.

Was sind die Alternativen?

- Du nutzt Windows? Dann wechsel zu Linux (Mint). Windows macht deinen Laptop mit der Zeit langsamer, da immer mehr unnötige und datenschutz problematische Prozesse im Hintergrund laufen. Linux ist dagegen datenschutzfreundlich und läuft auch auf älteren Geräten sehr flüssig. Wenn du Hilfe bei der Installation brauchst kannst du dich beim RAZ, dem Hextivisti-Kollektiv oder beim CCC melden. In vielen Städten finden auch monatlich Digital Independence Days statt.
- Du nutzt eine Gmail-E-Mail-Adresse? Hol dir doch eine Systemli-Email-Adresse (benötigt einen Einladungscode).
- Ihr nutzt als Kollektiv Instragram/Facebook/Twitter? Dann wechselt auf Mastodon, zum Beispiel auf https://systemli.social oder https://chaos.social. Vielleicht habt ihr dadurch nicht die größte Reichweite, aber alle können eure Nachrichten lesen, ohne einen Account zu haben.
- Ihr nutzt Zoom für eure Online-Meetings? Dann wechselt doch zu Senfcall (BigBlueButton), Systemli Meet (Jitsi). Wenn alle Signal haben könnt ihr auch einen Anruflink erstellen. Dann könnt ihr über Singal telefonieren, ohne in einer Gruppe sein zu müssen.
- Ihr nutzt eine Telegram-Gruppe für Broadcast-Nachrichten? Dann nutzt doch zusätzlich den Systemli-Ticker. Dann können Menschen auch ohne Telegram eure Nachrichten lesen.
- ~~Ihr braucht anonym und unkompliziert eine Webseite? Dann erstellt euch doch eine auf noblogs.org.~~ (Dienst wegen US-Sanktionen/Repressionen eingestellt)

Alle Dienste von Systemli findest du hier aufgelistet. Der Passwort-Manager Bitwarden (https://passwords.systemli.org) fehlt dabei noch. Die Dienste von Riseup findest du hier.

Synchronisation von Dateien, Kalender und Kontakten Für die Synchronisation von Dateien, Kalendern und Kontakten kannst du die Nextcloud verwenden. Nextcloud ist ein Open Source

Projekt, du brauchst jemanden, der eine Nextcloud betreibt:

- Die Nextcloud von Systemli ist am aktivismus-freundlichsten, allerdings habt ihr dort nur 1 GB Speicherplatz. Als politische Gruppe könnt ihr dort nach mehr Speicherplatz fragen.
- Gegen Geld erhältst du mehr Speicherplatz, zum Beispiel beim Datenkollektiv, der Freiheitswolke oder Proton.
- Wenn du keine Datei-Synchronisation benötigst, kannst du auch Posteo nutzen. Dort bekommst du datenschutzkonforme E-Mail-Adressen und kannst wie bei Nextcloud deine Kalender und Kontakte synchronisieren.
- Cryptomator verschlüsselt deine Daten, bevor sie in die Cloud geladen werden. Du kannst Cryptomator nicht nur für die Nextcloud, sondern für jeden anderen Cloud-Provider wie Google Drive verwenden. Cryptomator ist für Laptops konstenlos, für Mobilgeräte kostet es jedoch einmalig 30 Euro. Die Lizenz kann datenschutzfreundlich im ProxyStore (auch online) erworben werden.

Wie kann ich von Google auf Nextcloud umsteigen?

1. Erstelle dir einen Nextcloud Account
2. Exportiere deine Daten bei Google. Das geht am einfachsten am Laptop im Browser:
   - Logge dich in dein Google Konto ein
   - Unter https://takeout.google.com/ kannst du alle deine Google-Daten auf einmal exportieren
   - Du kannst aber auch in die einzelnen Apps (Kontakte oder Kalender) gehen und dort einezelne Kontaktbücher oder Kalender in eine Datei exportieren
   - Diese Datei kannst du dann in der Nextcloud importieren
3. Du kannst die Nextcloud im Browser nutzen. Ansonsten gibt es für alle Betriebssysteme auch Apps.

10) Lebe datensparsam - Langfristige Datenhygiene

Es gibt ein paar Dinge, die du langfristig immer wieder mal tun solltest. Dazu gehören beispielsweise das Erstellen von Backups , das Löschen des Browserverlaufs, das Verlassen alter Gruppenchats und das Löschen alter E-Mails. Diese Checkliste hilft dir dabei, diese Aufgaben abzuarbeiten. Am besten hinterlegst du eine Erinnerung in deinem Kalender (einmal im Quartal) und verlinkst die Checkliste.

> Die hier beschriebenen Regeln legen den Fokus auf Sicherheit statt auf Anonymität. Themen wie die Personalienverweigerung in Aktion, das Leben im Untergrund oder die Erstellung von Bewegungsprofilen durch Funkzellenabfragen werden nicht behandelt. Anonymität ist nochmal ein extra Thema. {.is-warning}

> Glückwunch! Du hast es bis zum Ende geschafft! Brauchst du Unterstützung oder hast Fragen? Dann melde dich beim RAZ (it-support@raz-ev.org). Alternativ bietet das Hextivisti-Kollektiv Wochenend-Skillshares für Aktivist*innen und Antifschist*innen zu genau diesen Themen an! Mehr Infos findest du auf https://kein-hexenwerk.org. {.is-success}

Version #1
Erstellt: 2026-11-19 14:17:25 UTC von RAZ Migration Bot
Zuletzt aktualisiert: 2026-11-19 14:17:25 UTC von RAZ Migration Bot