HINWEISE ZUR IT-SICHERHEIT FÜR POLITISCHE GRUPPEN

KLARA KOLLEKTIV

klara-kollektiv@riseup.net

2019–04–30

Inhalte

1 Allgemeine Hinweise

Dieses Dokument erhebt keinen Anspruch auf Vollständigkeit, sondern soll einen kompakten Überblick über kritische Punkte bei der Verwendung von IT in politischen Gruppen geben. Auf die Darstellung technischer Details wird im Weiteren weitgehend verzichtet. Das Dokument kann frei vervielfältigt und geteilt werden.

Sicherheit ist ein kontinuierlicher Prozess. Mitglieder einer Gruppe sollten diskutieren, welche Maßnahmen angesichts der Art der politischen Arbeit sinnvoll sind und welche Maßnahmen unangemessenen Aufwand zur Folge haben. Es ist gut, wenn sich Mitglieder gegenseitig bei der Umsetzung unterstützen. Damit Einzelpersonen und Gruppen sich (angst)frei engangieren können ist es wichtig, sich eine sichere Kommunikationsinfrastruktur aufzubauen, diese aufrechtzuerhalten, und bei Veränderungen anzupassen (etwa wenn sich gesetzliche Rahmenbedingungen und Technologien ändern).

Ganz allgemein zunächst folgende Hinweise:

— Private und politische Nutzung von Diensten voneinander entkoppeln (getrennte Identitäten)

— Politische Aktivitäten und Gruppenzugehörigkeit nicht-vertrauten Personen verschweigen

— Informationen über politische Aktivitäten, Gruppenzugehörigkeit und persönliche Details können zu Repression führen, bilden allerdings oftmals eine Grundlage für den Zusammenhalt, das Wachstum und das Wirken einer Gruppe. Je nach Schwerpunkt der Arbeit müssen Gruppen also eine gute Balance zwischen Verschwiegenheit und Offenheit finden

— Sichere Kommunikation dient nicht nur dem Schutz der eigenen Identität, sondern auch dem Schutz der Identität anderer Personen

— Geräte vor fremdem Zugriff schützen (etwa durch Verschlüsselung des Betriebssystems und Herunterfahren des Systems bei Abwesenheit)

— Betriebssysteme und Programme stets updaten (Schließung von Sicherheitslücken durch Updates)

— Keine unbekannten E-Mail-Anhänge öffnen

— Vorsicht bei unbekannten Speichermedien

— Verschlüsselte Backups von wichtigen Daten machen und an einem anderen Ort hinterlegen

— Es ist sinnvoll, über mehrere sichere Kommunikationskanäle zu verfügen, um einen zeitweisen Ausfall von Technologien oder Plattformen kompensieren zu können

— Leider gibt es niemals einen hundertprozentigen Schutz. Sicher in Bezug auf Verschlüsselung heißt immer auch *aktuell* sicher und nicht entschlüsselbar. Es ist durchaus denkbar, dass Verschlüsselungsmethoden, die heute als sicher gelten, in ein paar Jahren aufgrund des raschen Anstiegs von Rechenleistung keinen ausreichenden Schutz mehr bieten

2 Kommunikation mit Mobiltelefonen

2.1 SMS und Anrufe

Provider speichern den Inhalt von SMS-Nachrichten, bei Anrufen werden Verbindungsdaten gespeichert. Daher gilt:

— Möglichst nicht per SMS kommunizieren

— Anrufe verschlüsselt über Messenger-Dienste tätigen

2.2 Messenger

Aufgrund der zuvor beschriebenen Punkte zu SMS und Anrufen gilt es die Kommunikation ausschließlich über verschlüsselte Wege abzuwickeln. Es gibt eine Vielzahl von Messenger-Diensten, die kostenfrei oder sehr günstig Ende-zu-Ende-Verschlüsselung für Nachrichten und Anrufe anbieten, z.B. *Briar* oder *Wire*. Generell sollten bei der Nutzung von Messenger-Diensten folgende Punkte beachtet werden:

- Der Gruppenname sollte nicht dem tatsächlichen Namen der Gruppe entsprechen
- Ausgeschiedene Mitglieder sollten nicht mehr Teil einer Messenger-Gruppe sein
- Am besten für private und politische Aktivitäten nicht den gleichen Dienst verwenden
- Hat die Gruppe eine öffentliche Seite auf einer Plattform, sollte die interne Kommunikation der Gruppe nicht auch noch über einen Messenger-Dienst derselben Plattform laufen (z.B. Facebook und WhatsApp)

Je nach Verwendungszweck sind verschiedene Features mehr oder weniger wichtig. Wichtige Eigenschaften eines Messenger-Dienstes sind vor allem:

- Ende-zu-Ende-Verschlüsselung
- Keine Speicherung von Inhalten auf einem zentralen Server
- Keine Nummernbindung (Accounts sind nicht an Mobilfunknummer gebunden, wodurch eine Identifikation von Mitgliedern über deren Nummern erschwert wird)
- Open-Source-Software (Quelltext ist öffentlich einsehbar und somit eher auf Schwachstellen oder Hintertüren prüfbar)

Eine gute Übersicht über verschiedene Messenger-Dienste und ihre Eigenschaften gibt es z.B. hier:

https://mobilsicher.de/apps-kurz-vorgestellt/verschluesselt-kommunizieren-per-app

3 Ortung und Abhören von Mobiltelefonen

Auch unbeteiligte Personen können schnell und unbemerkt in Funkzellenabfragen gelangen, z.B. bei Demonstrationen. Funkzellenabfragen sind Auswertungen von Telekommunikationsverbindungen, die in einer Funkzelle in einem bestimmten Zeitraum anfallen. Überdies sucht jedes Mobiltelefon mit aktiviertem WLAN permanent nach WLAN-Verbindungen. Die ausgesendeten Signale können registriert werden, und durch WLAN-Tracking können Bewegungsprofile erstellt werden. Ähnliches gilt für Bluetooth. Überdies können Ermittlungsbehörden (nach richterlichem Beschluss) über eine sogenannte stille SMS Telefone orten oder Bewegungsprofile erstellen.

- Zum Schutz vor Ortung sollten Mobiltelefone auf kritischen Veranstaltungen ausgeschaltet werden, am besten bereits vor der Anfahrt
- WLAN sollte nur verwendet werden, wenn tatsächlich eine Verbindung benötigt wird
- Zum Schutz vor Abhören sollten Mobiltelefone bei kritischen Veranstaltungen nicht nur ausgeschaltet werden, sondern auch ihr Akku entfernt werden oder in einen anderen Raum platziert werden. Es ist technisch möglich, dass Mobiltelefone derart kompromitiert sind, dass ein Herunterfahren lediglich vorgegaukelt wird, um unbemerkt Konversationen abzuhören

4 Passwörter

4.1 Erstellung von Passwörtern

Ein sicheres Passwort zeichnet sich aus durch Länge und Komplexität (großer Zeichenraum) sowie Nicht-Nachschlagbarkeit.

- Grundsätzlich sind längere Passwörter besser
- Keine Namen oder nachschlagbare Wörter, Zahlenreichen oder Tastaturreihen verwenden
- Ein starkes Passwort enthält Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen
- Zur Erstellung von Passwörtern können Eselsbrücken verwendet werden, wie etwa die Wahl aller Anfangsbuchstaben eines Satzes mit Satzzeichen und Zahlen
- Passwörter für alle Zugänge in regelmäßigen Abständen ändern
- Niemals ein Passwort für mehr als einen Account verwenden

Weitere Hinweise zur Erstellung eines sicheren Passwortes gibt es z.B. hier:

https://www.heise.de/tipps-tricks/Sicheres-Passwort-finden-so-klappt-s-3836799.html

Viele Personen nutzen zur Entsperrung ihres Mobiltelefons Swipe-Patterns. Diese sind zwar angenehmer einzugeben, jedoch grundsätzlich weniger sicher als normale Passwörter. Es gibt weniger mögliche Kombinationen als bei normalen Passwörtern, da nur aufeinanderfolgende Punkte verbunden werden können und zwei gleiche Punkte nicht nacheinander verwendet werden können. Oftmals folgen die Muster vorhersehbaren Mustern und weisen Zusammenhänge mit Eigenschaften einer Person auf (z.B. Händigkeit und Name). Fettspuren auf dem Display können außerdem Rückschlüsse auf das Muster zulassen. Auch die Entsperrung über Gesichtserkennung und Fingerabdrucksensor lässt sich überlisten. Ohne weitere Kenntnis der verwendeten Methode und ihrer Sicherheit ist es daher ratsam, stattdessen starke Passwörter zu verwenden.

- Normales Passwort statt Swipe-Pattern verwenden (auch hier gilt: länger ist besser)
- Bei Swipe-Patterns lange & komplexe Patterns verwenden (z.B Richtungswechsel und Überkreuzen)
- Option 'Pattern sichtbar machen' deaktivieren

4.2 Speicherung von Passwörtern

Passwörter sollten niemals zugänglich niedergeschrieben sein und es ist nicht sicher, Passwörter für Online-Zugänge im Browser zu speichern. Bei zu vielen oder schwer zu merkenden Passwörtern bietet es sich an, einen Passwort-Manager zu verwenden, wie z.B. *KeePassXC* für Windows, Linux und macOS:

https://keepassxc.org/

5 Verschlüsselung von Dateien und Betriebssystemen

Es ist sinnvoll, bestimmte Dateien oder sogar das ganze Betriebssystem zu verschlüsseln. So kann z.B. das Login-Passwort unter Windows einfach und schnell umgangen werden. Um einzelne Dateien zu verschlüsseln, können diese in einem verschlüsselten Container abgelegt werden. Dieser Container ist eine Datei mit einer festen Größe, die nach dem Entschlüsseln wie ein Laufwerk behandelt wird. Solch ein verschlüsselter Container kann auch auf USB-Sticks erstellt werden. Es sollte ein langes Passwort gewählt werden, welches nicht nachschlagbar ist. Unter Umständen ist das Ablegen von Dateien in einem verschlüsselten Container jedoch nicht ausreichend. Denn obwohl auf den Inhalt von Dateien nach dem

Schließen des Containers nicht mehr zugegriffen werden kann, ist unter Windows im Schnellzugriff des Explorers sichtbar, welche Dateien zuletzt verwendet wurden. Wenn dies kritisch ist, sollte das ganze Betriebssystem verschlüsselt werden.

5.1 Desktop-Computer

Mit dem Programm *Veracrypt* (es gibt natürlich noch weitere geeignete Programme) kann eine Systempartition verschlüsselt werden, oder ein verschlüsselter Container erstellt werden. *Veracrypt* läuft unter Windows, Linux und macOS. Die sogenannte *Full Disk Encryption*, also die Verschlüsselung einer gesamten Festplatte, unterstützt *Veracrypt* allerdings nur für Windows. *Full Disk Encryption* von Linux-Betriebssystemen ist möglich mit *LUKS*, für macOS kann *FileVault* verwendet werden.

Veracrypt kann hier heruntergeladen werden:

https://www.veracrypt.fr/en/Downloads.html

Anleitung zum Erstellen eines verschlüsselten Containers mit *Veracrypt*:

https://www.kim.uni-konstanz.de/e-mail-und-internet/it-sicherheit-und-privatsphaere/sicheres-endgeraet/datenverschluesselung/containerverschluesselung-mit-veracrypt/

Anleitung zum Verschlüsseln einer Windows-Systempartition mit *Veracrypt*:

https://www.kim.uni-konstanz.de/e-mail-und-internet/it-sicherheit-und-privatsphaere/sicheres-endgeraet/datenverschluesselung/verschluesselung-einer-systempartition-mit-veracrypt/

Anleitung zur Festplattenverschlüsselung unter Linux mit *LUKS*:

https://wiki.ubuntuusers.de/LUKS/

Anleitung zur Festplattenverschlüsselung unter macOS mit *FileVault*:

https://support.apple.com/en-us/HT204837

5.2 Mobile Geräte

Hinweise zum Verschlüsseln von Android-Betriebssystemen gibt es z.B. hier:

https://mobilsicher.de/kategorie/verschluesseln-passwoerter/android-geraet-verschluesseln

6 Surfen und andere Aktivitäten

6.1 Anonymes Surfen

Kritische Seiten sollten ausschließlich mit dem *Tor*-Browser aufgerufen werden. *Tor* ist ein Anonymisierungs-Netzwerk, welches ein hohes Maß an Anonymität bietet, vorausgesetzt die UserInnen geben keine Informationen preis, die ihre Identität offenlegen. Es gibt es auch Situationen, in denen *Tor* keinen definitiven Schutz der Anonymität bietet. Folgende Punkte sind zu beachten:

- Keine privaten und politischen Aktivitäten zeitgleich durchführen (z.B. nicht davor oder währenddessen auf Facebook mit dem privaten Account einloggen)
- Keine persönlichen Informationen preisgeben

— Keine HTTP-Websiten besuchen

— Keine 2-Step-Verifikation (mit Mobiltelefon) von Anmeldungen durchführen

— Suchmaschinen verwenden, welche keine Suchanfragen speichern oder Nutzerprofile erstellen (z.B. *DuckDuckGo* oder *Startpage*)

Der *Tor*-Browser kann hier heruntergeladen werden:

https://www.torproject.org/

6.2 E-Mail-Verschlüsselung

Die E-Mail-Kommunikation (im Idealfall natürlich jede Form der Kommunikation) einer politischen Gruppe intern und nach außen erfolgt im besten Fall ausschließlich verschlüsselt, sodass niemand außer den Empfängern und Absendern den Inhalt zu sehen bekommt. Es gibt verschiedene Methoden, E-Mails zu verschlüsseln. Eine häufig verwendete und zu empfehlende Methode ist eine Verschlüsselung basierend auf einer Public-Key-Infrastruktur, wie OpenPGP (Open Pretty Good Privacy). Mit PGP können E-Mails verschlüsselt und signiert werden. Jedoch wird lediglich der Inhalt einer Nachricht verschlüsselt, nicht aber ihr Betreff oder die Meta-Daten der Kommunikation (z.B. wer mit wem kommuniziert hat). Eine Verschlüsselung mit PGP kann z.B. mit einem E-Mail-Programm wie *Mozilla Thunderbird* und der Erweiterung *Enigmail*, oder mit der Browser-Erweiterung *Mailvelope* realisiert werden. Mit der *Enigmail*-Version 2.0 (Erweiterung für das E-Mail-Programm *Mozilla Thunderbird*) kann nebst der Nachricht auch die Betreffzeile verschlüsselt werden.

Das Prinzip einer PGP-Verschlüsselung kann auf folgende Punkte heruntergebrochen werden:

— Bei einer Verschlüsselung mit PGP kommen zwei Schlüssel zum Einsatz: Der Private (oder Secret) Key und der Public Key. Beide Schlüssel sind reine Textdateien

— Mit dem Public Key wird eine Nachricht verschlüsselt, mit dem Private Key wird eine Nachricht entschlüsselt

— Zum Versenden einer PGP-verschlüsselten Nachricht wird der öffentliche Schlüssel des Gegenübers benötigt

— Der eigene öffentliche Schlüssel kann per Mail versendet werden, oder auf sogenannte Keyserver hochgeladen werden. Dort kann sich eine Kontaktperson dann den Schlüssel holen

— Der Private Key muss privat, also geheim bleiben

— Mit einer Signatur kann überprüft werden, ob eine Nachricht tatsächlich von der gewünschten Person versendet wurde

Anleitungen zur Verschlüsselung von E-Mails mit PGP gibt es z.B. hier:

https://support.mozilla.org/de/kb/nachrichten-digital-signieren-und-verschlusseln

https://netzpolitik.org/2013/anleitung-so-verschlusselt-ihr-eure-e-mails-mit-pgp/

Ein Benutzer-Manual zu *Enigmail* gibt es z.B. hier:

https://www.enigmail.net/index.php/en/user-manual

Um verschlüsselten E-Mail-Verkehr über das Anonymisierungs-Netzwerk *Tor* zu leiten, wird das *Tor Browser Bundle* und das E-Mail-Programm *Mozilla Thunderbird* mit der Erweiterung *Tor Birdy* benötigt. Eine Anleitung dazu gibt es z.B. hier:

https://www.privacy-handbuch.de/handbuch_24e.htm

https://www.whonix.org/wiki/Encrypted_Email_with_Thunderbird_and_Enigmail

6.3 Anonymes Betriebssystem

Für kritische Aktivitäten sollte am besten ein ein anonymes Betriebssystem verwendet werden, welches darauf ausgelegt ist, Anonymität und Privatsphäre zu gewährleisten. Hier bietet sich z.B. *Tails* an. *Tails* ist ein auf Linux basierendes Live-Betriebssystem, welches anonymes Surfen ermöglicht und auf dem verwendeten Rechner keine Datenspuren hinterlässt. *Tails* enthält viele nützliche Programme, wie z.B den *Tor*-Browser. Das Betriebsystem kann hier heruntergeladen werden:

https://tails.boum.org/install/

Auf der Website des *Tails Project* gibt es eine ausführliche Dokumentation sowie Installationsanleitungen zu *Tails* für verschiedene Betriebssysteme:

https://tails.boum.org/index.de.html

Eine Anleitung zur Nutzung von *Tails* gibt es z.B. hier:

https://capulcu.blackblogs.org/wp-content/uploads/sites/54/2019/01/Tails2019-01-27-A4.pdf

6.4 Metadaten in Dokumenten

Textdokumente und Bilddateien enthalten oft Metadaten, selbst wenn die entsprechende Option zum Übernehmen der Benutzerdaten im Text-Editor deaktiviert wurde. Daher sollte vor dem Upload geprüft werden, welche Metadaten das Dokument enthält. Auch unkritisch erscheinende Metadaten können Rückschlüsse auf die Identität einer Person zulassen. Es gibt spezielle Programme zum Entfernen von Metadaten, wie z.B. *MAT* für Linux, *ExifTool* für Windows, Linux und macOS oder *ExifToolGUI* für Windows. Manchmal können Metadaten jedoch nicht vollständig entfernt werden oder sie können wiederhergestellt werden (dies kann z.B. bei PDF-Dokumenten der Fall sein). Daher ist es wichtig, sich alle Metadaten ausgeben zu lassen und zu entscheiden, ob das Dokument veröffentlicht werden kann.

- Einen Text abzutippen anstatt eine Datei hochzuladen ist immer sicherer
- Spezielle Tools verwenden, um Metadaten aus Dateien zu entfernen
- Vor dem Upload von Dateien stets überprüfen, ob tatsächlich alle kritischen Metadaten entfernt wurden
- Eher eine einfache .txt-Datei erstellen, anstelle einer *Word*- oder *Libre-Office*-Datei (solche Programme legen standardmäßig meist mehr Metadaten an)

6.5 Löschung von Daten

Wenn Daten gelöscht werden sollen, ist Vorsicht geboten - meist werden vom Betriebssystem nur die Verweise auf die Daten gelöscht, nicht aber Daten selbst (auch wenn diese aus dem Papierkorb gelöscht wurden). Sie können dann mit entsprechender Software wiederhergestellt werden. Die Daten werden erst gelöscht, wenn der belegte Speicherbereich mit neuen Daten überschrieben wird. Hierzu gibt es spezielle Tools, wie z.B. *Disk Wipe* (für Windows), *Nautilus Wipe* (für Linux) oder *Disk Utility* (für macOS).

7 Verwendung von Pseudonymen

Pseudonyme, die in Online-Foren verwendet werden, sollten nicht im Messenger-Dienst genutzt werden (und auch nicht privat). Die Klarnamen der Personen sollten auch nicht in einer Gruppe des Messengers verwendet werden. Durch Verwendung eines Messengers ohne Nummernbindung kann dies eher umgesetzt werden. Im Idealfall werden die Klarnamen von Personen überhaupt nicht nach innen kommuniziert.

- Verschiedene Pseudonyme für verschiedene Zwecke, Dienste oder Gruppen verwenden
- Pseudonyme nicht nach außen kommunizieren

8 Aufnahme neuer Personen in eine Gruppe

Es gibt immer wieder Berichte über Spitzel (also verdeckte ErmittlerInnen oder InformantInnen), die sich in politischen Gruppen bewegen. Neue Personen sollten daher keinen sofortigen Zugang zur Kommunikations-Infrastruktur und zu den Accounts der Gruppe erhalten. Es sollte außerdem sichergestellt werden, dass Mitglieder welche die Gruppe verlassen, keinen Zugriff mehr darauf haben.

9 Weiterführende Links und Literatur

- **Capulco**

  Capulco ist eine kritische Gruppe von AktivistInnen, die zahlreiche Texte und Broschüren zu sicherheitstechnischen und gesellschaftspolitischen Aspekten von IT-Systemen veröffentlicht, sowie Veranstaltungen und Schulungen anbietet.

  https://capulcu.blackblogs.org

- **Chaos Computer Club**

  Auf der Website des *Chaos Computer Clubs* gibt es eine Vielzahl von Videos von Vorträgen, die sich um das Thema IT-Sicherheit drehen. Viele der Vorträge sind auch für Laien verständlich. Hier einige Beispiele:

  https://media.ccc.de/v/pw17-226-das_tor_okosystem

  https://media.ccc.de/v/pw17-97-sichere_authentifizierung

  https://media.ccc.de/v/35c3-10018-verhalten_bei_hausdurchsuchungen

- **Digitalcourage**

  Der Verein *Digitalcourage* setzt sich für freie Kommunikation und Datenschutz ein und veröffentlicht Tipps zur »digitalen Selbstverteidigung« sowie Informationsmaterial zur Überwachung von Kommunikationsdaten, Reise- und Krankendaten, sowie Video- und Wohnraumüberwachung.

  https://digitalcourage.de/digitale-selbstverteidigung

  https://digitalcourage.de/ueberwachungsgesamtrechnung

— **Privacy-Handbuch**

Das *Privacy-Handbuch* enthält Anleitungen zum spurenarmen Surfen, zur Verschlüsselung von E-Mails und Daten sowie zur anonymen Kommunikation für Windows und Linux. Es wird fortlaufend aktualisiert und ist als HTML- und PDF-Version erhältlich.

https://privacy-handbuch.de

— **Tactical Technology Collective**

Das *Tactical Technology Collective* (mit Sitz in Berlin) gibt ein Manual heraus, welches einer ganzheitlichen (d.h. verschiedene Lebensbereiche betreffenden) Agenda zur Vermittlung sicherheitsrelevanter für politisch aktive Personen folgt. Das Manual ist als PDF frei verfügbar und kann hier heruntergeladen werden:

https://holistic-security.tacticaltech.org

https://holistic-security.tacticaltech.org/downloads.html