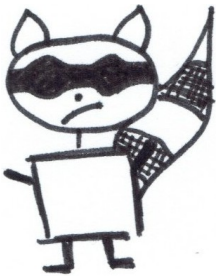
SURVEILLANCE SELF DEFENCE

A COLLECTIVE MATTER

Gedanken zu Kommunikationssicherheit, FOSS, Verschlüsselung, Smartphones und praktischen Tipps im Alltag



Stand: November 2020

Inhaltsverzeichnis

Kommunikationssicherheit

Durch die zunehmende Wichtigkeit von Information und Kommunikation wächst die Überwachungsgesellschaft immer weiter. Nationalstaaten reagieren auf neue Kommunikationstechnologien mit dem Aufbau von Infrastruktur, die einfach für totale soziale Kontrolle genutzt werden kann. Staatliche Überwachung hat eine lange Geschichte der Repression sozialer Bewegungen.

Konzerne sammeln, speichern und verkaufen unsere digitalen Spuren für an unser soziales Verhalten angepasste Werbung, damit wir mehr und mehr konsumieren. Eine relativ neu entdeckte Macht der Unternehmen gegenüber ihren Kund:innen.

Meist ist die erste Reaktion von Menschen, wenn sie von steigender Überwachung hören, eine Überforderung. Einige entscheiden, dass es unmöglich ist, sicher zu sein, also ergeben sie sich selbst der ständigen Überwachung oder geben alle Arten digitaler Kommunikation auf. Komplexe Fragestellungen oder Situationen auf ausschließlich zwei mögliche, simple, konträre Handlungsstrategien runterzubrechen ist eine Möglichkeit, mit Neuem umzugehen.

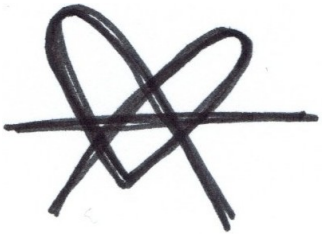
Die zentrale Frage bei digitaler Selbstverteidigung ist: “Was will ich vor wem schützen?”. Ein Anspruch könnte zum Beispiel sein, deine Kontakte, dich selbst, deine Dateien, deinen Standort und deine Kommunikation zu schützen. Es geht aber lange nicht mehr nur um das Benützen “richtiger” Tools oder Apps, die das verschleiern können. Deine digitalen Gewohnheiten (zB auf social media) sind das, was dich trotz allem verraten könnten. Was teilst du, was likest du? Mit wem

kommunizierst du? Wen lädst du wozu ein? Was klickst du an? Wo scrollst du drüber und wo bleibst du stehen?

Du kannst zum Beispiel all deinen Apps auf deinem Smartphone verweigern, auf deine Standortdaten zugreifen zu können. Und trotzdem kann über das Mobilfunksignal, Bluetooth, WLAN und auch über Bankomatkartenzahlungen in Geschäften ein ausgezeichnetes Bewegungsprofil von dir erstellt werden. Was kaufst du wo und wann ein?

Ja, 100 prozentige Sicherheit gibt's nicht. Deshalb gibt's einerseits einige Kollektive, die es sich zum Ziel gesetzt haben, einen hohen Grad an Sicherheit für alle einfach verfügbar zu machen. Andererseits gibt's auch Gruppen, die den Kampf gegen Überwachung durch das Führen von legalen Prozesse bestreiten.

Wichtig: Bei digitaler Sicherheit geht es nicht nur um das Risiko, das du für dich selbst bereit bist, einzugehen. Digitale Sicherheit ist eine kollektive Angelegenheit: Wir alle hängen voneinander ab! Verwende für digitale Kommunikation immer verschlüsselte Medien (wie zB signal oder verschlüsselte E-Mails) – auch, damit andere nicht exponiert sind.

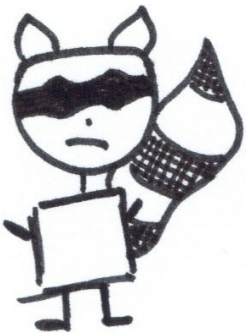


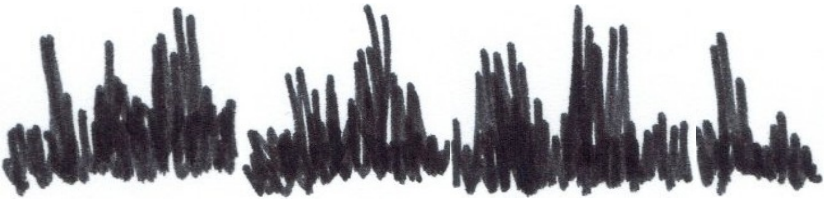
Free Open Source Software (FOSS)

Der Quellcode eines Programms wird im Englischen auch als Source Code bezeichnet.

Mit Closed Source wird Software bezeichnet, bei der der Source Code nicht öffentlich zugänglich ist. Die:der Benutzer:in kann das Programm nur installieren und anwenden. Es sind keine Änderungen im Code oder Überprüfung der Funktionsweise möglich.

Software, deren Quellcode der Welt offen steht - das heißt jede:r kann ihn lesen, ändern oder erweitern - wird als Open Source bezeichnet. Natürlich ist die meiste Software so komplex, dass auch vollkommene Transparenz des Codes keine Garantie dafür ist, dass im Quellcode keine mysteriösen Code-Schnipsel versteckt sind. Open Source ist nicht per se sicher. Free Open Source Software (FOSS) ist keine perfekte Lösung, stellt aber zumindest die beste (und einzige!) Garantie dar, dass die Software vertrauenswürdig ist. Die Alternative (Closed Source) kann dies nicht garantieren und verlangt absolutes Vertrauen in die jeweiligen Entwickler:innen.





Computer und Notebooks

Betriebssysteme

Windows ist immer noch das Standardbetriebssystem bei Computer und Notebooks, obwohl es teuer und proprietär, also in Eigentum befindlich, ist. Die Marktanteile an den weltweiten Page Views liegen bei rund 77%. Mit einem Marktanteil von 17,6% liegt macOS, auch teuer und proprietär, klar auf dem zweiten Platz. Dabei muss vielleicht nur kurz erwähnt werden, dass Microsoft bzw. Apple Inc. hinter den beliebten Betriebssystemen stecken.

Eine FOSS-Alternative ist Linux. Mit einer großen Gemeinschaft von Entwickler:innen und Nutzer:innen wird selbst dann, wenn wer ein Problem findet, dieses schnell behoben. Außerdem ist Linux auch mit alter und Low-End-Hardware kompatibel. Beim Installieren von Linux ist eine Festplattenverschlüsselung (LUKS – *Linux Unified Key Setup*) übrigens gleich mit dabei.

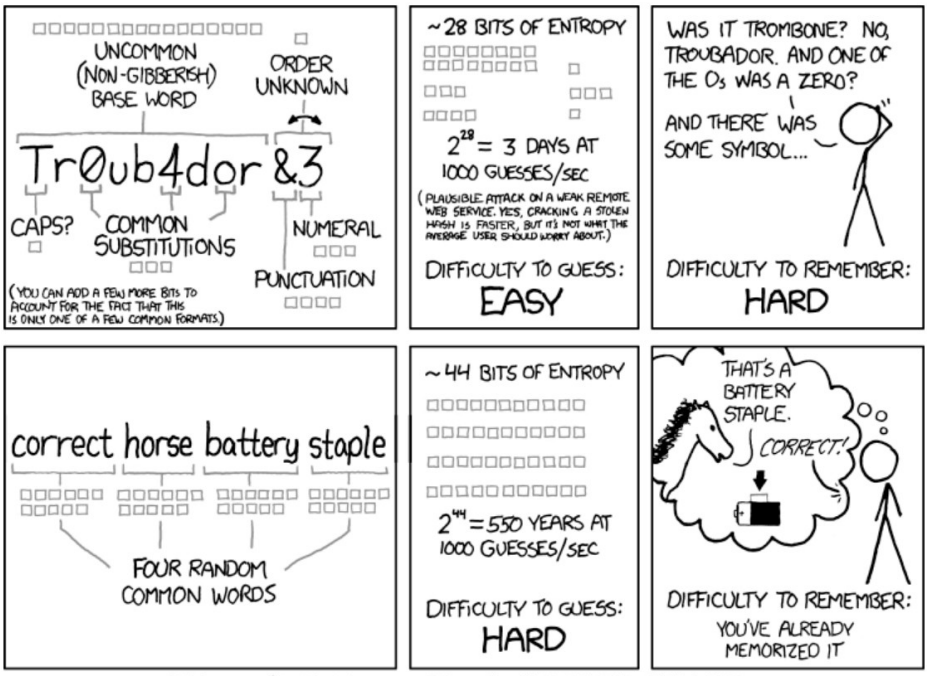
Externe Speichermedien

Auch Externe Speichermedien können verschlüsselt werden. Mit Veracrypt (FOSS) kann sowohl ein Speichermedium als auch ein bestimmter Bereich auf der internen Festplatte (=Container) verschlüsselt werden.

Passwörter

Es gibt beim Thema Passwörter einen ganzen Haufen an Tipps, wie sie noch sicherer gemacht werden können. Es hängt aber nicht nur am Passwort selbst, sondern auch der Umgang damit.

Du solltest zum Beispiel Passwörter nicht mehrfach verwenden und grundsätzlich nicht aufschreiben, sondern in einem verschlüsselten Passwort-Manager (zB KeePass) speichern. Gute Passwörter beinhalten Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Je länger ein Passwort ist, desto besser (>16 Zeichen). Einfacher merken kannst du dir Passwörter vielleicht, wenn du Passphrasen (zufällig aneinander gereihte Wörter) verwendest (Comic: xkcd.com/936).



(TOR)-BROWSER & SUCHMASCHINEN

Auch Browser – zumindest die meisten – speichern eine Menge an (Meta-)Daten und haben einiges an Sicherheitslücken (Stichwort: Browser-Fingerprinting). Deshalb sollten immer die Einstellungen durchgeschaut und (am Beispiel Firefox(die “Browser Privacy” erhöhen werden, “Do Not Track” aktivieren, keine Passwörter und nicht die History speichern lassen. Außerdem schadet es nie, die Erlaubnisse bzgl Standort, Kamera, Mikrophon, etc. durchzugehen. Auch AddOns können Browser sicherer machen: Wenn wir beim Beispiel Firefox bleiben wären empfohlene AddOns “HTTPS everywhere”, “Privacy Badger” und “uBlock Origin”.

Sollten diese Einstellungen gar nicht erst gemacht werden können, dann Finger weg vom Browser! Du kannst deinen Browser-Fingerprint selbst testen bei zB coveryourtracks.eff.org.

The Onion Routing Project (TOR-Project)

Ein besonderer Browser ist der TOR-Browser. Das Ziel des Onion-Routing war es, eine Möglichkeit zu haben, das Internet mit so viel Privatsphäre wie möglich zu nutzen, und die Idee war, den Datenverkehr über mehrere Server zu leiten und bei jedem Schritt des Weges zu verschlüsseln. Dies ist immer noch eine einfache Erklärung dafür, wie TOR heute funktioniert.

Wichtig beim TOR-Browser ist, dass du das Browser-Fenster nicht maximierst – das kann nämlich deine Identität unter Umständen verraten: Von der Bildschirmgröße kann auf das verwendete Gerät

geschlossen werden und so stehen plötzlich nur noch eine kleine Anzahl an möglichen Nutzer:innen hinterm Bildschirm.

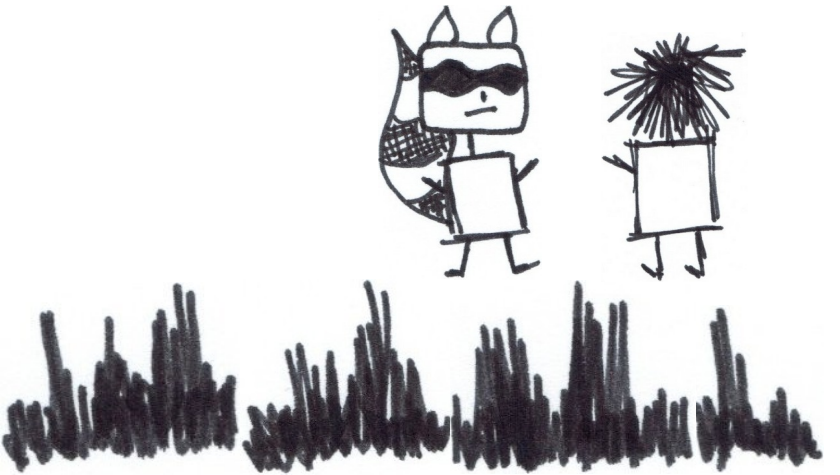
Suchmaschinen

Manche Suchmaschinen (wie zum Beispiel Google) können über deine IP-Adresse sehen, wo du bist, speichern und nutzen das zum Beispiel für die Bereitstellung der lokalen Version (Gibst du in ~~Deutschland~~ google.com ein, wirst du direkt zu google.de umgeleitet). Was Google mit Daten von Nutzer:innen noch alles anstellt, kommt später. Eine Suchmaschine, die keine Metadaten speichert, ist DuckDuckGo (Kann bei fast allen Browsern als Standard-Suchmaschine eingestellt werden).

E-Mails

E-Mails sind wie Postkarten, es kann sie praktisch jede:r lesen. E-Mails können und sollten immer verschlüsselt werden – ob für deine Privatsphäre oder ob du andere damit nicht exponieren willst. Eine recht einfache Möglichkeit, deine E-Mails zu verschlüsseln, ist mit Thunderbird. Dazu gibt's unzählige Anleitungen im Internet.

Außerdem empfiehlt es sich, eine E-Mail-Adresse bei zum Beispiel Riseup, Systemli oder Posteo zu machen und nicht bei Gmail, Hotmail, etc.



Google & co: Massenüberwachung

Gut 85 Prozent aller Smartphones und schätzungsweise 2 Milliarden Geräte weltweit laufen mit Android. Nahezu alle dieser Android-Smartphones haben **Google Services** installiert, mit deren Hilfe der Konzern massenhaft Daten wie Standortdaten, Browse- und Such-Historie, Anruf- und SMS-Protokolle, genutze Apps, etc. sammelt und dem persönlichen Google-Account zugeordnet speichert.

Die gesammelten Informationen geben tiefe Einblicke in die privatesten Themen und Vorlieben jede:r einzelnen Google-User:in - und mit diesem Wissen von unvorstellbarem Ausmaß dem Konzern eine enorme Macht. Selbst wenn die gespeicherten Informationen nicht immer direkt einem Namen zugeordnet sind, kann aus ihnen leicht ermittelt werden, welche reale Person hinter dem betreffenden Profil steckt. Die einmal erhobenen Daten können jederzeit in falsche Hände geraten und für alles mögliche verwendet werden. Auch welchen Ermittlungsbehörden Zugriff auf die erhobenen Daten gegeben werden (müssen), kann sich schnell ändern - etwa durch neue Gesetze.

Daten, die du selbst mitteilst

Jede:r, die irgendeinen Dienst von Google nutzt, stimmt dabei der Datenschutzerklärung des Konzerns zu. Das gilt also sowohl für Nutzer:innen, die ein Google-Konto anlegen, als auch für alle, die nur mal eben etwas googeln.

Dort steht, welche Daten das Unternehmen aufgrund dieser Zustimmung legal sammeln darf. Google bemüht sich darin um Verständlichkeit. Trotzdem bleibt die Erklärung an wichtigen Stellen undurchsichtig.

Google sammelt die Daten, die jede:r selbst mitteilt. Zum Beispiel die Profilinformationen, die man im eigenen Google-Konto angibt, etwa E-Mail-Adresse, Telefon- und Kreditkartennummer.

Auch alle Inhalte, die in anderen Google-Apps und Diensten eingegeben werden, landen beim Konzern: Kalendereinträge, Kontakte, E-Mails, Notizen, Sprachbefehle, eingetippte Suchanfragen und so weiter.

Daten, die Google nebenbei erfasst

Zum anderen sind da die Daten, die Google Zutun seiner Nutzer*innen ausliest. Zum Beispiel wird das verwendete Gerät, sein Betriebssystem, das Modell und die Bildschirmgröße erfasst.

Das ist grundsätzlich sinnvoll, um etwa Webseiten in der richtigen Form an das verwendete Gerät auszuliefern. Google erfasst aber auch explizit deine IP-Adresse, liest deine Telefonnummer von der SIM-Karte des Smartphones aus und speichert eindeutige Gerätekennungen. Das kann bei Smartphones zum Beispiel die IMEI-Nummer sein.

Mit der IP-Adresse lassen sich Rückschlüsse über den Aufenthaltsort ziehen, und mit der IMEI lässt sich das Gerät dauerhaft und eindeutig identifizieren. Google kann damit alle Daten, die von diesem Gerät bei dem Unternehmen landen, zusammenführen.

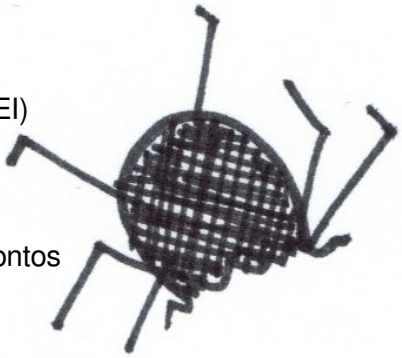
Google Play-Dienste

Die wenigstens Nutzer:innen wissen, dass es sie gibt, doch für die Verbindung zwischen Google und Android ist die App **Google Play-Dienste** das Herzstück.

Laut Studie sind die Google Play Services beim Privatsphärenschutz sogar als besonders problematisch einzustufen, da Android-Smartphones etwa alle zwanzig Minuten Verbindung mit Google-Servern aufnehmen und dabei etliche personenbezogene Daten übermitteln – und das trotz einer “datenschutzbewussten" Android-Konfiguration.

Zu den Daten zählen unter anderem:

- ➔ Telefonnummer
- ➔ SIM-Kartennummer
- ➔ eindeutige Gerätenummer (IMEI)
- ➔ WLAN-MAC-Adresse
- ➔ Android-ID
- ➔ E-Mail-Adresse des Google-Kontos
- ➔ IP-Adresse



Wer möchte, dass das eigene Gerät ganz aufhört, Informationen an Google weiterzugeben, die muss sich von den Google Play-Diensten und von allen anderen Google-Apps trennen. Das bedeutet in der Praxis, ein neues Betriebssystem zu installieren, das ganz ohne Google auskommt. Eine beliebte Variante ist zum Beispiel das alternative Betriebssystem **LineageOS**.

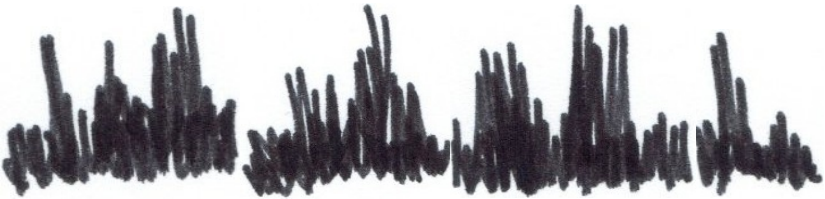
Glücklicherweise lässt sich mittlerweile ein google-freies Android-Smartphone einrichten, das sehr gut nutzbar ist, die wichtigsten Funktionen besitzt, regelmäßig mit Updates versorgt wird und ganz ohne die Google-Services auskommt. Daher der Appell: Probier es aus! Mach deine und die Kommunikation deiner Kontakte ein wenig sicherer und entzieh sie der Massenüberwachung durch Google und Co.

Smartphones - Alternatives Betriebssystem

Für ein google-freies Smartphone muss das gesamte Betriebssystem neu installiert werden. Die sogenannten G-Apps, welche die Google Services beinhalten, sind so tief in das System installiert, dass sie nicht einfach gelöscht werden können. Smartphone-Hersteller:innen liefern ihre Geräte fast immer mit einer Android-Version (der sogenannten “Stock ROM”) aus, bei der die G-Apps bereits installiert sind.

Es ist möglich, auf den allermeisten Android-Smartphones eine andere Android Variante (sogenannte “Custom ROM”) zu installieren. Dieser Vorgang überschreibt die aktuelle Android-Version.

Eine Empfehlung ist **LineageOS**, ein freier Nachbau von Android mit eigenen Sicherheits- und Privatsphäre-Erweiterungen. LineageOS wird durch ein großes Team von Entwickler:innen betreut und es werden regelmäßig Updates veröffentlicht – weshalb bekannte Sicherheitslücken schnell geschlossen werden. Außerdem legt das Community-Projekt großen Wert auf Transparenz, die Entwicklung passiert öffentlich



nachvollziehbar und es gibt kein Unternehmen mit kommerziellem Interesse im Hintergrund.

Da Smartphones unterschiedliche Hardware verwenden, gibt es leider keine Android-Variante, die für alle Smartphones verfügbar ist. Es muss also geschaut werden, ob LineageOS das eigene Smartphone unterstützt. Am besten wählst du das Smartphone direkt danach aus.

Smartphones - Verschlüsseln

Smartphones sind mittlerweile fast alle standarmäßig verschlüsselt (seit Android 6 bzw iOS 8), trotzdem schadet es nie, das zur Sicherheit nochmal in den Einstellungen nachzuschauen (auch eine gute Gelegenheit, wieder mal ein Software-Update zu machen!).

Auch wenn das Smartphone verschlüsselt ist, muss es das Back-Up nicht zwangsläufig sein. So ist es zum Beispiel bei iPhones, wo du dein Back-Up in der Cloud manuell verschlüsseln musst.

Auch wenn du dein Smartphone dann verschlüsselt hast, ist das noch lange keine Garantie dafür, dass keine andere Person Zugriff darauf kriegt. Die Praxis zeigt uns immer wieder, dass bei den Optionen “Fingerprint” und “Face-ID” Menschen von zum Beispiel der Staatsgewalt dazu gezwungen werden, das eigene Smartphone zu entschlüsseln (auch unter Anwendung von physischer Gewalt). Deshalb empfehlen wir, immer ein Passwort für die Verschlüsselung zu verwenden.

Vergiss übrigens nicht, deine externe SD-Karte zu verschlüsseln!

Smartphones - Messenger

Mit Messenger-Apps lassen sich Textnachrichten, Bilder, Videos und Dateianhänge über das Internet verschicken. Inzwischen gehören auch Gruppenchats und Internet-Telefonie zu den Standard-Funktionen. Messenger unterscheiden sich damit von der SMS-Funktion, bei der Text- oder Bildnachrichten über das Mobilfunknetz geschickt werden (falls du das Mobilfunknetz bevorzugst, empfehlen wir die App **Silence**).

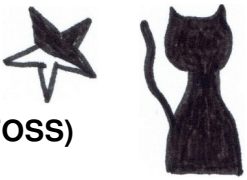
Lange Zeit verschickten Messenger-Apps Nachrichten weitgehend ungesichert über das Internet. Dritte konnten sehr einfach mitlesen. Erst seit den Enthüllungen des US-amerikanischen Whistleblowers Edward Snowden begannen die Anbieter nach und nach, Verschlüsselungsverfahren einzuführen.

Jede:r stellt individuelle Anforderungen an einen Messenger. Der einen Nutzer:in ist es wichtig, möglichst viele Leute zu erreichen, während eine andere gerne Nachrichten innerhalb einer Gruppe austauscht. Eine andere wiederum legt Wert auf eine verschlüsselte Kommunikation oder eine möglichst einfache Bedienung. Letztendlich muss jede:r selbst entscheiden, welcher Messenger die eigenen Bedürfnisse am ehesten erfüllt – eine universelle Lösung wird und kann es nie geben. Von dieser Wunschvorstellung sollten wir uns befreien und das Thema Messenger losgelöst von Emotionen betrachten.

Da es in dieser Broschüre aber explizit um die Sicherheit in der Kommunikation geht, widmen wir uns im Folgenden auch dieser. Zur Gewährleistung einer “abhörsicheren” Kommunikation setzen Messenger auf unterschiedliche Verschlüsselungstechniken. Beliebt und

sinnvoll ist der Nachrichtenaustausch via Ende-zu-Ende-Verschlüsselung (E2EE). Theoretisch verhindert diese Technik das Abhören der Nachrichten durch andere Parteien und nur die jeweiligen Kommunikationspartner:innen können Nachrichten entschlüsseln.

Selbst eine perfekte E2EE ist allerdings nur so sicher wie das jeweilige Endgerät, auf dem die Nachrichten gespeichert werden. Das Prinzip der E2EE betrachtet nämlich nicht die Risiken der Endpunkte der Kommunikation, nachdem die Nachrichten entschlüsselt wurden. Das bedeutet: E2EE schützt im Idealfall vor dem Abhören der Nachrichten auf dem Transportweg, allerdings bietet sie keinen Schutz vor lokalen Angriffen. Wir sollten uns daher stets vor Augen führen, dass die E2EE lediglich ein kleines Puzzelteil darstellt, wenn das Schutzziel der Vertraulichkeit eingehalten werden soll.



Signal: Krypto-Pionier aus den USA (FOSS)

Das Ende-zu-Ende-Verschlüsselungsprotokoll von Signal gilt als Goldstandard in der Kryptoszene und wurde auch von WhatsApp und dem Facebook-Messenger übernommen. Seit 2017 steht die App auch als Direkt-Download als .apk-Datei auf der Webseite zur Verfügung.

2020 führte Signal eine PIN ein, die bei Neuinstallation der App das Importieren der eigenen Profileinstellungen ermöglicht. Solltest du keinen Zugriff mehr auf deine Nummer haben, mit der du das Signal-Profil erstellt hast, kannst du dich so trotzdem authentifizieren. Chat-Inhalte sind mit der PIN nicht abrufbar, da die Nachrichten nur lokal gespeichert werden.

Deshalb hier nochmal kurz zusammengefasst, welche Einstellungen du überprüfen solltest:

- ➔ Screen Lock aktivieren
- ➔ Screen Lock inactivity timeout aktivieren
- ➔ Screen Security aktivieren
- ➔ Signal Pin machen (inklusive Registration Lock)

Telegram: Russische Alternative

Der populäre russische Messenger Telegram setzt ganz auf gute Nutzbarkeit. Doch Vorsicht: Chats sind standardmäßig nicht Ende-zu-Ende verschlüsselt. Auch ist der Umgang mit Metadaten nicht ganz transparent. Wegen rigider russischer Gesetze sitzt die Anbieter:in nun in Dubai.

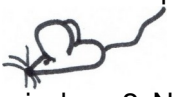
Der Quelltext des Telegram-Clients ist **quelloffen** (Lizenz GNU GPL) und damit für jeden einsehbar. Eine unabhängige Überprüfung der Sicherheit ist allerdings lediglich eingeschränkt möglich, da die serverseitige Infrastruktur proprietär ist.

Die Stärke von Telegram liegt in Push-Nachrichten. Wer heute ein gut laufendes Geschäft mit Verschwörungsideologien oder einfach nur den nächsten Hasskanal aufbauen möchte, kommt derzeit an Telegram nicht vorbei. Das ist etwas überspitzt gesagt, weil Telegram auch für andere Zwecke gerne genutzt wird, unter anderem wegen der praktischen Gruppenfunktionalitäten.

Die App ist standardmäßig transportverschlüsselt. Das heißt, die App verschlüsselt die Chats vom Mobilgerät zum Server und speichert sie in

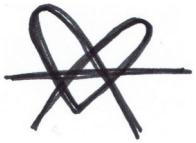
der Cloud der Anbieter:in. Vorteil: Du kannst von verschiedenen Geräten auf alle Ihre Chats zugreifen, ohne ein Backup anlegen zu müssen. Nachteil: Telegram selbst könnte theoretisch deine Nachrichten lesen und an Behörden weitergeben.

Wie Telegram mit den Informationen umgeht, wer wann mit wem kommuniziert, ist nicht bekannt. Auch zur Speicherung von Standortdaten sagt Telegram nichts.



Obwohl Telegram zumindest für Chats zwischen 2 Nutzer:innen eine E2EE integriert hat, ist diese standardmäßig **nicht** aktiv. Die Chats werden lediglich zwischen dem Endgerät und dem Server verschlüsselt. Nach Angaben der Betreiber:in sind die Chats zusätzlich auf den Servern verschlüsselt gespeichert. Für die Betreiber:in selbst sind die Daten jedoch einsehbar – das gilt ebenfalls für eine:n Angreifer:in, die sich Zugang zum System verschafft.

Wichtig: Laut Exodus beinhaltet die Google-Play-Version von Telegram zwei Tracking-Dienste (Google Firebase Analytics, HockeyApp). Gerade in einem Kontext, in dem womöglich sensible Inhalte ausgetauscht werden, sind Tracker:innen völlig fehl am Platz. Die F-Droid-Version ist übrigens frei von Tracker:innen.



Threema: Schweizer App für kleines Geld

Der Messenger der Schweizer Threema GmbH existiert seit 2012 und ist bei Bedarf anonym nutzbar. Obwohl nicht quelloffen (Open Source) genießt er einen hervorragenden Ruf. Die App kostet einmalig vier Euro und ist für Android und iOS verfügbar.

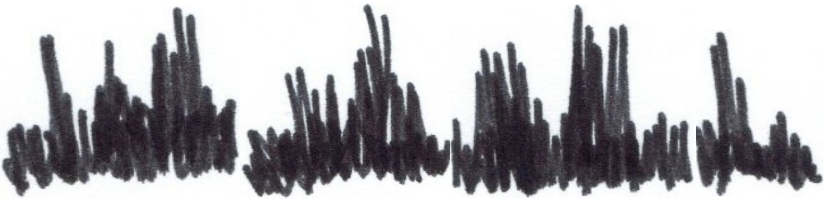
Die App-Server befinden sich nach Angaben des Unternehmens ausschließlich in der Schweiz. Threema ist besonders sparsam, was das Sammeln von Metadaten betrifft. Zur Identifizierung ihrer Nutzer:innen erstellt die App beim ersten Start eine ID. Die App erfordert weder eine Telefonnummer noch den Zugriff auf das Adressbuch.

WhatsApp: Marktführer von Facebook

Mehr als eine Milliarde Menschen nutzen WhatsApp weltweit. Nachrichten sind mit dem Signal-Protokoll End-zu-End verschlüsselt. Kritikpunkt: WhatsApp sammelt viele Metadaten und teilt Nutzer:innendaten mit Facebook - darunter auch die eigene Telefonnummer. Aber nicht nur das, Whatsapp lädt auch dein komplettes Telefonbuch auf Facebook-Server hoch.

WhatsApp-Backups auf Google Drive, iCloud und lokal auf dem Gerät sind zwar ebenfalls verschlüsselt, aber nicht Ende-zu-Ende. Es gibt den begründeten Verdacht, dass die Schlüssel zu diesen Backups auf den Servern von WhatsApp liegen. Das würde bedeuten, dass der Dienst die gesicherten Inhalte einsehen kann.

Die aufschlussreiche und ständig aktualisierte **Messenger-Matrix** findest du im Forum vom Kuketz-Blog.



Smartphones - Ortung von Personen

Dein Handy ist ständig im Kontakt mit Mobilfunkmasten, damit du jederzeit Nachrichten (SMS) versenden und bekommen oder Anrufe tätigen kannst. Diese Aktivität mit den Mobilfunkmasten wird von deiner Mobilfunkanbieter:in überwacht und protokolliert. Somit kann nochvollzogen werden wo du bist und wo du warst. Wo du die Nacht verbringst ("=wo du wohnst"), wo du den Tag verbringst ("=wo du hackelst") und was für regelmäßige Termine (Sport, Therapie, etc) hast.

Benutzt du "Mobile Daten" ohne VPN oder TOR wird außerdem jeder Website, die du besuchst, und deren Tracker:innen deine IP-Adresse mitgeteilt (was auch deinen Standort verrät).

Diese ("anonymisiten") Daten werden von diversen Mobilfunkanbieter:innen immer wieder (freiwillig) dem Staat bzw. der Staatsgewalt zur Verfügung gestellt. Auch wenn die Daten anonymisiert sind, ist es nicht unmöglich, rauszufinden, wer hinter einem Profil steckt.

Dein Smartphone ist außerdem ein GPS-Gerät. Wenn deine Standortdaten eingeschalten sind, kommuniziert der GPS-Chip in deinem Smartphone mit den GPS-Satelliten. Unter welchen Bedingungen wer auf diese Daten legal Zugriff hat, ist sehr unterschiedlich und kann recherchiert werden.

Seit einiger Zeit ist es auch möglich, mit dem Smartphone an der Supermarkt-Kasse zu zahlen. Das funktioniert grundsätzlich über den NFC-Chip in deinem Handy. Dann brauchst du noch Google Pay oder Apple Pay und schon gibst du Preis, wann du was und wo einkaufst.

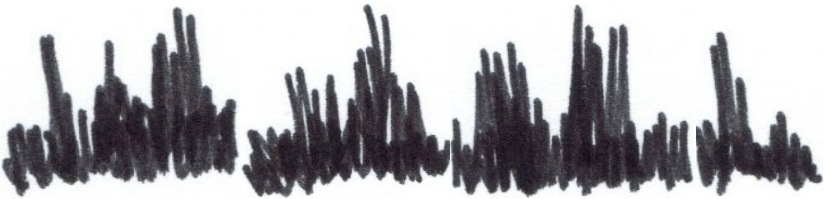
Oft vergessen werden auch Bluetooth und WLAN. Auch wenn du nicht verbunden bist, kann mit eingeschaltetem Bluetooth oder WLAN ein Bewegungsprofil von dir erstellt werden – weil dein Smartphone ständig auf der Suche ist, sich irgendwo einloggen zu können. Besonders problematisch ist das, wenn die Staatsgewalt schon Zugriff auf dein Smartphone hat.

Smartphones – "Kill Your Phone"

Auch wenn dein Handy aus ist, kannst du trotzdem "Silent SMS" empfangen. Selbst wenn du den Akku rausnehmen kannst, ist meist eine weitere Batterie im Handy eingebaut, die genügend Energie liefert, um die "Silent SMS" zu beantworten und so deinen Standort zu verraten.

Eine Möglichkeit, dein Smartphone vom Netz abzuschirmen und damit nicht mehr ortbar zu sein, bieten Handytaschen – selbstgemacht aus einem speziellen metallisiertes Polyestergewebe, das für den Schutz vor elektromagnetischer Strahlung entwickelt wurde. Als geschlossene Tasche bildet der Stoff einen Faraday'schen Käfig, der die elektromagnetische Strahlung des Mobilfunknetzes abschirmt (killyourphone.com). Dein Smartphone kommiuniziert dann nicht mehr mit Handymasten oder Satelliten und auch WLAN und Bluetooth funktionieren nicht mehr.

Wenn du also dein Handy irgendwohin mitnehmen willst/musst, temporär aber nicht nachverfolgbar sein soll, wo du bist, ist das eine Option.

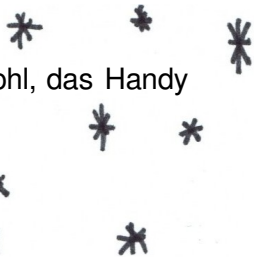


Der Nachteil davon ist aber nicht nur, dass dein Handy erfahrungsgemäß überhitzen wird, sondern auch, dass das eingebaute Mikrophon weiterhin aufzeichnen könnte.

Der Einsatz von solchen Handytaschen sollte aber ohnehin auch gut überlegt sein. Wenn zum Beispiel von mehreren Personen gleichzeitig am gleichen Ort das Handysignal verschwindet, war das in der Vergangenheit auch schon verdächtig genug für die Staatsgewalt.

Eine andere Option für Plena ist eine Handy-Disco. Alle Handys werden in eine schalldichte Box gelegt und von drinnen mit Musik beschallt.

Die Methode mit dem ausgeschaltetem Kühlschrank ist etwas bekannter, aber dafür auch unsicherer – kommt es doch stark auf das Gerät an. In der Theorie wirkt ein Kühlschrank nämlich – wie die Handytaschen – wie ein Faraday'scher Käfig. Außerdem sind Kühlschränke in der Regel stark gedämmt, wodurch verhindert werden kann, dass das im Handy eingebaute Mikrofon das Gespräch im Raum aufzeichnet.



Am sichersten für dich und deine Kontakte ist es aber wohl, das Handy für Plena, Aktionen und Demos daheim zu lassen.

Checklist Programme

Im Kuketz-Blog (und auch auf anderen Seiten) findest du in der **Empfehlungsecke** jede Menge nützliche Infos rund um die empfohlenen Programme. Deshalb hier nur kurz:

Passwortmanager

Hier empfiehlt sich KeePass2 für deinen Computer bzw. KeePassDroid für Android oder MiniKeePass für iOS.

Messaging

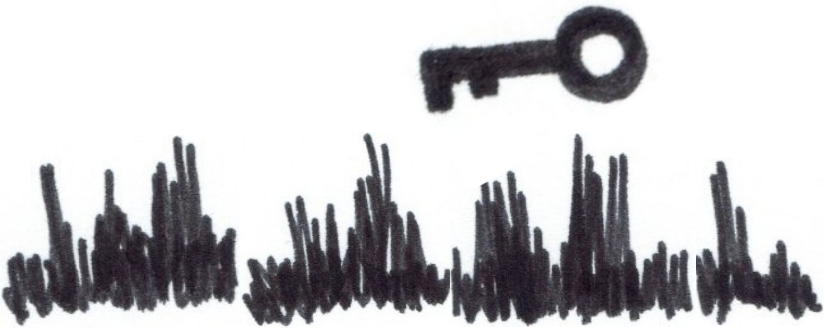
Signal Desktop kann nur empfohlen werden, wenn der Computer, auf dem es benutzt wird, verschlüsselt ist. Für dein Smartphone empfehlen wir Signal.

Browser

Ein Browser, in dem viele Sicherheitseinstellungen möglich sind, ist Firefox (mit AddOns und eventuell RiseUp-VPN). Für surfen ohne dass du dich mit einem deiner Konten anmeldest empfiehlt sich TOR. Beim Handy empfehlen wir Fennec, Orbot und Tor Browser.

Verschlüsselung

Bei Linux ist LUKS schon vorinstalliert, für Container immer Veracrypt.

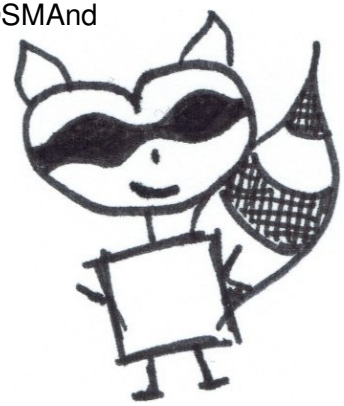


Terminfindung

Für die Terminfindung in der Gruppe empfehlen wir das verschlüsselte Croodle von den Genoss:innen von systemli.org.

Google-Alternativen

Google Suche	→	MetaGer
Google Hangouts	→	Jitsi (über vertrauenswürdigen Server), Signal
Gmail	→	riseup, systemli, posteo
Google Docs	→	(Ether)Pad von riseup, systemli, ccc
Google Sheets	→	EtherCalc von systemli, ccc
Youtube	→	PeerTube
Google Maps	→	OpenStreetMap, OSMAnd
Google Play Store	→	F-Droid
Google Drive	→	Nextcloud
Google Translate	→	DeepL



Veranstaltungen

Veranstaltungen könnten auf zeit.diebin.at, gegendielangeweile.net oder anderen Kalendern eingetragen werden, statt dass wir immer wieder auf Facebook zurückgreifen.

Quellen

Zusammengeklaut, dazugedichtet, gekürzt von:

- ➔ datadetoxkit.org
- ➔ digitalcourage.org
- ➔ exposingtheinvisible.org
- ➔ killyourphone.com
- ➔ kuketz-blog.de
- ➔ mobilsicher.de
- ➔ myshadow.org
- ➔ netzpolitik.org
- ➔ riseup.net
- ➔ systemli.org
- ➔ tacticaltech.org
- ➔ techboys.de
- ➔ torproject.org

Solltest du mehr Infos zu den Themen suchen, schau am besten zuerst bei den oben genannten Seiten vorbei :)