Allgemeines

- Hausdurchsuchung
- Checkliste Sicherer Umgang mit Technik
- Staatstrojaner in Deutschland

Hausdurchsuchung

Hier geht es um den Technikaspekt von Hausdurchsuchungen. Für den juristischen Teil gibt es eine eigene Seite im Legal-Teil des Wikis.

Laptop und andere Technik hausdurchsuchbar machen hat 2 Säulen:

1. Daten vor fremden Augen sichern
2. arbeitsfähig bleiben

Daten vor fremden Augen sichern

Allgemein

Alle angebotenen Betriebssystemupdates schnellstmöglich installieren.

Gerätespeicher verschlüsseln

- Android verschlüsseln
- iOS: ist von Haus aus verschlüsselt
- Windows verschlüsseln mit Bitlocker
- macOS verschlüsseln

Messenger

Verhindern, dass Team Blau sich Signal und Telegram mit eurer Nummer installieren kann:

- bei Signal eine PIN einrichten

- bei Telegram ein Passwort einrichten, denn Telegram synchronisiert alle Inhalte auf das Handy der Polizei, indass sie die Ersatzsimkarte vom Provider einlegen.

  Sollte dein Handy ohne Telegram-Passwort beschlagnahmt werden, keine Panik. Dann kannst du dein Telegram-Konto mittels https://my.telegram.org/auth?to=delete löschen.

PIN und Passwort solltest du in deinem Passwortmanager abspeichern.

nach Hausdurchsuchung arbeitsfähig bleiben

Die folgenden Schritte solltet ihr jetzt durchdenken, damit ihr nach einer Hausdurchsuchung arbeitsfähig bleibt.

- SIM-Karte nachbestellen: prüft vorher, ob ihr eine Hotline oder eine Onlinemöglichkeit findet, um bei eurem Mobilfunkanbieter eine SIM-Karte nachzubestellen.
  Die Lieferzeiten sind sehr unterschiedlich: Beim klimafreundlichen Anbieter WEtell geht das z.B. innerhalb eines Werktages; bei ALDI TALK dauert es 8 Werktage.

  Wenn ihr die Handynummer behaltet, dann sperrt ihr die Polizei aus Signal aus.
- Zugriff auf Passwörter behalten: Passwortmanager-Bitwarden
- verschlüsseltes Backup bei fernen Verwandten oder Nicht-LG-Freunden aufbewahren. Eine sichere Verschlüsselung für Backups von:
  - Laptops: z.B. `restic`.
  - iOS: auf einem Mac oder einem Windows-Computer mit iTunes herstellen. Wichtig: Backup mit Passwort sichern, damit es vollständig ist.
  - Android: bitte ergänzen, wie das genau geht.
- Habt ihr irgendwo eine 2-Faktor-Authentifizierung (2FA) aktiviert? Dann überlegt, ob ihr da noch rankommt, wenn die Technik von zu Hause verschwunden ist.

Skillshare-Video

_skillshare_passwortmanager_und_ger%C3%A4te_verschl%C3%BCsseln-youtube.png

Tipps für's Smartphone

1. Ihr könnt im Telefon Notfall-Kontakte hinterlegen. Die könnt ihr anrufen, ohne das Handy entsperren zu müssen. Da könnt ihr z. B. die Nummer vom EA hinterlegen oder von Menschen, die bei euch im Haus wohnen. Anleitung:

   https://www.chip.de/news/Notfallinfos-auf-dem-Sperrbildschirm-Das-kann-im-Ernstfall-Ihr-Leben-retten_184234487.html Es ist jedoch unrealistisch, dass die Polizei bei einer Hausdurchsuchung erlaubt, dass ihr euer eigenes Telefon berührt.
2. Wir haben die Erfahrung gemacht, dass die Polizei beschlagnahmte Smartphones in den Flugmodus setzt. Sie haben manchmal auch spezielle Beutel mit Powerbank, um das Telefon angeschaltet, aber funklos zu halten. Damit kann sie verhindern, dass das Gerät nicht aus der Ferne gelöscht wird.
   - auf Android:
     In den Quick Settings könnt ihr den Flugmodus aktivieren bzw mobile Daten ausschalten. Prüfe, ob das auch aus dem Sperrbildschirm heraus geht, ohne die PIN eingeben zu müssen. Wenn die PIN nicht eingegeben werden muss, kanns du Flugmodus/'mobile Daten ausschalten' aus dem Quick Menü entfernen.

     Um die Fernöschlung zu testen hier einloggen

     Hier könnt ihr euch mal anschauen, wie das dann ausschaut.
   - auf iOS:
     In der Einstellungen-App auf „Face/Touch ID & Code“ gehen und das „Kontrollzentrum“ abschalten. Dann lässt sich das Telefon nicht mehr in den Flugmodus stellen.

     Die Fernlöschung lässt sich nach der Beschlagnahme über iCloud.com » „Wo ist?“ aktivieren. Da Apple zum Einloggen bei iCloud.com einen 2. Faktor verlangt ist es praktisch, einen Notfall-Kontakt zu hinterlegen, der dann die SMS bekommt, wenn euer Handy bei der Polizei ist.
3. Es ist auch schon vorgekommen, dass mit Hilfe abgenommener Fingerabdrücke ein Smartphone entsperrt wurde.
4. Einige Menschen empfehlen, kein Face-ID zum Entsperren des Telefons zu nutzen. Face-ID ist automatisch ausgeschaltet, wenn ihr das Telefon ausschaltet. Außerdem ist es aus, wenn ihr die Seitentaste und eine der Lautstärketasten zwei Sekunden lang gedrückt haltet. Ausschalten ist eine gute Routine vor dem Einschlafen. Sonst hält euch die Polizei das Gerät vor's Gesicht und es ist entsperrt. Das klappt allerdings nicht, wenn ihr die Augen geschlossen haltet (Aufmerksamkeitsprüfung für Face ID).

E-Mails

Wenn deutsche Mailanbieter wie GMX, Web.de oder Posteo einen korrekten Gerichtsbeschluss zur Herausgabe von Daten bekommen, dann werden sie deine Mails herausgeben. Typischerweise ist

das keine Liveüberwachung, sondern eine Herausgabe zu einem fixen Zeitpunkt oder die Beschlagnahme des Kontos.

Das kannst du mit folgenden Strategien verhinden - eine davon reicht:

- Anbieter außerhalb der EU, der nicht mit Deutschland zusammenarbeitet.
- Mails mit PGP-Verschlüsselung empfangen und senden (für einzelne Mails einfach, flächendeckend unmöglich)
- zu einem Provider gehen, der Mails aus technischer Sicht nicht herausgeben kann:
  - ProtonMail: proton.me/legal/transparency
  - Mailadressen, die auf sicherer Infrastruktur abgelegt sind, z.B. @letztegeneration.org (nur für AGs, WiGs und interne Gruppen; nicht für Personen)

Google-Account

Bedenke auch: wo liegt dein Google-Konto? Bekommst du da Mails wie „Ihnen wurde das Google Doc Xyz freigegeben“? Falls ja, kann die Polizei das Dokument von Google bekommen, falls sie deine Mails lesen können. Es ist auch bereits vorgekommen, dass die StA Google per Gerichtsbeschluss gezwungen hat, ein von LG genutztes Konto zu sichern und zu schließen. Das bedeutet, dass auf einen Schlag alle Google-Dokumente unzugänglich werden, die diesem Konto gehören. Google-Konten lassen sich auch für Mailadressen anlegen, die bei einem Mailprovider liegen, der keine Mails an die Polizei rausgibt - siehe oben.

Die IT-AG empfiehlt, statt Google Docs unsere Nextcloud zu nutzen. Die findet ihr unter cloud.raz-ev.org/apps/files/

Hilfe dazu gibt es hier im Wiki.

ios-kontrollzentrum-deaktivieren.png

Checkliste Sicherer Umgang mit Technik

Hausdurchsuchungen & sicherer Umgang mit Technik

Neben den Checklisten findest du unten auch eine Liste mit hilfreichen Links.

Vorbereitung auf eine Hausdurchsuchung

Spiele es mal durch: Angenommen die Polizei schaut morgen vorbei und nimmt dir deine Geräte weg. Wie gut bist du vorbereitet?

- ☐ Alle meine Geräte sind verschlüsselt (Laptop, Handy, Tablet, externe Festplatten, USB-Sticks
- ☐ Ich habe Sachen aus der Wohnung geschafft, die die Polizei nicht mitnehmen/sehen soll (muss auch nicht Aktivismus related sein, z. B. externe Festplatten mit Familienfotos oder alte Tagebücher. Oder unverschlüsselte Festplatten, weil du noch nicht dazu gekommen bist, sie zu verschlüsseln)
- ☐ Ich mache regelmäßig Backups
  - ☐ Meine Backups sind verschlüsselt
  - ☐ Ich habe auch Backups, die nicht zu Hause gelagert sind

- ☐ Meine Backups enthalten alles wichtige (Passwörter, Signal-Account, Browser-Historie/Lesezeichen, Kontakte, Dokumente)
- ☐ Ich kann auch nach der Hausdurchsuchung auf meine Passwörter zugreifen (denke auch an Zwei-Faktor-Authentifizierung)
- ☐ Ich kann auch nach der Hausdurchsuchung auf meine E-Mails zugreifen (um im Notfall Passwörter zurücksetzen zu können)
- ☐ Ich kann auch nach der Hausdurchsuchung auf Kalendar, Kontakte und Dokumente/Cloud zugreifen
- ☐ Ich kann jederzeit mit dem EA oder der AG Kontakt aufnehmen (Zettel an der Wand)
- ☐ Ich habe im Vorfeld mit meinen Mitbewohner*innen gesprochen und teile diese Informationen mit ihnen

Wir haben die Erfahrung gemacht, dass die Polizei alles an elektronischen Geräten mitnimmt, was sie findet. Wenn sich der Beschluss gegen euch richtet habt ihr darauf keinen Einfluss. Aber wenn sich die Durchsuchung nicht gegen euch richtet (ihr seid Beziehungsmensch/Mitbewohner*in, bzw betrifft das eure Mitbewohner*innen), dann beschwert euch lautstark/wehement, dass diese Sachen nicht mitgenommen werden.
Bei den bisherigen Durchsuchungen war es dann oft so, dass sich die Polizei die Geräte vor Ort angeschaut und geprüft hat, ob da relevante Infos vorhanden sind und entscheidet dann vor Ort. Mit unterschiedlichem Ausgang:

- Menschen durften ihre Technik behalten
- die Festplatte wurde vor Ort gespiegelt (kopiert), dafür wurde sie nicht mitgenommen
- Festplatte/Laptop wurde trotzdem mitgenommen

Wichtig dabei: Die Menschen mussten dabei ihre Geräte (Handy/Laptop) entschlüseln/entsperren. Das ist natürlich gefährlich. Deshalb müsst ihr euch **vorher** fragen, wie wichtig euch das jeweilige Gerät ist und wie sensibel die Daten darauf sind.

Macht euch auch bewusst, dass eine Hausdurchsuchung eine absolute Stress-Situaion ist. Menschen wurden von der Polizei unter Druck gesetzt und haben Passwörter herausgegben/eingegeben. Ihr müsst der Polizei nicht eure Passwörter geben. Ihr habt das Recht, keine Aussage zu machen und euch nicht selbst zu belasten. Dazu gehört auch das Verweigern der Herausgabe der Passwörter. Die Rechtslage ist aber (leider) so, dass sie euch (mit Gewalt) zwingen können, mit biometrischen Mitteln (Fingerabdruck, Gesichtserkenung) Geräte zu entsperren.

Die 4 goldenen Sicherheitsregeln

☐ Alle meine Geräte sind verschlüsselt

☐ Ich nutze Verschlüsselung für meine Kommunikation (Signal für Telefonie/Nachrichten, PGP für E-Mail-Verschlüsselung). Ich aktiviere verschwindende Nachrichten auf Signal.

☐ Wenn ich in Aktion gehe, nutze ich nicht mein privates Telefon, sondern ein Aktions-Telefon

☐ Ich gehe davon aus, dass die Polizei das Aktions-Telefon entsperren und auslesen kann. Ich setze das Gerät vor der Aktion zurück und achte darauf, was für Daten darauf gespeichert sind.

Genereller Umgang mit Technik

☐ Ich nutze nur noch verschlüsselte Geräte (Laptop, Handy, Tablet, externe Festplatten)

☐ Mir ist bewusst, dass die Polizei eventuell Zugriff auf meine unverschlüsselten Telefonate bekomment (TKÜ/Telekommunikationsüberwachung)

☐ Mir ist bewusst, dass die Polizei eventuell Zugriff auf meine E-Mails/SMS bekommt (TKÜ)

☐ Ich bevorzuge eine private Nextcloud (z. B. Systemli) gegenüber der Google-Cloud

☐ je älter mein Handy ist (bezogen auf: bekommt es noch Updates?), desto unsicherer ist es. Ich bevorzuge dann lieber meinen Laptop für die Aktivismus-Arbeit

☐ mein Handy ist mit einer sicheren PIN/Passwort gesichert

Umgang mit Signal

☐ Ich habe eine Signal-PIN hinterlegt (Registration Lock/Registrierungssperre), damit bei der Neu-Einrichtung des Accounts eine PIN eingegeben werden muss - der Empfang einer SMS reicht dann nicht mehr aus (Dokumentation)

☐ Wenn mein Handy beschlagnahmt wird, lasse ich meine SIM-Karte vom Provider sperren, bestelle mir eine neue SIM-Karte und nutze die bisherige Nummer weiter. Damit kann die Polizei nicht einfach ungemerkt meinen Signal-Account nutzen

☐ Ich aktiviere verschwindende Nachrichten (auch als Standardeinstellung für neue Chats)

☐ Ich nutze Signal auch auf dem Laptop, um im Falle eines gestohlenen/defekten/beschlagnahmten Gerätes weiter arbeitsfähig zu bleiben

☐ Ich kann auch noch noch Bildschirmsperre (Screen lock) aktivieren, die eingegeben werden muss, um die Signal-App auf dem Handy zu öffnen (Dokumentation)

☐ Ich nutze die Backup-Funktion von Signal und backupe ein paar mal im Jahr meine Signal-Chats/Kontakte (Dokumentation)

☐ Ich schaue in Signal (und anderen Messengern) nach "linked devices" (verknüpften Geräten). Die Polizei nutzt das Feature, um verschlüsselte Messenger abzuhören (Quelle)

Empfehlungen

- Smartphone Empfehlung: Besorgt euch ein gebrauchtes Google Pixel Smartphone auf Kleinanzeigen und installiert das GrapheneOS Betriebssystem
- Nutze Chat-Ordner, um einen besseren Überblick zu behalten
- Auf Android kann ich Molly installieren, um ganz einfach einen zweiten Signal-Account nutzen zu können (eine zweite Signal-App)
- Ihr könnt eure Telefon-Nummer verstecken. Dann wird sie in (Gruppen-)Chats nicht mehr angezeigt. Allerdings erschwert das die Kontaktaufnahme. Wenn die Polizei es schafft, euer Handy auszulesen, dann kommt sie an euren Signal-Account (eure "Account ID"). Mit der kann sie zu Signal gehen und nach der hinterlegten Telefonnummer fragen. (Dokumentation

Kontakt

Meldet euch gerne bei Fragen oder Anregungen mit einer Mail an it-support@raz-ev.org (gerne auch PGP verschlüsselt).

Links

- Verschlüsselung:
  - Allgemeines zum Thema Verschlüsselung
  - Windows verschlüsseln mit Bitlocker
  - Windows verschlüsseln mit Veracrypt
  - Android verschlüsseln
  - MacOS verschlüsseln

    - PGP-Verschlüsselung einrichten
- Signal:
    - Signal sicher benutzen
    - Signal auf dem Laptop nutzen
    - Mehrere Signal-Accounts auf dem Handy nutzen
- Generelles:
    - Auf eine Hausdurchsuchung vorbereiten
    - Bitwarden Passwort-Manager
    - Nextcloud
- externe Ressourcen
    - Vortrag (mit LG-Bezug): Staatliche Überwachung: Erfahrungen und Beispiele aus der Praxis
    - Checkliste mit konkreten Vorschlägen zur Verbesserung deiner Smartphone-Sicherheit
    - Webseite von esc-it (Kollektiv, das IT-Sicherheitstrainings für Aktivist*innen gibt)
    - IT-Sicherheitstrainings für Aktivisti

Staatstrojaner in Deutschland

Staatstrojaner in Deutschland

2011 hat der CCC (Chaos Computer Club) einen deutschen Staatstrojaner aufgedeckt. Auf dieser Seite findet ihr Vorträge vom CCC mit einer gesellschaftlichen, rechtlichen und technischen Einordnung.

1. Aufdeckung, Analyse und Bewertung: 28c3: Der Staatstrojaner, (Youtube, aus 2011).
2. Ein Jahr später: Was ist seitdem passiert: 29c3 staatstrojaner (Youtube, aus 20212.
3. Stand 2023: Über den Gesetzesvorschlag der Ampel zur Einschränkung von Staatstrojanern: Staatstrojaner für bereits begangene Straftaten (Youtube, Camp 2023)
4. Statistiken zum Einsatz von Staatstrojanern: Staatliche Überwachung: Erfahrungen und Beispiele aus der Praxis (2024)

Artikel

- Um einen aktuellen Überblick (Oktober 2023) zum Thema Staatstrojaner zu bekommen: https://netzpolitik.org/2023/gesetzentwurf-polizei-soll-staatstrojaner-etwas-seltener-nutzen-duerfen/
- Pressemitteliung vom CCC zum neuen Gesetzentwurf: https://www.ccc.de/en/updates/2023/schon-wieder-staatstrojaner-vorm-verfassungsgericht
- Aktuelle Infos rund um Staatstrojaner findet ihr auch bei Netzpolitik

Hausdurchsuchung

Hier geht es um den Technikaspekt von Hausdurchsuchungen. Für den juristischen Teil gibt es eine eigene Seite im Legal-Teil des Wikis.

Laptop und andere Technik hausdurchsuchbar machen hat 2 Säulen:

1. Daten vor fremden Augen sichern
2. arbeitsfähig bleiben

Daten vor fremden Augen sichern

Allgemein

Alle angebotenen Betriebssystemupdates schnellstmöglich installieren.

Gerätespeicher verschlüsseln

- Android verschlüsseln
- iOS: ist von Haus aus verschlüsselt
- Windows verschlüsseln mit Bitlocker
- macOS verschlüsseln

Messenger

Verhindern, dass Team Blau sich Signal und Telegram mit eurer Nummer installieren kann:

- bei Signal eine PIN einrichten

- bei Telegram ein Passwort einrichten, denn Telegram synchronisiert alle Inhalte auf das Handy der Polizei, indass sie die Ersatzsimkarte vom Provider einlegen.

  Sollte dein Handy ohne Telegram-Passwort beschlagnahmt werden, keine Panik. Dann kannst du dein Telegram-Konto mittels https://my.telegram.org/auth?to=delete löschen.

PIN und Passwort solltest du in deinem Passwortmanager abspeichern.

nach Hausdurchsuchung arbeitsfähig bleiben

Die folgenden Schritte solltet ihr jetzt durchdenken, damit ihr nach einer Hausdurchsuchung arbeitsfähig bleibt.

- SIM-Karte nachbestellen: prüft vorher, ob ihr eine Hotline oder eine Onlinemöglichkeit findet, um bei eurem Mobilfunkanbieter eine SIM-Karte nachzubestellen.
  Die Lieferzeiten sind sehr unterschiedlich: Beim klimafreundlichen Anbieter WEtell geht das z.B. innerhalb eines Werktages; bei ALDI TALK dauert es 8 Werktage.

  Wenn ihr die Handynummer behaltet, dann sperrt ihr die Polizei aus Signal aus.
- Zugriff auf Passwörter behalten: Passwortmanager-Bitwarden
- verschlüsseltes Backup bei fernen Verwandten oder Nicht-LG-Freunden aufbewahren. Eine sichere Verschlüsselung für Backups von:
  - Laptops: z.B. `restic`.
  - iOS: auf einem Mac oder einem Windows-Computer mit iTunes herstellen. Wichtig: Backup mit Passwort sichern, damit es vollständig ist.
  - Android: bitte ergänzen, wie das genau geht.
- Habt ihr irgendwo eine 2-Faktor-Authentifizierung (2FA) aktiviert? Dann überlegt, ob ihr da noch rankommt, wenn die Technik von zu Hause verschwunden ist.

Skillshare-Video

_skillshare_passwortmanager_und_ger%C3%A4te_verschl%C3%BCsseln-youtube.png

Tipps für's Smartphone

1. Ihr könnt im Telefon Notfall-Kontakte hinterlegen. Die könnt ihr anrufen, ohne das Handy entsperren zu müssen. Da könnt ihr z. B. die Nummer vom EA hinterlegen oder von Menschen, die bei euch im Haus wohnen. Anleitung:

   https://www.chip.de/news/Notfallinfos-auf-dem-Sperrbildschirm-Das-kann-im-Ernstfall-Ihr-Leben-retten_184234487.html Es ist jedoch unrealistisch, dass die Polizei bei einer Hausdurchsuchung erlaubt, dass ihr euer eigenes Telefon berührt.
2. Wir haben die Erfahrung gemacht, dass die Polizei beschlagnahmte Smartphones in den Flugmodus setzt. Sie haben manchmal auch spezielle Beutel mit Powerbank, um das Telefon angeschaltet, aber funklos zu halten. Damit kann sie verhindern, dass das Gerät nicht aus der Ferne gelöscht wird.
   - auf Android:
     In den Quick Settings könnt ihr den Flugmodus aktivieren bzw mobile Daten ausschalten. Prüfe, ob das auch aus dem Sperrbildschirm heraus geht, ohne die PIN eingeben zu müssen. Wenn die PIN nicht eingegeben werden muss, kanns du Flugmodus/'mobile Daten ausschalten' aus dem Quick Menü entfernen.

     Um die Fernöschlung zu testen hier einloggen

     Hier könnt ihr euch mal anschauen, wie das dann ausschaut.
   - auf iOS:
     In der Einstellungen-App auf „Face/Touch ID & Code“ gehen und das „Kontrollzentrum“ abschalten. Dann lässt sich das Telefon nicht mehr in den Flugmodus stellen.

     Die Fernlöschung lässt sich nach der Beschlagnahme über iCloud.com » „Wo ist?“ aktivieren. Da Apple zum Einloggen bei iCloud.com einen 2. Faktor verlangt ist es praktisch, einen Notfall-Kontakt zu hinterlegen, der dann die SMS bekommt, wenn euer Handy bei der Polizei ist.
3. Es ist auch schon vorgekommen, dass mit Hilfe abgenommener Fingerabdrücke ein Smartphone entsperrt wurde.
4. Einige Menschen empfehlen, kein Face-ID zum Entsperren des Telefons zu nutzen. Face-ID ist automatisch ausgeschaltet, wenn ihr das Telefon ausschaltet. Außerdem ist es aus, wenn ihr die Seitentaste und eine der Lautstärketasten zwei Sekunden lang gedrückt haltet. Ausschalten ist eine gute Routine vor dem Einschlafen. Sonst hält euch die Polizei das Gerät vor's Gesicht und es ist entsperrt. Das klappt allerdings nicht, wenn ihr die Augen geschlossen haltet (Aufmerksamkeitsprüfung für Face ID).

E-Mails

Wenn deutsche Mailanbieter wie GMX, Web.de oder Posteo einen korrekten Gerichtsbeschluss zur Herausgabe von Daten bekommen, dann werden sie deine Mails herausgeben. Typischerweise ist

das keine Liveüberwachung, sondern eine Herausgabe zu einem fixen Zeitpunkt oder die Beschlagnahme des Kontos.

Das kannst du mit folgenden Strategien verhinden - eine davon reicht:

- Anbieter außerhalb der EU, der nicht mit Deutschland zusammenarbeitet.
- Mails mit PGP-Verschlüsselung empfangen und senden (für einzelne Mails einfach, flächendeckend unmöglich)
- zu einem Provider gehen, der Mails aus technischer Sicht nicht herausgeben kann:
  - ProtonMail: proton.me/legal/transparency
  - Mailadressen, die auf sicherer Infrastruktur abgelegt sind, z.B. @letztegeneration.org (nur für AGs, WiGs und interne Gruppen; nicht für Personen)

Google-Account

Bedenke auch: wo liegt dein Google-Konto? Bekommst du da Mails wie „Ihnen wurde das Google Doc Xyz freigegeben“? Falls ja, kann die Polizei das Dokument von Google bekommen, falls sie deine Mails lesen können. Es ist auch bereits vorgekommen, dass die StA Google per Gerichtsbeschluss gezwungen hat, ein von LG genutztes Konto zu sichern und zu schließen. Das bedeutet, dass auf einen Schlag alle Google-Dokumente unzugänglich werden, die diesem Konto gehören. Google-Konten lassen sich auch für Mailadressen anlegen, die bei einem Mailprovider liegen, der keine Mails an die Polizei rausgibt - siehe oben.

Die IT-AG empfiehlt, statt Google Docs unsere Nextcloud zu nutzen. Die findet ihr unter cloud.raz-ev.org/apps/files/

Hilfe dazu gibt es hier im Wiki.

ios-kontrollzentrum-deaktivieren.png

Checkliste Sicherer Umgang mit Technik

Vorbereitung auf Hausdurchsuchungen & sicherer Umgang mit Technik

Neben den Checklisten findest du unten auch eine Liste mit hilfreichen Links.

Vorbereitung auf eine Hausdurchsuchung

Spiele es mal durch: Angenommen die Polizei schaut morgen vorbei und nimmt dir deine Geräte weg. Wie gut bist du vorbereitet?

- ☐ Alle meine Geräte sind verschlüsselt (Laptop, Handy, Tablet, externe Festplatten, USB-Sticks, SD-Karten) (warum das manchmal nicht reicht)
  - ☐ Auf Android nutze ich für Signal die Molly-App (mehr dazu hier TODO)
- ☐ Ich habe Sachen aus der Wohnung geschafft, die die Polizei nicht mitnehmen/sehen soll, z. B. externe Festplatten mit Familienfotos, alte Tagebücher oder unverschlüsselte Festplatten, die du noch nicht verschlüsselt hast
- ☐ Ich mache regelmäßig Backups auf externe Datenträger

- [ ] Ich nutze lieber eine private Nextcloud anstatt Google Drive oder die Microsoft/Apple-Cloud. Mir ist bewusst, dass Unternehmen/Dienstleister meine Daten an die Polizei herausgeben und meine Accounts sperren/einfrieren können.
- [ ] Meine Backups sind verschlüsselt
- [ ] Ich habe auch Backups, die nicht zu Hause gelagert sind (falls die Polizei sie mitnimmt)
- [ ] Meine Backups enthalten alles wichtige (Passwörter, Signal-Account, Browser-Historie/Lesezeichen, Kontakte, Dokumente)

☐ Ich kann auch nach der Hausdurchsuchung auf meine Passwörter zugreifen (denke auch an Zwei-Faktor-Authentifizierung)

☐ Ich kann auch nach der Hausdurchsuchung auf Kalender, Kontakte und Dokumente/Cloud zugreifen

☐ Ich habe im Vorfeld mit meinen Mitbewohner*innen gesprochen und teile diese Informationen mit ihnen

☐ Ich nutze keine biometrischen Mittel (Fingerabdruck, Gesichtserkenung) zum Entsperren von Geräten. Die Polizei darf euch mit Gewalt dazu zwingen, Geräte zu entsperren. Das ist rechtlich mittlerweile eindeutig geklärt und wird auch in der Praxis so umgesetzt.

Erfahrungen bei Letzten Generation

Bei der Letzten Generation haben wir die Erfahrung gemacht, dass die Polizei alle elektronischen Geräte der beschuldigten Person mitnimmt. Wenn sich der Beschluss gegen dich richtet hast du darauf keinen Einfluss. Aber wenn sich die Durchsuchung nicht gegen dich richtet (Gäst*innen/Mitbewohner*innen), dann beschwert euch lautstark/wehement, dass diese Sachen nicht mitgenommen werden.
Bei den bisherigen Durchsuchungen war es dann oft so, dass sich die Polizei die Geräte vor Ort anschaut und prüft, ob auf dem Gerät relevante Informationen vorhanden sind. Sie entscheidet dann vor Ort, mit unterschiedlichem Ausgang:

- Menschen durften ihre Technik behalten
- die Festplatte wurde vor Ort gespiegelt (kopiert), dafür wurde sie nicht mitgenommen
- Festplatte/Laptop wurde trotzdem mitgenommen

Wichtig dabei: Die Menschen mussten dabei ihre Geräte (Handy/Laptop) entschlüseln/entsperren. Das ist natürlich gefährlich. Deshalb müsst ihr euch **vorher** fragen, wie wichtig euch das jeweilige Gerät ist und wie sensibel die Daten darauf sind. Teilweise haben haben Menschen ihr Smartphone entsperrt, um zu zeigen, dass es ihr Smartphone ist. Es wurde dann nicht beschlagnahmt.

Macht euch auch bewusst, dass eine Hausdurchsuchung eine absolute Stress-Situation ist. Menschen wurden von der Polizei unter Druck gesetzt und haben Passwörter herausgegben/eingegeben. Ihr müsst der Polizei nicht eure Passwörter geben. Ihr habt das Recht, keine Aussage zu machen und euch nicht selbst zu belasten. Dazu gehört auch das Verweigern der Herausgabe der Passwörter.

Die 4 goldenen Sicherheitsregeln

- ☐ Alle meine Geräte sind verschlüsselt (warum das manchmal nicht reicht)
- ☐ Ich nutze für digitale Kommunikation ausschließlich Ende-zu-Ende-Verschlüsselung. Das schützt mich (und andere!) vor einer möglichen Telekommunikationsüberwachung (TKÜ)
  - ☐ Ich telefoniere/schreibe ausschließlich über Signal
  - ☐ Ich aktiviere verschwindende Nachrichten auf Signal
  - ☐ Ich nutze PGP für E-Mail-Verschlüsselung, bzw. verzichte möglichst auf E-Mail-Kommunikation
- ☐ Wenn ich in Aktion gehe, nutze ich nicht mein privates Telefon, sondern ein Aktions-Telefon
- ☐ Ich gehe davon aus, dass die Polizei das Aktions-Telefon entsperren und auslesen kann (meist alte Android-Geräte). Ich setze das Gerät vor der Aktion auf Werkseinstellungen zurück und achte darauf, was für Daten darauf gespeichert sind.

Umgang mit Signal

- ☐ Ich hinterlege eine Signal-PIN hinterlegt (Registration Lock/Registrierungssperre), damit bei der Neu-Einrichtung des Accounts eine PIN eingegeben werden muss - der Empfang einer SMS reicht dann nicht mehr aus (falls die Polizei die SIM-Kartei beschlagnahmt, Dokumentation)
- ☐ Ich aktiviere verschwindende Nachrichten (auch als Standardeinstellung für neue Chats)
- ☐ Ich nutze Signal auch auf dem Laptop, um im Falle eines gestohlenen/defekten/beschlagnahmten Gerätes weiter arbeitsfähig zu bleiben
- ☐ Ich kann auch noch noch Bildschirmsperre (Screen lock) aktivieren, die eingegeben werden muss, um die Signal-App auf dem Handy zu öffnen (Dokumentation)

☐ Ich nutze die Backup-Funktion von Signal und backupe ein paar mal im Jahr meine Signal-Chats/Kontakte auf meine **verschlüsselte** externe Festplatte (Dokumentation)

☐ Ich schaue in Signal (und anderen Messengern) nach "linked devices" (verknüpften Geräten). Die Polizei nutzt das Feature, um verschlüsselte Messenger abzuhören (Quelle)

☐ Auf meinem Sperrbildschirm werden keine Inhalte angezeigt (Dokumentation)

Empfehlungen

- Smartphone Empfehlung: Besorgt euch ein gebrauchtes Google Pixel Smartphone auf Kleinanzeigen und installiert das GrapheneOS Betriebssystem
- Nutze Chat-Ordner in Signal, um einen besseren Überblick zu behalten
- Auf Android kann ich Molly installieren, um ganz einfach einen zweiten Signal-Account nutzen zu können (eine zweite Signal-App)
- Ihr könnt eure Telefon-Nummer verstecken. Dann wird sie in (Gruppen-)Chats nicht mehr angezeigt. Allerdings erschwert das die Kontaktaufnahme. Wenn die Polizei es schafft, euer Handy auszulesen, dann kommt sie an euren Signal-Account (eure "Account ID"). Mit der kann sie zu Signal gehen und nach der hinterlegten Telefonnummer fragen (Dokumentation).

Kontakt

Meldet euch gerne bei Fragen oder Anregungen mit einer Mail an it-support@raz-ev.org (gerne auch PGP verschlüsselt).

Links

- Verschlüsselung:
  - Allgemeines zum Thema Verschlüsselung
  - Windows verschlüsseln mit Bitlocker
  - Windows verschlüsseln mit Veracrypt
  - Externe Festplatte/USB-Stick verschlüsseln
  - Android verschlüsseln
  - MacOS verschlüsseln

    - PGP-Verschlüsselung einrichten
- Signal:
    - Signal sicher benutzen
    - Signal auf dem Laptop nutzen
    - Mehrere Signal-Accounts auf dem Handy nutzen
- Generelles:
    - Auf eine Hausdurchsuchung vorbereiten
    - Bitwarden Passwort-Manager
    - Nextcloud
- externe Ressourcen
    - Vortrag (mit LG-Bezug): Staatliche Überwachung: Erfahrungen und Beispiele aus der Praxis
    - Checkliste mit konkreten Vorschlägen zur Verbesserung deiner Smartphone-Sicherheit
    - Webseite von esc-it (Kollektiv, das IT-Sicherheitstrainings für Aktivist*innen gibt)
    - IT-Sicherheitstrainings für Aktivisti

Staatstrojaner in Deutschland

Staatstrojaner in Deutschland

2011 hat der CCC (Chaos Computer Club) einen deutschen Staatstrojaner aufgedeckt. Auf dieser Seite findet ihr Vorträge vom CCC mit einer gesellschaftlichen, rechtlichen und technischen Einordnung.

1. Aufdeckung, Analyse und Bewertung: 28c3: Der Staatstrojaner, (Youtube, aus 2011).
2. Ein Jahr später: Was ist seitdem passiert: 29c3 staatstrojaner (Youtube, aus 20212.
3. Stand 2023: Über den Gesetzesvorschlag der Ampel zur Einschränkung von Staatstrojanern: Staatstrojaner für bereits begangene Straftaten (Youtube, Camp 2023)
4. Statistiken zum Einsatz von Staatstrojanern: Staatliche Überwachung: Erfahrungen und Beispiele aus der Praxis (2024)

Artikel

- Um einen aktuellen Überblick (Oktober 2023) zum Thema Staatstrojaner zu bekommen: https://netzpolitik.org/2023/gesetzentwurf-polizei-soll-staatstrojaner-etwas-seltener-nutzen-duerfen/
- Pressemitteliung vom CCC zum neuen Gesetzentwurf: https://www.ccc.de/en/updates/2023/schon-wieder-staatstrojaner-vorm-verfassungsgericht
- Aktuelle Infos rund um Staatstrojaner findet ihr auch bei Netzpolitik