Tipps für Informationssicherheit insbesondere für Mobile Geräte mit Hinweisen zum Datenschutz

Informationssicherheit: Technische und organisatorische Maßnahmen zu Gewährleistung von

- *Geheimhaltung* der Informationen/Daten (Dritte können keine Kenntnis von den Daten nehmen)
- *Erreichbarkeit* der Informationen/Daten (wie kann ich sicherstellen an meine Daten zu kommen)
- *Manipulationsvermeidung* Informationen/Daten (wie verhindere ich die unbefugte Manipulation meiner gespeicherten Daten und der Daten die ich versende, bspw. durch jemanden der sich bei mir „einklinkt")
- *Authentizität* besonders in der Kommunikation von Personen, d.h. es kommunizieren wirklich die Personen miteinander, die vorgeben es zu sein

Datenschutz: Schutz im Umgang / Verwendung von personenbezogenen Daten

Dieses Informationspapier will kurze und knappe Informationen liefern, wie Ihr für Euch selbst und andere mehr Sicherheit mit Daten erreichen könnt. Das umfasst Hintergründe, Werkzeuge und weiterführende Informationen für diejenigen die mehr wissen wollen. Auf eine detaillierte Beschreibung der Bedienung/ Einstellung relevanter Software/Apps wird weitgehend verzichtet. Die Einstellung sind vielfach selbsterklärend, konkrete Auswirkungen weitgehend transparent. Teilweise gibt es Links mit weitergehenden Erläuterungen. Wo diese vermisst werden, ist das dem Umfang dieser Ausführungen geschuldet.

1 Einführung und Grundsätze

Sicherheit ist immer ein Kompromiss. Maximale Sicherheit ist am Ende weniger Sicherheit, weil sie dann wegen des Aufwands zumeist nicht annähernd beachtet wird. Es muss also darum gehen eine angemessene Sicherheit zu gewährleisten, d.h. unter Beachtung des Risikos. Niemals jedoch darf das zu der Einstellung führen, wo man scheinbar nichts zu verbergen hat, braucht es auch keinen Schutz. Jede Information kann interessant sein und sei es in Kombination mit weiteren Daten oder im Hinblick darauf, dass Angreifer ihre Mittel effizienter einsetzen können, nämlich nur auf geschützte Informationen von Euch oder anderen. Informationssicherheit zu brechen ist regelmäßig auch eine Frage der Priorisierung und Kapazität (Rechenleistung, Personal). Zum Datenschutz ein paar beliebige Beispiele für „Verschwörungstheoretiker": https://www.privacy-handbuch.de/handbuch_16b.htm ; https://www.privacy-handbuch.de/handbuch_16.htm

Software / Apps im Zusammenhang mit Kommunikation und Datenspeicherung sollten wo immer möglich „Open Source", also quelloffen sein. Nur so lässt sich zuverlässig überprüfen, ob und inwieweit eine Software / App sicher ist. Und wenn ein Kommunikationsdienst etwa per Gerichtsbeschluss oder Gesetz verpflichtet wird Informationen herauszugeben, dann kann einem das völlig egal sein, soweit der Dienst diese Informationen nicht oder nur verschlüsselt hat („protected by strict Swiss privacy laws", „Deutscher Serverstandort" usw. ist Augenwischerei und das was suggeriert wird entspricht oft genug auch gar nicht der Rechtslage). Ob bspw. eine App „Open Source" ist, muss man recherieren bzw. findet hier Hinweise zu den empfohlenen Apps.

Da mobile Geräte (Smartphone/Tablet) heute überwiegend genutzt werden, kommt immer wieder die Frage auf, ob unter Sicherheitsaspekten Android oder Apple iOS bevorzugt werden soll. Apple bietet aufgrund seiner Einschränkungen und des geschlossenen Kosmos relativ viel Sicherheit auch für diejenigen, die sich wenig Gedanken um Sicherheit machen. Die Einschränkungen ermöglichen jedoch auch keine Eingriffe zum Guten. Die Nutzung von Apple ist mehr als bei anderen Anbietern eine Frage des Vertrauens. Vermutlich wird Apple jedoch für den durchschnittlichen Dissidenten sicher sein.

Wer sich mit Informationssicherheit und Datenschutz beschäftigt fährt aber nicht zuletzt im Hinblick auf das Preis-/Leistungsverhältnis zweifellos mit Android besser. Eine andere Frage ist, ob man Google von seinem Handy verbannt (Kurzfassung über Verzicht auf Google Konto: https://www.techbook.de/mobile/android/android-ohne-google-konto; wer trotzdem Apps braucht, die nur im Playstore von Google sind, nutzt dazu die App *Aurora Store* (der bezieht die Apps über Google Play, nehmt bitte sein Konto, nicht Eures, was möglich wäre) https://f-droid.org/de/packages/com.aurora.store/ Sofern Ihr auch alle Google Apps, insbesondere Google Play Dienste deaktiviert habt, besteht die Gefahr, dass einzelne Apps, bspw. die Ihr über den Aurora Store bezogen habt, Google Play Dienste haben wollen; vielfach funktionieren sie dennoch ausreichend ohne.)

Im Verlauf dieser Ausführung wird mehrfach auf einen alternativen Android-Appstore hingewiesen. Es handelt sich dabei um F-Droid https://www.f-droid.org/de/. Dieser Appstore beinhaltet kostenlose, freie Open Source Apps und ist absolut zuverlässig. Wer diesen Store bspw. über den Browser installiert hat, kann die Apps anschließend wie im Playstore suchen. Hier werden nur Apps angesprochen, die kein Rooten des Smartphones erforderlich machen. Wichtiger Hinweis: nach Installation des F-Droid Store entzieht bitte Eurem Browser unbedingt wieder die Berechtigung zur Installation von Software. Nicht alle Open Source Apps sind bei F-Droid verfügbar, wenn diese nämlich nicht frei sind und andere Komponenten enthalten (bspw. derzeit Signal) oder es wird eine spezielle Version angeboten, ohne unzulässige Komponenten (bspw. eine spezielle Version von Telegram oder Fennec, ein Firefox-Browser ohne Pocket). Ihr könnt schauen, ob es eine bei F-Droid verfügbare App auch im Playstore gibt, jedoch muss im Einzelfall geklärt werden, inwieweit die Playstore App mit der Version bei F-Droid identisch ist. So ist etwa die App Blokada, die dem Geschäftsmodell von Google zuwiderläuft, lediglich in abgespeckter Version verfügbar.

2 Basis Sicherheitsaspekte

2.1 Passwörter

Die Sicherheit eines Passworts hängt ab von

- Länge
- Komplexität (Groß-, Kleinbuchstaben, Zahlen, Sonderzeichen)
- Zufälligkeit

Darüber hinaus spielt es eine Rolle, ob beliebig viele Versuche ein Passwort einzugeben möglich sind oder der Zugang nach einer bestimmten Anzahl von Versuchen dauerhaft oder zeitweilig gesperrt wird oder sogar eine Löschung des Speichers erfolgt. Auch die Zugangsmöglichkeit spielt eine Rolle.

Es gibt heute Software die das Knacken von Passwörtern deutlich erleichtert. Diese Software verfügt u.a. über häufig genutzte Passwörter, Standardpasswörter von Geräten (bspw. WLAN-Router), generelle Wörterbuchattacken und kann um potentielle Vorlieben einer Zielperson ergänzt werden. Wichtig ist dabei zu wissen, eine solche Software beherrscht auch den Umgang mit Permutationen und Ersetzungen aller Art, also bevorzugte Codes/Zeichenfolgen/Geburtsdaten usw. werden in ihrer Reihenfolge getauscht und anderweitig kombiniert oder ersetzt (Bsp: aus Eselsbrücke Alles für Deutschland! 88 20.4. wird Passwort: all20.E$4land!DeutschBB und das kann mit dem nötigen Willen auch bei 23 Zeichen inkl. Sonderzeichen relativ schnell gefunden werden, bei einer entsprechenden Zielperson und nicht sonderlich limitierten Eingabeversuchen). Ein knapper Hinweis zu Quantencomputern. Unabhämgig von der Verfügbarkeit von Quantencomputern – wer ein zufälliges, komplexes Passwort (Passwortmanager, Passwortgenerator) von 30 Zeichen hat, muss sich über Quantencomputer zum Brechen des Passworts für den Rest seines Lebens keine Gedanken machen!

Empfehlungsbeispiele:

- für Smartphones: mindestens 8, besser 10 Zeichen mit Groß-, Kleinbuchstaben, Zahlen, Sonderzeichen
- PC (Annahme langfristige und besonders wichtige Daten) mindestens 10 Zeichen (Groß-, Kleinbuchstaben, Zahlen, Sonderzeichen) für die Festplattenverschlüsselung (siehe auch Zugriffschutz)
- WLAN (unbedingt Standardpasswörter ändern, teilweise sogar auf der Geräteunterseite angegeben
    - WLAN Router/Accesspoint Einrichtungspasswort mindestens 20 Zeichen (solche Router sind oft von außerhalb zugänglich und haben oft keine Eingabewiederholungsbeschränkung)
    - WLAN Passwort mindestens 20 Zeichen
- Für Speichermedien, E-Mail-Accounts, Internet-Accounts oder gesonderte App-Passwörter je nach Risiko und ggf. der zusätzlichen Verwendung eines sogenannten 2. Faktors, sofern das möglich ist.
- Passwortmanager: verwendet einen Passwortmanager auf der Basis von Keepass. Keepass ist für praktisch alle Systeme verfügbar und die Datenbanken können zwischen PC und Handy

getauscht und geöffnet werden, auch wenn die Keepass Programme nicht aus einer Hand kommen (erforderlich sind Passwortdatenbanken mit der Endung „.kdbx“)

  - Homepage des eigentlichen Keepass Projekts mit weiterführenden Links: https://keepass.info (englisch)
  - Empfehlenswert
    - für Android die Variante *KeePassDX* https://f-droid.org/de/packages/com.kunzisoft.keepass.libre/
    - für Windows/Linux/Mac die Variante *KeePassXC* https://keepassxc.org/download/
    - für Apple iOS *AuthPass*

- Passwort Manager sollten immer Open Source sein. Der cloudbasierte Open Source Passwort Manager Bitwarden (auch kostenlos für praktisch alle Plattformen verfügbar) https://bitwarden.com / https://bitwarden.com/download/ kann in Betracht gezogen werden. Dabei sollte unbedingt die 2. Faktor Authentifizierung aktiviert werden, die auch in der kostenlosen Variante mittels TOTP (Time-Based One-Time Password) genutzt werden kann (Erläuterung zu TOTP hier https://itsecblog.de/2fa-zwei-faktor-authentifizierung-mit-totp/).
- Tastatur: Tastaturen sind teilweise kritisch, können auch Passwörter lesen und verarbeiten diese im Rahmen von Rechtschreibkontrolle und Vorhersagen und einige haben Verbindung zum Internet. Schaut daher bitte auch in die Einstellungen Eurer Tastaturen, deaktiviert Funktionen oder die ganze Tastatur. Deshalb sind gerade viele Komforttastaturen für kritische Eingaben ein No-Go, weil die Art der Verwendung dieser Daten reine Vertrauenssache ist. Rechtschreibkontrollen sind kein Problem, wenn Wörterbücher lokal sind und individuelle Wörter nur im Ausnahmefall gepflegt werden.
  - Sichere Tastaturen: die Android Orignal Tastatur (das ist nicht die Google Tastatur Gboard)
  - Empfehlung: Simple Keyboard (Android) https://f-droid.org/de/packages/rkr.simplekeyboard.inputmethod/
  - Weitere Informationen z.B. hier https://mobilsicher.de/ratgeber/tastatur-app-ersetzen
  - Beachtet bitte im Zusammenhang mit der Passwort Eingabe aus einem Passwortmanager das Thema AutoType / Autofill. Hintergrund ist, dass kopierte Passwörter und Benutzername usw. in einem Speicher sind, auf den alle möglichen Apps zugreifen können, auch bösartige, die ansonsten aufgrund des Sicherheitskonzepts von Android (Sandkastenprinzip) sich womöglich nicht zu schädlich auswirken könnten. Im Ergebnis, beim Thema Tastatur, nutzt bei *KeePassDX* idealerweise für die Passworteingabe die mitgelieferte Tastatur (Magikeyboard). Neue Tastaturen müssen in den Einstellungen aktiviert werden. Ein Wechsel kann durch langes Drücken auf die Leertaste angestoßen werden. Vertiefung des Themas https://www.kuketz-blog.de/keepassdx-magikeyboard-und-autofill-im-android-alltag-nutzen-passwoerter-teil2/

2.2 Zugriffschutz

2.2.1 Geräte

2.2.1.1 **PC Windows**: wichtig ist es die Festplatte zu verschlüsseln. Die Entschlüsselung erfolgt also bevor Windows überhaupt starten kann. Das sog. Windows Passwort ist nicht so entscheidend und kann je nach (zurückliegender) Windowsversion auch vergleichsweise einfach ausgehebelt werden. Für die Verschlüsselung der Festplatte nutzt bitte VeraCrypt https://www.veracrypt.fr/en/Home.html Eine Einrichtungsanleitung findet Ihr hier https://de.phhsnews.com/how-to-encrypt-your-windows-system-drive-with-veracrypt3639 Von Bitlocker, der Windowsverschlüsselung ab der Windows Pro-Variante ist abzuraten, da es sich nicht um offene Software handelt und Microsoft in der Vergangenheit bereits mit Behörden zusammengearbeitet hat.

2.2.1.2 **PC Linux** sollte ebenfalls eine Festplattenverschlüsselung haben. Hier sollte die Linux eigene LUKS (Linux Unified Key Setup) Verschlüsselung genutzt werden. Empfehlenswert und einfach wie Windows zu bedienen sind die LINUX Distributionen Ubuntu (https://ubuntu.com/download/desktop) oder Mint (eine noch mehr an Windowsnutzer gerichtete Anpassung von Ubuntu) (https://linuxmint.com/download.php). Im Installations- bzw. Einrichtungsdialog kann die Verschlüsselung einfach umgesetzt werden und ist selbsterklärend**.** An der entsprechenden Stelle die sogenannte Partitionierung im LVM Modus auswählen und das komplette System über Auswahl verschlüsseln (hier die etwas zu komplizierte Beschreibung im Ubuntu Wiki https://wiki.ubuntuusers.de/System_verschlüsseln/ ; man braucht sie nicht)

2.2.1.3 **Smartphone / Tablet**

2.2.1.3.1 **Android**: ist ab Android 6 verpflichtend verschlüsselt (es gibt wenige Ausnahmen u.a. bei FireOS, dem Amazon Android; einige Hersteller, z.B. LG, Huawei inkl. Submarken sind verschlüsselt, obwohl es den Standard-Hinweis in den Einstellungen / Verschlüsselung und Anmeldedaten nicht gibt. Der Zugang beim Systemstart kann über ein Muster, Pin oder Passwort gesichert werden. Hier unbedingt ein Passwort (Groß-, Kleinbuchstaben, Zahlen, Sonderzeichen) wählen mit nicht weniger als 8 Zeichen (16 sind möglich).

- Je nach Android Implementierung durch die Hersteller erzwingt das Gerät nach einigen Fehleingaben eine kurze Eingabepause, einige Hersteller begrenzen die Falscheingabe absolut (bspw. auf 30 Versuche). Mit der App *Locker* https://www.f-droid.org/de/packages/net.zygotelabs.locker/ (nicht zu verwechseln mit der App *AppLocker -> dazu unten)*) kann das Verhalten selbst gesteuert werden, wobei man die Wahl hat die verbleibenden Versuche anzuzeigen oder nicht. Eine solche App kann besonders sinnvoll sein, wenn man ein Passwort von lediglich 8 Zeichen hat, welches nicht völlig zufällig ist. Die App löscht das Gerät bei Überschreiten der zulässigen Eingabeversuche.
- Nach dem Systemstart kann eine erneute Sperre auf bis zu 30 Min. verzögert werden. Aus Sicherheitsgründen empfiehlt sich eine deutlich kürzere Zeit einzustellen, in jedem Fall ist einzurichten, dass die Systemsperre durch Antippen des An-/Ausschalters sofort aktiviert wird
- Nach dem Systemstart kann bei entsprechender Einrichtung für i.d.R. 72 Std. auch eine biometrische Entsperrung erfolgen. Eine biometrische Einrichtung birgt Risiken. Das gilt in erster Linie, wenn die Möglichkeit besteht Euren echten Finger oder Euer Gesicht zu nutzen (Festnahme/Überfall). Ggf. kann dieses Risiko durch die App *Admin Control* https://f-droid.org/de/packages/com.davidshewitt.admincontrol/ mitigiert werden. Mit der App kann per „Knopfdruck“ die biometrische Entsperrung deaktiviert und wieder aktiviert (in dem Fall Passworteingabe vor Knopfdruck) werden, bspw. vor einer Demo, in der Nacht usw.. Einige Geräte bieten auch die Entsperrung per Bluetooth-Gerät. Hier kann also organisatorisch die Nutzung begrenzt werden. Der Einsatz sollte allerdings sehr gut durchdacht sein, zumal Bluetooth immer wieder durch Sicherheitslücken auffällt – hier konkret das Entsperrgerät zu simulieren – weshalb Bluetooth nur punktuell genutzt werden sollte (beachte dazu Automatisierung über die App Greentooth https://www.f-droid.org/de/packages/com.smilla.greentooth/)
- Interessierte können sich mit diesen Apps beschäftigen, die das Gerät in Abhängigkeit von der Bewegung sperren: *PrivateLock* https://www.f-droid.org/de/packages/com.wesaphzt.privatelock/ sowie einer derzeit nicht

ausgereiften App *MotionLock* https://www.f-droid.org/de/packages/us.spotco.motionlock/

2.2.1.3.2 **Apple iOS** ist grundsätzlich verschlüsselt. Beim Systemstart sollte ebenfalls ein Passwort wie bei Android gewählt werden. Für die biometrische Entsperrung (bei neueren Geräten nur Face-Entsperrung) gelten die gleichen Risiken wie bei Android

2.2.1.4 **Router / Access Points für WLAN**

- Standardpasswort Router/Accesspoint ändern; Zugriff auf Administrationsbereich im Idealfall nicht über WLAN zulassen.
- WPS deaktivieren
- WLAN nur mit WPA2 oder WPA3 (neu) Verschlüsselung betreiben. WPA3 nur möglich, wenn Smartphone / Tablet das auch beherrschen. WPA / WPA2 Mixed Mode nicht benutzen. Ihr solltet kein Gerät haben, welches WPA technisch voraussetzt. WPA2 / WPA3 Mixed Mode kann genutzt werden.
- Personen denen ihr nicht blind vertraut nur ein Gästezugang aufs WLAN anbieten. Alternativ und ebenso für den Fall, dass Ihr auch alte, eventuell unsichere Geräte oder einige schlecht gemachte bzw. gewartete SmartHome Geräte im WLAN nutzen möchtet, könnt ihr kaskadierende Router einrichten. Zum Aufbaukonzept und weiteren Hintergrundinformationen recht einfach erklärt, ein Video (Fritzbox ist ersetzbar durch andere Router): https://www.youtube.com/watch?v=Q0YuAgMO4os hier Text aus gleicher Quelle https://ittweak.de/router-kaskade-schutz-des-eigenen-netzwerks-wegen-iot/ (IoT (z.B. SmartHome) ist wie erwähnt nur ein Anwendungsfall, es geht generell um die Separierung von eher unsicheren und sicheren Geräten)
- MAC-Filter sind überflüssig und bei Beachtung der anderen Grundsätze auch nicht notwendig. Mac-Filter halten vielleicht einen beliebigen Nachbarn fern, nicht aber jemanden mit Erfahrung in der IT Sicherheit.

2.2.2 Apps

- Apps können allgemein über eine weitere App geschützt werden. Anbieter von Security-Software haben diese Funktion oft mit an Bord (z.B. Kaspersky Sicherheit; AVG Protection). Eine Open Source App ist *AppLocker* https://www.f-droid.org/de/packages/com.gueei.applocker/
- Viele Apps haben eigene Zugangssicherungen, z.B. Messenger. Hinweise dazu bei den entsprechenden Apps.

2.2.3 Dateien, Speichermedien, BackUp

- Für unterschiedliche Zwecke wollen und müssen wir Dateien, Sammlungen von Dateien (z.B. Fotos) oder generell BackUps (z.B. von Passwortdatenbanken) sicher und geschützt aufbewahren. Dafür benutzen wir idealerweise Verschlüsselungssoftware die uns verschlüsselte Container bereitstellt, quasi wie ein Tresor oder gleich ein ganzes Laufwerk bspw. einen USB-Stick verschlüsselt. Nutzbar über fast alle relevanten Geräte / Betriebssysteme ist *Veracrypt* (Nachfolger von Truecrypt), d.h. Ihr erstellt bspw. einen Container auf dem Windows PC und nutzt den ebenfalls auf dem Android Smartphone und umgekehrt: https://www.veracrypt.fr/en/Downloads.html (dort auch die detaillierte Dokumentation in Englisch). Eine genügende deutsche Dokumentation findet sich unter diesem Link: https://www.rz.uni-wuerzburg.de/dienste/it-sicherheit/it-arbeitsplatzsicherheit/schritt-fuer-schritt-anleitung-veracrypt/ Ihr könnt solche Container auch in die Cloud schieben.
- **Anmerkung zu Linux**: Einige tun sich vielleicht etwas schwer *Veracrypt* auf einem Linux-System zu Installieren. Einfacher ist es womöglich aus dem offziellen Softwaredepot bei Ubuntu das Programm *zuluCrypt* zu laden. Erläuterung hier: https://wiki.ubuntuusers.de/zuluCrypt/ . *zuluCrypt* kann sowohl mit *Veracrypt* aber auch

bspw. mit LUKS umgehen, das heisst Verschlüsselungen einrichten und entschlüsseln, wobei ich mich allerdings für die Art der Verschlüsselung jeweils entscheiden muss.

- **Anmerkungen zu Android**: für Android-Geräte nutzt Ihr bitte die Open Source App *EDS Lite* *https://f-droid.org/de/packages/com.sovworks.edslite/* (es gibt auch im Google Playstore eine kostenpflichtige Version, die u.a. 2 Faktor Authentifizierung beherrscht oder die gleichzeitige Nutzung von mehreren Chiffrierverfahren, also bspw. die gleichzeitige Verschlüsselung mit AES, Twofish und Serpent. Wenn Ihr demnach *EDS Lite* nutzt, was bei einem guten Passwort absolut ausreicht (Passwort Manager ist Euer Freund, lasst Euch eines generieren, das müsst Ihr Euch weder merken, noch merken können) und am PC einen Container erstellt, bitte nur ein Chiffrierverfahren gleichzeitig nutzen und keinen 2. Faktor. PIM (Personal Iterations Multiplier) ist kein 2. Faktor in diesem Sinne, kann aber quasi als eine zusätzliche PIN mit VeraCrypt auch bei EDS Lite genutzt werden. Erläuterung hier: https://blog.doenselmann.com/veracrypt-mit-pim-nutzen/ . *EDS* unterstützt die Verschlüsselungscontainer VeraCrypt, TrueCrypt, LUKS, EncFs. Beim Erstellen eines verschlüsselten Containers muss ich mich ausdrücklich für ein Format entscheiden, beim Entschlüsseln probiert EDS selbständig was passt.
- **Anmerkungen zu Apple iOS:** nutzt bitte die App *Disk Decipher* von Richard Huveneers, derzeit 1,09 €. Diese App kann auch VeraCrypt Container verarbeiten.

2.3 Webzugang und allgemeine Nutzung des Internet

Schutzziele sind allgemein wie eingangs erwähnt die Informationssicherheit und hier rückt vermehrt der Datenschutz in den Focus. Wir wollen Informationen vertraulich und sicher austauschen (vgl. auch Kap. Kommunikation), Webseiten oder webbasierte Dienste (z.B. Cloud) im Idealfall weitgehend anonym besuchen, eine Profilerstellung von uns verhindern. Und da wir hier eben nicht für uns allein sind und sein wollen, möchten wir nicht von anderen absichtlich oder unabsichtlich mit Schadsoftware kompromittiert werden (Kap. Schadsoftware). Der Staatstrojaner ist ein Anwendungsfall (der Staatstrojaner ist nicht eine Software und die Angriffsszenarien sind vielfältig). Im Folgenden geht es also auf einer hohen Flughöhe, mithin ohne Details, darum, wer was von uns im Web sieht oder sehen könnte, welcher Schaden uns zugefügt werden kann und wie wir unsere Lage diesbezüglich verbessern.

2.3.1 Sichtbarkeit im Web

Euer Internet Service Provider (ISP), z.B. Telekom sieht verständlicherweise sehr viel, laufen Eure Daten doch über seine Server: welche Websiten besucht Ihr, eintsprechend Social Media, mit wem tauscht Ihr E-Mails aus, auch das Betriebsystem sieht diese Daten, bei Einstellung auch den Standort und es übermittelt diese auch, etwa an Microsoft, Apple, Google. Auch Websiten, Suchmaschinen oder Apps können Euer Verhalten tracken. Das hängt entscheidend von den Einstellungen ab. Und insbesondere bei den BigTechunternehmen laufen die Informationen zusammen. Durch die Verschärfung der Überwachung werden auch private Unternehmen verpflichtet solche Daten herauszugeben oder wie bei ISPs Hilfestellungen bei Angriffen zu geben.

2.3.2 Anonymisierung und VPN

Ein VPN (Virtual Private Network) baut einen verschlüsselten Tunnel zwischen Eurem Endgerät und dem VPN-Anbieter auf, der dann die Anfrage und Auslieferung von Daten (bspw. einer Internetseite) weiterleitet und mit der IP Andresse des VPN Anbieters versieht.

Damit ist unsere Identität ein wenig und das was wir tun im Prinzip sehr gut geschützt, d.h. welche Seiten wir besuchen und generell unsere Datenströme (das ist alles in dem Tunnel verborgen). Auch hat unser Internetanbieter nicht die Möglichkeit Mitwirkungen zu erbringen, zu denen mit dem „Gesetz zur Anpassung des Verfassungsschutzrechts“, welches im Juni 2021 beschlossen wurde, leicht verpflichtet werden kann, etwa unsere Anfrage nach einer Internetseite auf eine manipulierte Seite umzuleiten.

Dennoch sind wir nicht sicher anonym, die IP-Adresse ist ein einfaches und doch nur eines von vielen Merkmalen. So könnten wir über den sog. Fingerabdruck unseres Browsers-/Browserfensters, also eine Vielzahl von Eigenschaften zuverlässig identifiziert werden. Welche Daten das sind, könnt Ihr mit diesem Anonymitätstest feststellen http://ip-check.info/?lang=de Außerdem wird unser Datenstrom vielleicht außerhalb des Tunnels geleitet, das testen wir hier https://www.dnsleaktest.com (dort auch Hintergrundinformationen).

Somit verlagert sich irgendwo der Angriffspunkt von Behörden, die im Idealfall zwar den Tunnel nicht kontrollieren, aber ab dem VPN Anbieter wieder dabei sind. Zuordnungen können angesichts der Tatsache einer nur scheinbaren Anonymität dann womöglich teilweise gemacht werden. Viel entscheidender ist aber ein Problem, was Edward Snowden prägnant beschrieben hat und was mit Vertrauen zu tun hat:

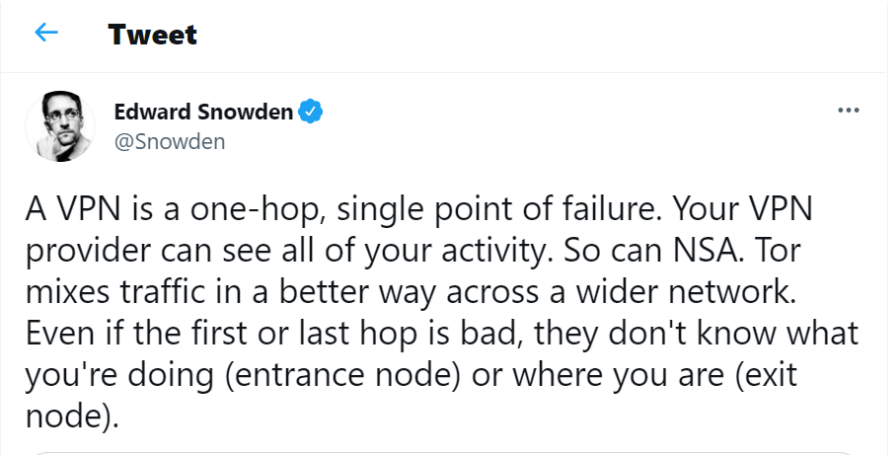

Abbildung 1 https://twitter.com/snowden/status/941015513915908096

VPN Anbieter haben es daher in der Hand und es gibt leider nicht wenige, die wenigsten entgegen der Werbung das Thema Datenschutz nicht so genau nehmen (Weitergabe von Daten, Tracker → dadurch ist man identifizierbar) https://www.kodi-tipps.de/nordvpn-gibt-persoenliche-daten-an-behoerden-weiter/ Vgl. auch generell https://www.privacy-handbuch.de/handbuch_97e.htm

Es geht letztlich nicht darum, kein VPN zu benutzen, vielmehr muss man sich der Grenzen bewusst sein.

Achtet bei einem VPN darauf Einstellungen zu treffen, dass der Internetverkehr unterbrochen wird, wenn die VPN Verbindung zusammenbricht. Das geht entweder über einen KillSwitch, den die VPN App bereitstellt oder dies kann in den VPN Einstellungen des Betriebssystems vorgenommen werden, bspw. Android: geht in Einstellungen/VPN zum VPN Anbieter und klickt dort das Zahnrad an. Aktiviert Verbindungen ohne VPN blockieren.

2.3.3 Tor

Tor ist ein Netzwerk, das den Datenverkehr über mehrere Server leitet und daher eine hohe Sicherheit bietet, selbst wenn unter den Servern einer ist, der von einem Geheimdienst betrieben wird. Die Geschwindigkeit von Tor ist nicht so hoch wie die Euch üblicherweise zur Verfügung stehende, aber sie ist mittlerweile einigermaßen flott.

Hier die Seite des Projekts mit Erläuterungen https://www.torproject.org/de/

Ihr könnt für alle Plattformen zum Internetsurfen fertige Programme / Apps herunterladen, die drei Standard-Sicherheitsstufen haben, aber individuell anpassbar sind.

- **PC**: Download von Projektseite oder bei Linux den Tor Installer aus dem Softwaredepot
- **Android**: Tor Projekt App aus Google Play-Store
- **Apple**: bitte ladet den Onion Browser von Mike Tigas

Wollt Ihr den gesamten Traffic eurer Apps oder ausgewählter Apps über Tor leiten, könnt Ihr das zuhause bspw. am Router einrichten, hier nur ein Hinweis auf das Vorgehen bei Android:

Ladet im Google Play Store die App *Orbot* und wählt unter VPN Modus / Tor aktivierte Apps die aus, deren Traffic über Tor geführt werden soll.

2.3.3 Cloud-Speicher

Cloud-Speicher sind sinnvoll, weil sie den Aspekt der Informationssicherheit „Verfügbarkeit“ gut abbilden. Andererseits liegen unsre Daten in der Cloud auf dem Präsentierteller. Ziel muss es sein, die Daten für uns, nicht aber für andere verfügbar zu machen. Das erreichen wir über Verschlüsselung. Bitte achtet darauf, was Euer Gerät ggf. automatisch in die Cloud schiebt, was dort besser nicht landen sollte (Android: Google Drive; Apple: iCloud)

Zwei Wege:

a. Man schiebt verschlüsselte Container in eine mehr oder weniger beliebige Cloud wie Google Drive. Diese Daten sind dann im Normalfall nicht direkt im laufenden Betrieb nutzbar, als wären sie ein Ordner wie jeder andere auch.
b. Es gibt entweder Cloud-Anbieter die komplett verschlüsselt sind oder einen verschlüsselten Bereich haben, der in Euer Gerät integriert wird, so dass Daten dort direkt abgelegt bzw. ausgelesen werden, wobei die Daten immer erst auf Eurem Gerät entschlüsselt werden (Apps dazu in den Stores bei Apple und Google):
    - Mega: https://mega.io (kostenlose Leistung genügt oftmals)
    - SecureSafe: https://www.securesafe.com/de/privatkunden/uebersicht

    Alternativ könnt ihr unverschlüsselte Clouds nehmen in Verbindung mit einer Software die zwischen Eurem Gerät und einem Speicherbereich in dieser Cloud (einem sog. Vault/Tresor) eine Ende-zu-Ende Verschlüsselung sicherstellt und daher im laufenden Betrieb ohne weiteren Zwischenschritt Zugriff bietet. Empfehlenswert die Open Source Lösung *CRYPTOMATOR* https://cryptomator.org/de/ , kostenlos für PC (Windows, Linux, Mac), die Apps für Android kosten derzeit bei Google und Apple je 9,99 €. Dokumentation hier: https://docs.cryptomator.org/en/latest/ *CRYPTOMATOR* braucht entweder die Clouds: Apple iCloud Drive, Dropbox, Google Drive, Microsoft OneDrive oder einen Cloudanbieter der WebDAV unterstützt. Mega und SecureSafe gelten als sicher, mit dem *CRYPTOMATOR* wäre man allerdings noch besser aufgestellt.

2.4 Kommunikation

2.4.1 Messenger

- ***Threema*** (https://threema.ch/de) : Messenger der seit Ende 2020 mit den Apps für Android, Apple und das Web Open Source ist, jedoch nicht der Threema Server. Der Dienst kann als sicher angesehen werden. Details zu Verschlüsselung hier https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf
    - Besondere Vorteile: kann vollständig anonym genutzt werden, d.h. die Angabe persönlicher Daten (E-Mail, Telefonnummer usw.) ist nicht erforderlich
    - In den Sicherheitseinstellung kann ein separater Zugriffsschutz eingestellt und die Verschlüsselung lokaler Dateien mit einer eigenen Passphrase belegt werden. Dies einzurichten bietet einen deutlich höheren Schutz gegen bestimmte Angriffsszenarien bei Menschenmengen oder Festnahmen/Überfällen.
    - ID Wiederherstellung und Datenbackup möglich mit eigenem Passwort (Threema Safe Cloud sowie lokal), das entsprechend sicher sein muss.
    - Kosten bei Apple und Google derzeit je 3,99 €, im Threema-Shop https://shop.threema.ch 3,65 €
- ***Signal*** (https://signal.org/de/download/) ebenfalls Open Source Messenger (App und Server) der spendenfinanziert und für Nutzer kostenlos für alle relevanten Plattformen bereitgestellt wird.
    - Für die Erst-Anmeldung muss eine Telefonnummer angegeben werden an die ein Verifizierungscode geschickt wird, d.h. Signal kann dennoch auf weiteren Geräten ohne SIM genutzt werden
    - Die App kann mit der Android Sperre bzw. Fingerabdruck zusätzlich geschützt werden. Die Wiederherstellung auf einem anderen Gerät mit den Alt-Daten erfordert eine PIN, die trotz Bezeichnung als PIN auch alphanumerisch sein kann.
- ***Telegram*** (https://telegram.org) die Vorteile als Twitter und Youtube-Ersatz sind unbestritten (Gruppen mit bis zu 250.000 Mitgliedern und öffentliche Kanäle). Zwar Open Source, aber als Messenger nicht unkritisch, weil nicht standardmäßig Ende-zu-Ende verschlüsselt. Die Praxis zeigt die Schwäche dieses Konzepts. Viele Verfahren wegen mitgelesener Chats durch staatliche Einrichtungen.
    - Weil bei den Ende-zu-Ende Verschlüsselungen oft Bedienungsfehler gemacht werden, hier eine Anleitung: https://www.netzwelt.de/anleitung/182704-telegram-so-aktiviert-ende-ende-verschluesselung.html
    - Die App hat eigene Pin-Sperre, die in Privatsphäre und Sicherheit aktiviert werden kann. Dort auch unbedingt die „Zweistufige Bestätigung“ aktivieren, um einen Identitätsdiebstahl zu verhindern (Kurzbegründung: bei Sicherung nur Über SMS kann Staat - nach neuer Gesetzeslage auch auf niedrigster Schwelle legal - SMS abfangen und Account mit Eurer Identität aufmachen). Wer das bisher versäumt hat, kann unter „Aktive Sitzungen“ ebenda nachschauen, ob mehr Sitzungen laufen als man selber betreibt.
    - Ladet die App nicht bei Apple oder Google, sondern bei Telegram selbst oder für Android die Version bei F-Droid Telegram FOSS: https://f-droid.org/de/packages/org.telegram.messenger/

2.4.2 E-Mail

Die E-Mail wird vorerst nicht aussterben. Unser Schutzziel ist der möglichst vertrauliche Informationsaustausch und wir wollen über den E-Mail Kanal kein Einfallstor für Schadsoftware eröffnen.

- Den vertraulichen Informationsaustausch erreichen wir über eine Verschlüsselung mittels PGP. Obwohl es nicht so schwer ist, zeigt die Existenz von Anbietern wie Protonmail oder Tutanota, dass hier offenbar eine Hürde vorliegt.
    - Komplette Anleitung für **PCs** am Bsp. des E-Mail Programms Thunderbird hier https://www.giga.de/software/sicherheit-utilities/sicherheit/e-mail-verschlusseln-einfache-anleitung/
    - Komplette Anleitung für **Android** Smartphones https://mobilsicher.de/ratgeber/e-mail-verschluesselung-fuer-android
    - Für **Apple** kann die App *Pretty Easy Privacy* (pEp) https://www.pep.security/docs/de/ios.html genutzt werden
    - Da sich nicht jeder die Einrichtung zutraut, können auch vorgefertigte Dienste genutzt werden, wobei idealerweise beide Nutzer einen Account bei dem Anbieter haben müssen, der kostenlos zu haben ist (bei Tutanota gibt es einen sehr einfachen Workaround). Eine Bewertung für Protonmail und Tutanota findet Ihr hier: https://www.privacy-handbuch.de/handbuch_31x.htm Tutanota hat abweichend von der Beschreibung inzwischen ebenfalls einen PC E-Mail Client in der Beta-Phase. Auf Smartphones sind diese Open Source Dienste aus Sicht Informationssicherheit bei Einsatz von deren Apps eingeschränkt zu empfehlen (vgl. Privacy Handbuch)
        - https://ctemplar.com (Android App auch bei f-droid)
        - https://protonmail.com
        - https://tutanota.com/de/ (Android App auch bei f-droid)

- Schadsoftware abzuwehren ist entscheidend eine Frage der Aufmerksamkeit. Allerdings gibt es E-Mail Programme, die hier unterstützen, indem bspw. Links beim Anklicken erst hervorgehoben und einer weiteren Inspektion unterzogen werden können, wie der Abfrage des Domaininhabers. Für Android die absolute Empfehlung mit vielen Sicherheits- und Datenschutzfunktionen die App *FairEmail* https://f-droid.org/de/packages/eu.faircode.email/ Für 5 € (auf beliebig vielen Geräten nutzbar) werden einige interessante zusätzliche Funktionen freigeschaltet, aber die meisten Funktionen sind kostenlos; auch im Google Playstore. Regelmäßige Weiterentwicklung, hervorragende Arbeit!
    - Sicherheits- und Datenschutz-Funktionen in der kostenlosen Version gemäß Beschreibung:
      * Ver-/Entschlüsselung wird unterstützt (OpenPGP, S/MIME)
      * Reformatierung von Nachrichten zur Verhinderung von Phishing
      * Bestätigen der Anzeige von Bildern, um Tracking zu verhindern
      * Bestätigen der Öffnung von Links, um Tracking und Phishing zu verhindern.
      * Versuch, Tracking-Bilder zu erkennen und zu deaktivieren
      * Warnung, wenn Nachrichten nicht authentifiziert werden konnten
      * Keine Datenspeicherung auf fremden Servern
      * Verwendung offener Standards (IMAP, POP3, SMTP, OpenPGP, S/MIME, usw.)
      * Sichere Nachrichtenansicht (Styling, Scripting und unsicheres HTML entfernt)
      * Bestätigung des Öffnens von Links, Bildern und Anhängen
      * Keine speziellen Berechtigungen erforderlich
      * Keine Werbung
      * Keine Analyse und kein Tracking (Fehlerberichte sind opt-in)
      * Kein Google-Backup
      * Kein Firebase Cloud Messaging
      * FairEmail ist eine Originalentwicklung, keine Abspaltung oder ein Klon

    - **E-Mail Proxy/Alias Dienst**: Ein E-Mail Proxy bietet mit eigenen, Eurem dort anzulegenden Konto zugeordneten E-Mailadressen (E-Mail Alias), einen Weiterleitungsservice. Sinnvoll unter Datenschutzgesichtspunkten und um diese Alias-E-Mailadressen leicht deaktivieren zu können, wenn diese für Angriffe genutzt werden. Eure eventuell langjährig genutzte E-

Mailadresse bleibt gegenüber potentiell fragwürdigen Kommunikationspartnern bzw. generell Konten im Internet geheim.

- *AnonAddy* for Android https://anonaddy.com Kostenloses Angebot ziemlich begrenzt. Android Open Source App https://f-droid.org/de/packages/host.stjin.anonaddy/
- *SimpleLogin* | Anti-spam. Solides Angebot auch vor der Bezahlschwelle. Mit etwas Probieren gibt es auch dabei seriös aussehende E-Mailadressen. E-Mail schreiben und empfangen https://simplelogin.io Android Open Source App: https://f-droid.org/de/packages/io.simplelogin.android.fdroid/

2.5 Schadsoftware

Schadsoftware gelangt selten ohne Unachtsamkeit auf Eure Geräte. Auf welche Internetseiten gehe ich? Könnte es sich bei einer Internetseite vielleicht um einen sog. Honeypot handeln (Geheimdienste, Antifa oder andere Kriminelle locken Euch auf eine präparierte Seite: Download „Mein Kampf“, Threema kostenlos usw.)? Mit wem kommuniziere ich? Welche Anhänge oder Links öffne ich? Stelle ich eine Prüfung an? Öffne ich im Zweifel Anhänge auf einem eher sicheren System wie Linux? Für kritische Fälle könnt Ihr einen „quasi mobilen Rechner“ erstellen, auf Basis der sehr abgesicherten Linux Distribution Tails (https://tails.boum.org/index.de.html). Ihr benötigt dazu lediglich einen USB-Stick ab etwa 8 GB Speichervolumen. Das System ist ausreichend dokumentiert und so sei an dieser Stelle darauf verwiesen; https://tails.boum.org/doc/index.de.html Weitere Erläuterungen sprengen den Rahmen des vorliegenden Überblicks.

Eine gute Möglichkeit Links/URLs und Dateien/Anhänge vor dem Öffnen zu prüfen, ist die Seite VIRUSTOTAL https://www.virustotal.com/gui/

- **Windows**: Regelmäßige Updates. Ein Virenscanner ist hier empfehlenswert, wenigstens der (kostenlose) von Microsoft: Microsoft Defender.
- **Linux**: neben regelmäßigen Updates, keine weitere Software erforderlich. Wer erhöhte Sicherheitsansprüche hat kann sein Linux System härten. Hier findet sich eine gute Anleitung, bestehend aus 4 Teilen (die weiteren Folgen sind verlinkt): https://www.kuketz-blog.de/sicheres-desktop-system-linux-haerten-teil1/
- **Apple iOS**: regelmäßige Updates, kein Virenscanner erforderlich
- **Android**: regelmäßige Updates, im Google-Kontext auch von Apps wie Webview; an sich braucht Ihr keinen Virenscanner und vom Konzept her ist er auch nicht notwendig. Apps laufen grundsätzlich in einem geschlossenen Sandkasten und der Nutzer selbst gewährt regelmäßig Berechtigungen, das gilt auch für Virenscanner. Daher funktionieren Virenscanner auch nicht so wie unter Windows, vielmehr werden in erster Linie – und so arbeitet bereits Google Play Protect – existierende Apps mit Vergleichslisten abgeglichen. Wer weniger auf Google setzt und vor allem nicht möchte, dass seine Scans das eigene Gerät verlassen (wie bei den Kasperskys, Nortons usw.) oder noch ein altes, nicht mit Updates versorgtes Gerät hat, dem sei diese Open Source App empfohlen, *Hypatia*: https://www.f-droid.org/de/packages/us.spotco.malwarescanner/ u.a. mit Signaturen von Eset.
  - Wichtig: überlegt Euch gut, von wo Ihr Apps ladet und habt einen Überblick, welche Apps die Berechtigung zur Installation haben. Das sollten nur sichere Stores sein, wie Google Play, F-Droid und temporär der Browser, mit dem Ihr Apps aus seriösen Quellen ladet. Seriöse Anbieter haben darüber hinaus auch Prüfsummen bzw. -Signaturen für Ihre Apps (SHA256 --> beherrschen viele Dataeimanager oder PGP --> Kurzanleitung hier https://www.codingblatt.de/software-signaturen-verifizieren/).

3 Weitere interessante Apps für Android

Da die meisten Kameraden Android haben, werden hier lediglich Android Apps gelistet.

- Insular- Isoliere deine Big Brother-Apps https://f-droid.org/de/packages/com.oasisfeng.island.fdroid/
- Kostenlose VPNs
  - Riseup https://www.f-droid.org/de/packages/se.leap.riseupvpn/
  - Lavabit https://www.f-droid.org/de/packages/com.lavabit.pahoehoe/
  - ProtonVPN https://f-droid.org/de/packages/ch.protonvpn.android/
- Apps für 2 Faktor Authentifizierung basierend auf TOTP

    - Aegis: https://www.f-droid.org/de/packages/com.beemdevelopment.aegis/
    - AndOTP https://www.f-droid.org/de/packages/org.shadowice.flocke.andotp/
- App für Kontakte, um diese vor Schnüffel-Apps zu isolieren
    - OpenContacts: https://www.f-droid.org/de/packages/opencontacts.open.com.opencontacts/
- Apps nach Trackern durchsuchen (die erste ist flexibler, aber nicht für jeden so verständlich):
    - ClassyShark3xodus https://f-droid.org/de/packages/com.oF2pks.classyshark3xodus/
    - Exodus https://f-droid.org/de/packages/org.eu.exodus_privacy.exodusprivacy/
- Privatsphäre über verschlüsselte DNS Anfragen, Durchleitung Tor und I2P
    - InviZible Pro https://www.f-droid.org/de/packages/pan.alexander.tordnscrypt.stable/
- Zwischenablage bereinigen – darauf kann jede App zugreifen
    - Clipboard Cleaner https://f-droid.org/de/packages/io.github.deweyreed.clipboardcleaner/
- App zum Blockieren von Werbung/Tracking (da auf VPN Technologie basierend, nicht parallel mit anderen Apps nutzbar, die VPN-technologie benötigen; einige VPN Anbieter haben integrierte Werbe- und Trackingblocker, ggf. nicht gegen die eigenen)
    - Blockada 5 https://f-droid.org/de/packages/org.blokada.fem.fdroid/

4 Weiterführende Informationen

- Umfassende Vertiefung:

https://www.privacy-handbuch.de/handbuch_11.htm

- Passwörter, allgemein

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

- Sicherheit von Fingerabdruck-Sensoren: https://blog.talosintelligence.com/2020/04/fingerprint-research.html
- VPN Verschlüsselung vertiefend und fast marketingfrei erklärt: https://www.smartydns.com/de/wissensdatenbank/vpn-verschlusselung/
- Entwicklung Staatstrojaner https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/ (da steht auch was zu quantitativen Anwendungsfällen – wenn dann können die Autoren bestenfalls wissen, wie oft er zugegebener Weise (legal) eingesetzt wurde oder der Einsatz aufgedeckt werden konnte.)