



All Computers Are Beschlagnahmt

Wie schütze ich meine
Daten vor Einsicht
durch die Behörden?

Commit e944cd3bace662dc3e3597d0d9a0c8643990e865

built on 23. Februar 2021, 06:36UTC

Weitergabe und Vervielfältigung ausdrücklich erwünscht.

beschlagnahmt@riseup.net

96D2 D925 9050 EFBD C187 5334 A02F 772C 7A0E 353F

Online verfügbar unter beschlagnahmt.org oder via Tor unter

hkku46njdrc6zj76hhaeflyyccsrpuwimclhs75rkowbbguyudmbinad.onion

Lizenziert unter WTFPL (<http://www.wtfpl.net/txt/copying/>)

Inhaltsverzeichnis

1 Hausdurchsuchung	7
2 Nach der Beschlagnahme	9
3 Kommunikationsüberwachung	11
3.1 Statistik	12
4 Online Durchsuchung und Quellen TKÜ	14
4.1 Online-Durchsuchung	14
4.2 Quellen-TKÜ	15
4.3 Gegenmaßnahmen	15
5 Dateien löschen	17
5.1 Löschen mit Eraser (Win):	17
5.2 Löschen mit SDelete (Win):	18
5.3 Löschen mit shred (Linux):	18
6 Daten verschlüsseln	20
6.1 Grundsätzliches	20
6.2 Laptop / Desktop	21
6.2.1 Systemverschlüsselung mit VeraCrypt (Windows)	21
6.2.2 Systemverschlüsselung bei der Installation (Linux)	23
6.2.3 Systemverschlüsselung mittels Bitlocker (Windows)	23
6.2.4 Systemverschlüsselung mittels FileFault (MacOS)	24
6.2.5 Container mit VeraCrypt (Windows und Linux)	24
6.3 Smartphone	25

7 Mail-Verschlüsselung	27
7.1 Grundsätzliches	27
7.1.1 Asymmetrische Verschlüsselung	27
7.2 Verschlüsselte Kommunikation mit GPG4Win und Kleopatra (Win)	29
7.2.1 Installieren und eigene Schlüssel erstellen	29
7.2.2 Eigenen öffentlichen Schlüssel rausfinden	29
7.2.3 Eine Nachricht verschlüsseln	29
7.2.4 Eine Nachricht entschlüsseln	30
7.3 Verschlüsselte Kommunikation mit Thunderbird (Windows, Linux und MacOS)	31
7.4 Verschlüsselte Kommunikation mit GPG (Linux)	31
7.4.1 Eigene Schlüssel erstellen	31
7.4.2 Eigenen öffentlichen Schlüssel rausfinden	32
7.4.3 Eine Nachricht verschlüsseln	32
7.4.4 Eine Nachricht entschlüsseln	32
7.5 Android	32
7.6 PGP-Fingerprints	33
8 Messenger	34
8.1 Bezugsquellen	34
8.2 Keine Anonymität	34
8.3 Nachrichten auf dem Sperrbildschirm	35
8.4 Apps und Protokolle	35
8.4.1 Signal	35
8.4.2 Threema	36
8.4.3 WhatsApp	37
8.4.4 Telegram	37
8.4.5 SMS	38
8.4.6 Jabber/XMPP	38
8.4.7 Matrix	38
9 Telefonie	40
10 Passwörter	42
10.11. Daten entschlüsseln	42
10.22. Anmeldung bei Diensten	44
10.3 Sonderfall Smartphones	44

11 Passwort-Manager	46
11.1 Windows, Linux und MacOS	46
11.1.1 Datenbank synchronisieren	47
11.1.2 Browser-Integration	47
11.2 Android und iOS	48
12 Glaubliche Abstreitbarkeit	49
13 Two-Factor Authentication	52
14 Phishing	54
15 Anonym im Netz	58
15.1 Tor	58
15.1.1 Funktionsweise	58
15.1.2 Tor Browser	60
15.1.3 Betriebssysteme mit Tor-Integration	60
15.2 VPN	62
16 IMSI Catcher und Stille SMS	64
17 OpSec	68
18 Dienste und Anbieter	71
18.1 Mail	71
18.2 Matrix	72
18.3 Jabber/XMPP	72
18.4 Jitsi Meet	73
18.5 BigBlueButton	73
18.6 DNS	73
19 Resümee	74

Behörden können deine elektronischen Geräte beschlagnahmen, auslesen, Deine Konten übernehmen, deine Kommunikation und Anschlüsse überwachen. Das passiert gar nicht so selten.

Sei für diesen Fall vorbereitet!

Mit ein paar Vorsichtsmaßnahmen kannst du dafür sorgen, dass die ganze Aktion zwar nervig ist, aber der Staat nicht in deinen persönlichen Daten rumschnüffelt¹. Hier bekommst du einige Anhaltspunkte wie du dich schützen kannst, auch ohne ein Computernerd zu sein. Lieber jetzt ein wenig Arbeit investieren und dafür bleiben später deine Daten für die Cops tabu.

Der Quelltext von ACAB ist unter <https://github.com/beschlagnahmt-org/beschlagnahmt> zu finden. Wenn du einen Fehler gefunden oder einen Verbesserungsvorschlag hast, lass es uns wissen². Gerne kannst du direkt auf Github einen Verbesserungsvorschlag einreichen³. Sollte dir das zu öffentlich sein, melde dich gerne per Mail.



(Computer: CC-BY-SA-3.0 Thomas Kaiser, Montage: Beschlagnahmt)

¹<https://www.kontextwochenzeitung.de/debatte/438/linksunten-6138.html>

²<https://github.com/beschlagnahmt-org/beschlagnahmt/issues>

³<https://github.com/beschlagnahmt-org/beschlagnahmt/pulls>

Kapitel 1

Hausdurchsuchung

Guten Morgen Sonnenschein! Es ist 6 Uhr¹ morgens und einige unfreundliche Beamte:innen stehen in deiner Wohnung und erklären dir, dass sie nun eine Durchsuchung durchführen werden. Du bleibst natürlich cool und rufst dir in Erinnerung wie du dich in so einer Situation verhalten solltest².

Deine Computer fährst du herunter, falls du keine Zeit hast hälst Du den Power-Knopf ein paar Sekunden lang gedrückt. Bei Geräten ohne Akku kannst Du auch den Stecker ziehen. Dank Verschlüsselung und von dir clever gewählten Passwörtern sind die Daten damit nach wenigen Sekunden sicher. Aus dem gleichen Grund schaltest du auch dein Handy aus. Falls du telefonieren musst, nimm ein anderes Gerät z. B. das deiner ‘Gäste’.

Irgendwann werden sie dann anfangen deinen Kram einzupacken. Achte darauf, dass sie sich an den Durchsuchungbeschluss halten und sei ansonsten ganz entspannt. Du bist nicht verpflichtet Passwörter oder PINs heraus zu geben, mache das auch nicht³.

¹<https://www.ferner-alsdorf.de/hausdurchsuchung-zeiten/>

²<https://rote-hilfe.de/downloads1/category/3-was-tun-wenn-s-brennt-und-rechtshilfe-infoflyer-zu-spezifischen-themen?download=10:infoflyer-hausdurchsuchung-was-tun>

³<https://www.youtube.com/watch?v=bpPv1WEi6ZY>

Falls möglich lasse deine elektronischen Geräte vor Ort versiegeln.

Kapitel 2

Nach der Beschlagnahme

Jetzt werden die Cops oder ein:e Sachverständige:r sich daran machen deine Daten auszulesen und "gerichtssicher" zu machen. Wenn du deinen Kram anständig verschlüsselt hast werden sie dabei nicht weit kommen. Andernfalls werden die Daten akribisch durchsucht. Den dabei verwendeten Forensikprogrammen entgeht kaum etwas und selbst gelöschte Daten können wiederhergestellt werden.

Auch gesperrte Handys können mit der Spezialsoftware und -hardware ausgelesen werden. Die Funde werden mit einer Prüfsumme versehen und katalogisiert, so dass sie vor Gericht als Beweis verwendet werden können.

Wird das Verfahren irgendwann eingestellt bekommst du deine beschlagnahmten Sachen zurück. Das kann aber dauern und es soll auch schon vorgekommen sein, dass Festplatten die nicht entschlüsselt werden konnten bei der Rückgabe auf einmal leer waren.

Kapitel 3

Kommunikationsüberwachung

Bei der Telekommunikationsüberwachung, oder kurz TKÜ hören die Behörden Kommunikation direkt beim Dienstbetreiber ab. Das kann zum Beispiel euer Handyanbieter sein, euer Internet-Provider oder euer E-Mail Service. Bei Telefonaten kann bereits ab dem Zeitpunkt des Verbindungsauftaupunkt mitgehört werden. Wenn du noch das piepen hörst, weil die angerufene Person das Gespräch bisher nicht angenommen hat und dich dabei mit jemanden neben dir unterhältst - wird das protokolliert, der analysiert und auch mit den Geodaten abgeglichen, die den Schnüfflern bekannt sind. Es können viele Daten auch im Nachhinein angefordert werden, zum Beispiel die Websites die du aufgerufen hast, die Nummern die du angerufen hast, die E-Mails die du geschrieben hast und die Privatnachrichten die du auf Facebook verschickt hast. (Vorausgesetzt der Anbieter hat diese Daten noch gespeichert.) Auch hier kannst du dich wieder durch verschiedene Verschlüsselungsverfahren schützen.

Um das Thema Vorratsdatenspeicherung wird aktuell noch gestritten. Momentan ist diese ausgesetzt, wie sich das in Zukunft entwickeln wird ist aber noch unklar. Halte dich am besten gelegentlich etwas auf dem Laufenden.

Neben solchen Anfragen bei Dritten gibt es auch noch den sogenannten "Großen Lauschangriff" also das direkte Abhören der Wohnung mit Mi-

krofonen. Dieser wird aber recht selten angewandt. Im Jahr 2019 wurden im repressiven Bereich 9 Maßnahmen angeordnet und 7 davon vollzogen. Beachte das eine Hausdurchsuchung für die Cops eine gute Gelegenheit ist Wanzen zu deponieren.

Wer ebenfalls gelegentlich mithört sind die Sprachassistenten von Google, Apple und Amazon. Diese Geräte nehmen kontinuierlich ihre Umgebung auf. (Sonst könnten sie ja auch gar nicht auf ein "Hey Google" reagieren.) Aufzeichnungen von Sprachbefehlen werden auf den Servern der Anbieter gespeichert und können theoretisch auch von den Behörden angefragt werden.

Mensch sollte es sich auf jeden Fall zweimal überlegen welche Gespräche in der Gegenwart von Alexa oder einem Handy mit aktivierter Google-Sprachsteuerung geführt werden sollten.

3.1 Statistik

Wie oft werden eigentlich Überwachungsmaßnahmen angeordnet? Beispielhaft schauen wir uns hier mal die Statistiken von 2015 und 2017 an, welche von netzpolitik.org aufbereitet wurden. Im Jahr 2015 gab es 3332 Festnetz-Überwachungen, 21906 Mobilfunküberwachungen und 7431 Internetüberwachungen. Verkehrsdatenüberwachungen, also das Sammeln von Metadaten über die Kommunikation wurde in ganzen 26265 Fällen angeordnet und die Anordnung in weiteren 899 Fällen verlängert. Im Jahr 2017 sind diese Zahlen leicht abgesunken, aber im Vergleich noch immer ausgesprochen hoch.



Bild: Creative Commons BY-NC-SA 4.0. Netzpolitik.org

Links:

- Wikipedia - Vorratsdatenspeicherung¹
- Polizei überwacht vor allem wegen Drogen²
- Polizei überwacht erstmals weniger³

¹<https://de.wikipedia.org/wiki/Vorratsdatenspeicherung>

²<https://netzpolitik.org/2016/statistik-polizei-ueberwacht-weiterhin-vor-allem-wegen-drogen/>

³<https://netzpolitik.org/2019/ueberraschung-polizei-ueberwacht-erstmals-weniger-kommunikation/>

Kapitel 4

Online Durchsuchung und Quellen TKÜ

*

4.1 Online-Durchsuchung

Eine ‘Online-Durchsuchung’ lässt sich mit einer heimlichen Hausdurchsuchung vergleichen. Die Behörden versuchen dabei einen Trojaner auf dem Zielsystem zu installieren und so alle gespeicherten Daten (Fotos, Adressbuch, Kalender, Chats, ...) abzugreifen. So hat zum Beispiel die Firma DigiTask, der Hersteller des “Staatstrojaners¹”, Funktionen in die Software eingebaut die die Behörden überhaupt nicht nutzen dürften². Auch die Software FinFisher der deutschen Firma Gamma Group wurde zeitweise ohne Rechtsgrundlage vom LKA Berlin lizenziert.

¹<https://youtu.be/8REBKuFGfk8>

²<https://www.ccc.de/de/updates/2011/staatstrojaner>

4.2 Quellen-TKÜ

Die harmlos klingende Bezeichnung ‘Quellen-TKÜ’ ist in der Praxis nichts anderes als eine ‘Online-Durchsuchung light’. Auch hier wird eine Schadsoftware auf euer(e) System(e) aufgebracht, mit dem Unterschied, dass nur ‘laufende Kommuniaktion’ abgeört werden soll. Durch die starke Zunahme von Messengern mit Ende-zu-Ende-Verschlüsselung ist die Quellen-TKÜ ein immer beliebteres Mittel der Behörden. Es ist jedoch relativ aufwändig und teuer, so dass es nicht annähernd so oft eingesetzt wird wie das ‘klassische’ Abhören von Telefonaten und SMS. So gab es im Jahr 2019³, bis zum 20. November, 20 “tatsächlich durchgeföhrte” Online-Durchsuchungen und 368 “tatsächlich durchgeföhrte” Quellen-TKÜs.

4.3 Gegenmaßnahmen

Um dir gar nicht erst so einen Staatstjaner ein zu fangen ist es wichtig, dass du darauf achtest das deine Systeme sauber bleiben. Hinweise dazu findest du im Kapitel “Systemsicherheit”⁴. Gegen eine dauerhafte Infektion schützt dich auch die Verwendung des im Kapitel “Anonym im Netz”⁵ beschriebenen Betriebssystems ‘Tails’.

Nette Geschichte am Rande: Die Firmen Gamma und Hacking Team wurden beide von einem Frosch namens Phineas Phisher gehackt und interne Daten über ihre Geschäfte ins Netz gestellt.

³<https://netzpolitik.org/2020/justizstatistik-2019-die-polizei-setzt-taeglich-staatstjaner-ein/>

⁴[/systemsicherheit/](#)

⁵[/anonym-im-netz/](#)

**PHINEAS
PHISHER
HAS
A
Posse**

**Hack
Back**



Kapitel 5

Dateien löschen

*

Wie wir vorhin Erfahren haben können die Cops und Sachverständige also gelöschte Daten wiederherstellen. Wie kann das angehen? Wenn du eine Datei auf deinem Computer löscht verschwinden die Einsen und Nullen auf der Festplatte nicht automatisch. Sie werden nur zum Überschreiben freigegeben falls der Platz für was anderes gebraucht wird. Du kannst die Datei also nicht mehr sehen, aber sie lässt sich mit etwas Arbeit noch rekonstruieren. (Auch wenn du den Papierkorb bereits "geleert" hast.) Die Lösung ist zum Glück ganz einfach. Wenn du die Daten sofort beim Löschen überschreibst kommt da keine:r mehr dran. Es gibt auch Programme die das für dich machen.

5.1 Löschen mit Eraser (Win):

1. Eraser¹ installieren (Standardinstallation)
2. Rechtsklick auf die Datei
3. "Eraser" und Unterpunkt "Erase" auswählen
4. Nochmal mit Klick auf "Yes" bestätigen

¹<https://eraser.heidi.ie/>

5. Warten bis die Datei verschwunden ist



Wenn dir das bei großen Dateien zu lange dauert kannst du in den Eraser-Einstellungen als Löschmethode auch „Pseudorandom Data (1 Pass)“ auswählen.

Wenn du mit der Kommandozeile zurecht kommst kannst du auch „SDelete“ von Microsoft verwenden. Das ist wahrscheinlich sogar etwas gründlicher.

5.2 Löschen mit SDelete (Win):

1. SDelete² installieren
2. In der CMD zum Speicherort navigieren
3. „sdelete DATEINAME“
4. Warten bis Datei verschwunden ist

5.3 Löschen mit shred (Linux):

1. wipe³ installieren (Paketverwaltung)
2. Im Terminal zum Speicherort navigieren
3. “wipe -f DATEINAME” eingeben
4. Warten bis die Datei verschwunden ist

Eine weitere Option für die du kein laufendes Betriebssystem brauchst ist DBAN⁴. Diese Techniken sind nur für klassische Festplatten geeig-

²<https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete>

³<http://lambda-diode.com/software/wipe/>

⁴[https://dбан.org](https://dban.org)

net. Für SSDs, SD-Karten, USB-Sticks und den internen Speicher von Handys funktioniert das leider nicht so gut. Das Überschreiben schadet dem Gerät und es können trotzdem noch Daten zurückbleiben. Wenn du so einen Speicher hast kannst du dich auf den Seiten des Hersteller erkundigen ob es für das Gerät sichere Löschfunktionen gibt. Fast alle Hersteller stellen dafür Software zur Verfügung. Ein weiteres Risiko ist das sogenannte Journaling. Das ist eine nützliche Technik um zu verhindern das Daten verloren gehen, die fast überall eingesetzt wird. Allerdings führt sie dazu das Forensiker:innen eventuell Metadaten wie Dateinamen oder sogar Dateiinhalte aus dem Journal wiederherstellen können, selbst wenn die eigentlichen Daten überschrieben wurden.

⚠ Fallstrick beim Löschen ⚠

Manche Systeme speichern zu Bilddateien kleine Vorschaubilder ab. Diese bleiben auch nach dem Löschen der Originaldatei erhalten.

Windows: %userprofile%\AppData\Local\Microsoft\Windows\Explor
Linux: ~/.cache/thumbnails/

Du bist mit allen Datenträgerarten auf der sicheren Seite wenn du deine Datenträger von vornherein verschlüsselst. Denn dann würde zum Wiederherstellen von Daten immer noch das Passwort benötigt werden. Oder du arbeitest einfach gleich ohne eine Festplatte. Dazu gibt es Live-Systeme wie Tails. Du kannst dann alle Festplatten aus deinem Gerät ausbauen und das Betriebssystem von einem USB-Stick starten. Nach dem herunterfahren sind alle Daten verschwunden. Mehr dazu findest du bei „Whonix“⁵ im Kapitel Anonym im Netz⁵. Als letzte Option bleibt immer den Datenträger physisch zu zerstören⁶. Sei dabei ruhig gründlich und trage eine Staubschutzmaske um keinen Glas- oder Metallstaub einzutragen, das ist wirklich sehr ungesund.

⁵ [/anonym-im-netz/](#)

⁶ <https://www.youtube.com/watch?v=4uRtRaHQp40>

Kapitel 6

Daten verschlüsseln

*

So schützt du also die Daten die du eh nicht mehr haben willst. Aber was ist mit denen die du noch brauchst? Diese solltest du verschlüsseln. Wenn du das richtig machst haben die Behörden kaum eine Chance an die Daten heranzukommen.

6.1 Grundsätzliches

Ein Versteck ersetzt keine Verschlüsselung. Irgendwo tief in einem Ordner abgelegte Dateien werden die Behörden mit großer Sicherheit finden. Gleiches gilt für in der Wohnung versteckte Datenträger, denn auch der Einsatz von Datenspeicher-Spürhunden hat zugenommen. Effektiv schützen kannst du dich nur in dem du deine Daten verschlüsselst. Wenn sie Datenträger mitnehmen ist das egal, da sie dich nicht zwingen können das Passwort herauszugeben. In den gleich folgenden Anleitungen wirst du dir an einigen Stellen ein Passwort ausdenken müssen. Bitte beachte hierfür auch das Kapitel "Passwort". Ein gutes Passwort ist für die Sicherheit deiner Daten essentiell. Wenn du Backups von deinen Daten anlegst, denk daran auch diese zu verschlüsseln. Bevor du

versuchst deine Geräte zu verschlüsseln lege auch eine Sicherung an, falls dabei was schiefgeht. Und noch was: Am sichersten sind die Daten die du gar nicht erst speicherst. Halte dich besonders bei heiklen Informationen an das Konzept der Datensparsamkeit. Wenn du unbedingt Papiere aufbewahren musst tue dies in einem Umschlag der mit "Für meinen Anwalt" o. Ä. beschriftet ist.

⚠️ Bedenke das diese Verfahren umgangen werden können indem in deine Wohnung eingedrungen wird und ein Keylogger installiert wird. Das ist ein kleines Gerät am USB Anschluss oder eine Software welche die Tastatureingaben mitschneidet. Statte also dein UEFI und ggf. deinen Bootloader mit einem Passwort aus¹ und prüfe immer mal wieder den Anschluss deiner Tastatur auf Unregelmäßigkeiten.

⚠️

6.2 Laptop / Desktop

Für deinen Computer hast du zwei grundlegende Optionen. Du kannst das gesamte System verschlüsseln², oder einen verschlüsselten Container anlegen in dem du vertrauliche Dateien ablegst.

6.2.1 Systemverschlüsselung mit VeraCrypt (Windows)

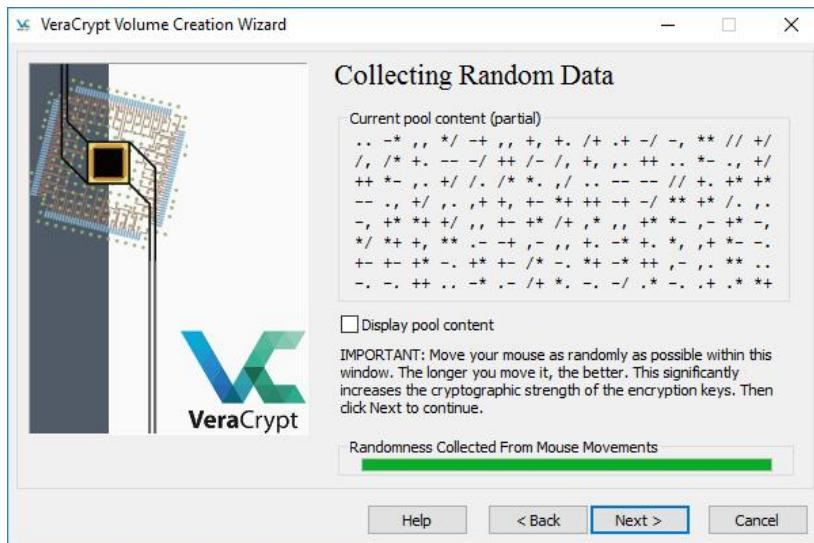
1. VeraCrypt³ installieren und starten
2. "Create Volume" klicken
3. "Encrypt the system partition" anwählen und "Next" klicken
4. "Normal" anwählen, "Next"
5. "Encrypt the whole drive"
6. Single- oder Multiboot auswählen. Wenn du nicht weißt worum es geht wähle einfach ersteres

¹<https://www.wikihow.com/Set-a-BIOS-Password>

²<https://www.veracrypt.fr/en/System%20Encryption.html>

³<https://www.veracrypt.fr/>

7. Algorithmen auswählen (AES und SHA-256 sind in Ordnung)
8. Passwort eingeben (siehe dazu Kapitel „Passwort“)
9. Die Maus möglichst zufällig durch das Fenster bewegen bis der grüne Balken voll ist, dann “Next”
10. “Next”
11. Entsprechend der Anweisungen eine Rescue Disk erstellen. Wenn du kein CD-Laufwerk hast kannst du auch einen USB-Stick verwenden. Mit der CD bzw. dem USB-Stick kannst du das System nicht wiederherstellen wenn du dein Passwort vergessen hast. Sie dienen nur dazu das System zu retten falls Dateien beschädigt wurden die VeraCrypt zum entschlüsseln benötigt. Du solltest den Datenträger also gut aufbewahren, aber falls die Cops ihn kriegen sind deine Daten aber trotzdem noch sicher.



VeraCrypt benötigt Zufallsdaten zum verschlüsseln.

12. “1-Pass” Wipemode auswählen (Das kennen wir schon vom Löschern)
13. “Test” klicken. Der Rechner wird nun neustarten und du kannst dich das erste mal mit deinem Passwort anmelden. Wenn ein

“PIM” verlangt wird drücke einfach Enter. Wenn alles funktioniert hat kann es weitergehen.

14. VeraCrypt sollte sich automatisch gestartet haben. Auf den Button “Encrypt” klicken
15. Notfallanweisungen lesen, ggf. drucken und mit “Ok” bestätigen
16. Abwarten bis alles verschlüsselt ist.

6.2.2 Systemverschlüsselung bei der Installation (Linux)

Fast alle Linux-Betriebssysteme bringen bereits Verschlüsselungsmechanismen mit. Zwischen den Verschiedenen Linux-Distributionen gibt es einige Unterschiede. Meistens ist es am einfachsten die Verschlüsselung direkt bei der Installation zu aktivieren. Beispielsweise stehen hier die Schritte für Ubuntu, hier⁴ findest du aber auch Anleitungen für andere Distributionen und Möglichkeiten auch ohne Neuinstallation ein verschlüsseltes System zu bekommen.

1. Installationsprozess starten
2. Im Fenster “Art der Installation” einen Haken bei “Encrypt the new Ubuntu installation for security” setzen und weiter zum nächsten Schritt
3. Passwort eingeben (siehe dazu Kapitel „Passwort“)
4. Haken bei “Overwrite empty disk space” setzen
5. Mit “Install Now” die eigentliche Installation starten.

6.2.3 Systemverschlüsselung mittels Bitlocker (Windows)

Sollte dir das wirklich viel zu kompliziert sein kannst du auch schauen ob deine Windows Version “Bitlocker”⁵ unterstützt. Das ist das Verschlüsselungsprogramm von Microsoft. Es ist einfacher zu bedienen, allerdings ist es

⁴<https://svenfila.wordpress.com/2010/11/04/encrypt-root-partition-without-re-installing-linux/>

⁵<https://docs.microsoft.com/de-de/windows/security/information-protection/bitlocker/bitlocker-basic-deployment>

sehr wahrscheinlich das dort Hintertüren eingebaut wurden. Grundsätzlich kann VeraCrypt da deutlich mehr Vertrauen entgegen gebracht werden, aber bevor du stattdessen gar keine Verschlüsselung benutzt verwende lieber Bitlocker.

6.2.4 Systemverschlüsselung mittels FileVault (MacOS)

1. Drücke die „Apple“-Taste > „Systemeinstellungen“ und klicke auf „Sicherheit“ und dann auf „FileVault“. (Wenn das Schloss unten links geschlossen ist, klicke auf das Schloss, um die Systemeinstellung zu entsperren.)
2. Klicke auf „FileVault aktivieren“. Du wirst daraufhin möglicherweise aufgefordert, dein Passwort einzugeben.
3. Nun kann du die eine Methode zum Aufheben des Schutzes auswählen, falls Du Dein Passwort vergessen hast. Klicke hier auf „Wiederherstellungsschlüssel erstellen und meinen iCloud-Account nicht verwenden“. Schreibe den Wiederherstellungsschlüssel auf und lege ihn an einem sicheren Ort ab.
4. Klicke auf „Fortfahren“. Wenn dein Mac weitere Benutzer hat, werden deren Informationen ebenfalls verschlüsselt. Die Benutzer entsperren die verschlüsselte Festplatte mit ihrem Anmeldepasswort.

6.2.5 Container mit VeraCrypt (Windows und Linux)

Das war die Systemverschlüsselung. Alternativ kannst du auch einen Container erstellen und deine Daten darin ablegen, anstatt das ganze System zu verschlüsseln. Dann musst du natürlich darauf achten keinerlei kritische Daten außerhalb des Containers zu belassen, was nicht immer ganz einfach ist.

1. VeraCrypt installieren und starten
2. „Create Volume“ klicken
3. „Create an encrypted file container“ anwählen und „Next“ klicken

4. "Standard VeraCrypt volume"
5. Einen Speicherort und Dateinamen für deinen Container auswählen, den Haken bei "Never save history" belassen
6. Algorithmen auswählen (AES und SHA-256 sind in Ordnung)
7. Größe des Containers festlegen
8. Passwort eingeben (siehe dazu Kapitel „Passwort“)
9. Ein Dateisystem auswählen (FAT ist in Ordnung) und die Maus möglichst zufällig durch das Fenster bewegen bis der grüne Balken voll ist, dann "Format"
10. Abwarten bis die Erstellung abgeschlossen ist und mit "Exit" das Programm verlassen

Container mit VeraCrypt öffnen

1. VeraCrypt starten
2. Freien Laufwerksbuchstaben auswählen
3. "Select File" und die Containerdatei auswählen
4. "Mount"
5. Passwort eingeben und "Ok" klicken

6.3 Smartphone

Die meisten Smartphones kommen heutzutage 'ab Werk' mit verschlüsseltem Speicher. Ob die Speicherverschlüsslung wirklich aktiv ist, solltest du zur Sicherheit trotzdem einmal überprüfen. Das geht auf jedem Gerät ein wenig anders. Meist wirst du in den Einstellungen unter 'Sicherheit' fündig, den genauen Weg für dein Gerät recherchierst du am besten selber. Sollte die Verschlüsselung nicht aktiviert sein, solltest Du das sofort nachholen. Du lädst deinen Smartphone auf und wählst die Option zum Verschlüsseln, gibst zweimal deine gewünschtes Passwort/PIN ein. Wie Du ein möglichst sicheres wählst, kannst du im Kapitel Passwörter⁶ nachlesen. Nun wartest bis der Prozess abgeschlossen ist. Teilweise muss nochmal explizit angewählt werden das auch die externe

⁶/passwort/

Speicherkarte verschlüsselt werden soll. Grundsätzlich ist das alles auch genau so sicher wie auf dem Computer, aber besonders ältere Geräte, die nicht mehr mit Updates versorgt werden stellen ein zusätzliches Risiko dar. Trotz Verschlüsselung ist es also vernünftig zu Aktionen nur ein billiges Zweit-Handy mitzunehmen, auf dem keine persönlichen Daten gespeichert sind. Auch eine SIM-Karte, die nicht mit deinem Namen verknüpft ist, ist dabei eine gute Idee.

The screenshot shows a mobile device's settings interface. At the top, there are icons for signal strength, battery level (36%), and other connectivity status. Below the header, there are two main sections: "VERSCHLÜSSELUNG" and "ANMELDEDATENSPEICHER".

VERSCHLÜSSELUNG

- Smartphone verschlüsseln
- Verschlüsselt

ANMELDEDATENSPEICHER

- Speichertyp
- Hardware-gestützt

Vertrauenswürdige Anmelddaten

Vertrauenswürdige CA-Zertifikate anzeigen

Kapitel 7

Mail-Verschlüsselung

*

7.1 Grundsätzliches

Wenn du eine Mail über das Internet versendest wird sie viele Stellen durchlaufen bis sie am Ziel angekommen ist. Vielen davon musst du, ohne Verschlüsselung einfach vertrauen, dass sie deine Daten schützen und sich im Zweifel auch gegen Behördenanfragen zur Wehr setzen. Das machen aber leider viele nicht. Zum Beispiel ist bekannt das 1&1 zu denen auch GMX und Web.de gehören ohne große Rückfragen gespeicherte Daten weitergeben. Aber auch bei kleineren Anbietern solltest du dich nicht darauf verlassen, dass die Betreiber:innen für dich in den Knast gehen werden wenn sie eine Anfrage bekommen. Die Lösung ist auch hier wieder Verschlüsselung.

7.1.1 Asymmetrische Verschlüsselung

Was wir gerade für die Verschlüsselung unserer Geräte verwendet haben war eine traditionelle symmetrische Verschlüsselung. Das bedeu-

tet das die Person an die Daten kommt die das Passwort hat. Für Kommunikation ist das etwas unpraktisch, da so das Passwort zwischen allen Kommunikationsteilnehmer:innen auf einem sicheren Kanal ausgetauscht werden muss bevor kommuniziert werden kann. Das ist umständlich und bringt das Risiko mit sich, dass das Passwort beim Austausch abgefangen wird. Dieses Problem wird mit asymmetrischer Verschlüsselung gelöst. Bei dieser haben unsere Kommunikationsteilnehmer:innen Alice und Bob je einen öffentlichen und einen privaten Schlüssel. Der öffentliche Schlüssel wird nur zum verschlüsseln verwendet, der private Schlüssel wird nur zum entschlüsseln verwendet.

Alice und Bob?

Alice und Bob sind die “Anna und Arthur” der Kryptografie, In unserem Beispiel wollen die beiden miteinander kommunizieren ohne dass Mallory mitlesen kann.

Ein privater und ein öffentlicher Schlüssel bilden ein Schlüsselpaar. Eine Nachricht die mit Bobs öffentlichem Schlüssel verschlüsselt wurde kann nur mit seinem privatem Schlüssel entschlüsselt werden. Selbst Alice die die Nachricht verschlüsselt hat kann die Verschlüsselung nicht rückgängig machen, denn nur Bob kennt den privaten Schlüssel.



Dieses Verfahren wird fast überall verwendet wo ohne einen sicheren Kanal zum Passwtaustausch kommuniziert werden muss. Es ist auf den ersten Blick etwas kompliziert, funktioniert aber gut.

7.2 Verschlüsselte Kommunikation mit GPG4Win und Kleopatra (Win)

7.2.1 Installieren und eigene Schlüssel erstellen

1. GPG4Win¹ installieren (bei der Komponentenauswahl “Kleopatra” ausgewählt lassen)
2. “New Key Pair” klicken
3. Optional Name und Mail vergeben
4. “Create” klicken
5. Passwort vergeben (siehe dazu Kapitel „Passwort“)
6. Während der Erstellung die Maus zufällig über den Bildschirm bewegen (das benötigt der Algorithmus als Zufallswert, wir kennen das schon von VeraCrypt)

7.2.2 Eigenen öffentlichen Schlüssel rausfinden

Diesen kannst du anderen Leuten geben damit sie dir verschlüsselte Mails schreiben können 1. In Hauptfenster den neu erzeugten Eintrag klicken 2. “Export” klicken 3. Gesamten des Fensters kopieren 4. In einem Texteditor alle Zeilen die mit “Comment” beginnen entfernen, die Leerzeilen ebenso 5. Der restliche Text ist dein öffentlicher Schlüssel

7.2.3 Eine Nachricht verschlüsseln

1. Öffentlichen Schlüssel der Person der du schreiben willst in die Zwischenablage kopieren
2. In Kleopatra auf “Extras” - “Clipboard” - “Import Certificate” klicken
3. Auf “No” klicken
4. Auf “Notepad” wechseln und die Nachricht eingeben
5. Im Anschluss auf den anderen Tab wechseln

¹<https://www.gpg4win.org/>

6. Alle 3 Häkchen sollen aktiviert sein, die oberen sollen deinen eigenen Schlüssel enthalten, im unteren gibst du den die Empfängerin ein. (Deren Schlüssel haben wir vorhin importiert, der ist nun auf der Hauptseite zu finden)
7. "Sign/Encrypt Notepad" klicken
8. Passwort eingeben
9. Im Tab "Notepad" sollte jetzt etwas stehen was mit "BEGIN PGP MESSAGE" anfängt und mit "END PGP MESSAGE" aufhört
10. Kopiere den gesamten des Textfeldes und pack den in die E-Mail die du versenden willst. Die andere Person wird ihn entschlüsseln können

7.2.4 Eine Nachricht entschlüsseln

1. Empfangene Nachricht in die Zwischenablage kopieren
2. "Notepad" auswählen
3. Nachricht einfügen
4. "Decrypt Notepad" klicken
5. Wenn die Nachricht mit deinem öffentlichen Schlüssel erstellt wurde kannst du sie nun lesen

⚠ Fallstrick beim Verschlüsseln von E-Mails ⚠ Empfängerin und Betreff einer E-Mail werden nicht verschlüsselt werden. Wähle also einen neutralen Betreff der keinen Rückschluss auf den der Nachricht zulässt. Gegebenfalls sollten auch die E-Mail-Adressen der Kommunikationsteilnehmerinnen neutral sein, also frei von Hinweisen auf die reale Person.

Ja, das ist schon etwas umständlich. Falls du PGP öfters nutzen willst kannst du auch ein Plugin in deinem E-Mail Programm installieren. Im Folgenden ist das mal für Thunderbird erklärt, sowas gibt es aber für die meisten E-Mail Programme. Beachte aber auch, dass es etwas sicherer ist das stattdessen von Hand zu machen.

7.3 Verschlüsselte Kommunikation mit Thunderbird (Windows, Linux und MacOS)

Thunderbird nutzt ab der Version 78 einen eigenen Schlüsselbund, eventuell müssen Schlüssel aus PGP exportiert und in Thunderbird importiert werden, falls du vorher Enigmail genutzt hast

1. Thunderbird² installieren und mit deinem E-Mail-Konto verbinden
2. In den Konteneinstellungen unter "Ende-zu-Ende-Verschlüsselung" einen Schlüssel hinzufügen
3. Den Schlüssel in den Einstellungen auswählen
4. Schlüssel können über das Menü "Konten-Einstellungen -> Ende-zu-Ende-Verschlüsselung -> OpenPGP" importiert und exportiert werden.
5. Achte auch darauf, dass du die Schlüsselakzeptanz mindestens auf "Ja, aber ich habe nicht überprüft ob es sich im den korrekten Schlüssel handelt." gesetzt ist
6. An dich gerichtete verschlüsselte Nachrichten werden beim Empfang automatisch entschlüsselt
7. E-Mails die du schreibst sollten automatisch verschlüsselt werden, sofern du den entsprechenden öffentlichen Schlüssel importiert hast und dieser akzeptiert ist. Achte auf das Schloss-Symbol unten rechts.

7.4 Verschlüsselte Kommunikation mit GPG (Linux)

7.4.1 Eigene Schlüssel erstellen

1. gpg installieren (Paketverwaltung)
2. Im Terminal "gpg --gen-key" ausführen
3. Einen beliebigen Namen eingeben
4. Optional E-Mail eingeben
5. Mit "O" bestätigen
6. Optional Passphrase eingeben

²<https://www.thunderbird.net/de/>

7.4.2 Eigenen öffentlichen Schlüssel rausfinden

1. “gpg -armor -export NAME” im Terminal ausführen (Mit dem Namen der im vorherigen Schritt eingegeben wurde)
2. Schlüssel kopieren

7.4.3 Eine Nachricht verschlüsseln

1. Öffentlichen Schlüssel der Person der du schreiben willst in einer Textdatei speichern
2. “gpg -import DATEINAME” ausführen
3. Deine Nachricht in einer Textdatei speichern
4. “gpg -e -armor -r ADRESSE DATEINAME” dabei ist Adresse der Name oder die E-Mail Adresse die zu dem Schlüssel gehört den du gerade gespeichert hast
5. Im gleichen Verzeichnis sollte nun eine Datei mit der Endung .asc liegen, die enthält deine verschlüsselte Nachricht.

7.4.4 Eine Nachricht entschlüsseln

1. Verschlüsselte Nachricht in einer Datei speichern
2. “gpg -decrypt DATEINAME” ausführen

7.5 Android

Für E-Mail Verschlüsselung unter Android kann an dieser Stelle die Kombination aus K9-Mail³ und OpenKeychain⁴ wärmstens empfohlen werden. K9-Mail unterstützt die Kopplung mit OpenKeychain, zu finden in den Accounteinstellungen unter dem Punkt “Ende-zu-Ende-Verschlüsselung”. Nun kann in den Mails die Verschlüsselung durch das Schloss am oberen rechten Bildschirmrand eingeschaltet werden, sollten die jeweiligen

³<https://k9mail.app/>

⁴<https://www.openkeychain.org/>

Schlüssel hinterlegt sein. Dafür ist nichts weiter notwendig, als diese in der Openkeychain-App mittels Dateiimport, QR-Code oder Onlineschlüsselsuche hinzuzufügen. Zum Entschlüsseln darf der eigene Privatekey an dieser Stelle natürlich nicht fehlen.

7.6 PGP-Fingerprints

Während du Schlüssel erstellst oder importierst werden dir immer wieder die „Fingerprints“ der Schlüssel angezeigt. Was ist das eigentlich? Der Name „Fingerprint“ ist schon ziemlich sprechend. Jeder Schlüssel hat einen Fingerprint der nur zu diesem Schlüssel gehört. Wenn du einen Schlüssel aus dem Internet bekommst, zum Beispiel weil die Person ihn dir per Klartext E-Mail geschickt hat, dann kannst du dir nicht sicher sein ob das auch wirklich der richtige Schlüssel ist. Vielleicht hat auch eine Behörde die Leitung abgehört und den echten Schlüssel durch einen Schlüssel ersetzt mit dem sie das Gespräch mitlesen kann. Deswegen gibt es diesen kurzen Fingerprint. Du und die andere Person können über einen sicheren Kanal die Fingerprints vergleichen und so feststellen ob beide den richtigen Schlüssel haben, die Kommunikation also sicher ist. Das kann zum Beispiel bei einem Treffen in der echten Welt passieren, oder der Fingerprint kann in einer Zeitung abgedruckt worden sein. Wenn du den Fingerprint einfach nur per Mail bekommen hast oder auf der Website der anderen Person gefunden hast dann bringt das natürlich nichts. Dort könnte wieder jemand „auf der Leitung sitzen“ und den Fingerprint durch eine Fälschung austauschen.

Kapitel 8

Messenger

*

Wesentlich einfacher bedienbar als PGP/GPG sind Messenger. Einige davon haben mittlerweile eine Ende-Zu-Ende-Verschlüsselung, doch auch hier gibt es Unterschiede.

8.1 Bezugsquellen

Die sicherste **Bezugsquelle** ist der vorinstallierte App-Store deines Gerätes. Mehr dazu findest Du beim Thema Systemsicherheit.

8.2 Keine Anonymität

Beachte das Verschlüsselung dich **nicht automatisch anonym** macht. Keine der hier vorgestellten Apps hat das Ziel anonyme Kommunikation möglich zu machen. In der Praxis ist es zwar recht aufwendig, aber nicht unmöglich, mittels Überwachung eurer Anschlüsse fest zu stellen wer mit wem kommuniziert. Deshalb wichtig: Ende-Zu-Ende-Verschlüsselung schützt 'nur' den eurer Kommunikation, nicht wer mit wem und wann kommuniziert.

8.3 Nachrichten auf dem Sperrbildschirm

Die beste Verschlüsselung bringt wenig, wenn jeder einfach die ankommenden Nachrichten auf deinem Sperrbildschirm lesen kann. Stelle dein Smartphone deshalb so ein, dass die sogenannte 'Vorschau' nicht den Nachrichten-Text anzeigt.

8.4 Apps und Protokolle

8.4.1 Signal

Wenn du mit deinem Handy verschlüsselt kommunizieren willst ist Signal¹ der einfachste und sicherste Weg das zu erreichen. Alle Nachrichten, Anrufe und Video-Chats sind bei Signal Ende-Zu-Ende-verschlüsselt. Der Messenger wird von einer gemeinnützigen Organisation entwickelt und der Quelltext der Apps² ist öffentlich zugänglich. Um deine Kontakte zur erreichen benötigst Du aktuell aber noch deren Telefonnummer.

Menschen mit erhöhtem Schutzbedürfnis sollten von den zusätzlichen Möglichkeiten der App gebrauch machen: - Überprüfe bei Deinen Kontakten die Sicherheitsnummer. Die Cops registrieren regelmäßig vorhandene Accounts auf Ihren Geräten³ und greifen dann die Nachrichten statt des eigentlichen Kontakts ab oder lesen in Gruppen mit. Prüfe die Sicherheitsnummer auch und besonders wenn sich diese bei einem Kontakt ändert. Wenn nicht persönlich über den QR-Code, dann lest Euch die Nummer z. B. übers Telefon vor. Eine ausführliche Anleitung gibt es auf support.signal.org⁴. - Aktiviere die 'Registrierungssperre'⁵. Diese Funktion schützt dich vor der eben erwähnten Übernahme deines

¹<https://www.signal.org>

²<https://github.com/signalapp>

³<https://www.vice.com/de/article/435gbd/telegram-ueberwachung-bka-chat-app-verschluesslung>

⁴<https://support.signal.org/hc/de/articles/360007060632-Was-ist-eine-Sicherheitsnummer-und-weshalb-sehe-ich-dass-sie-sich-ge%A4ndert-hat->

⁵<https://support.signal.org/hc/de/articles/360007059792-Signal-PINs>

Accounts z. B. durch die Behörden. - Lange Signal-PIN⁶ wählen. Signal speichert einige deiner Daten (z. B. Profil, Gruppen und Kontakte) verschlüsselt auf Ihren Servern⁷. Für 'Oma Erna' bietet eine 4-stellig PIN ausreichend Schutz. Für Aktivist ist jedoch eine lange Passphrase sinnvoll. Falls Du auf Deinem Gerät einen Passwordmanager benutzt, dann verwende diesen für die Erzeugung und Speicherung eurer Signal-PIN. - Verschwindende Nachrichten⁸ nutzen. In der App kannst du auch einstellen, dass Nachrichten nach einiger Zeit, zum Beispiel nach einem Tag, automatisch gelöscht werden. So kann selbst im Falle einer Sicherstellung wenig gefunden werden. Stelle den Zeitraum möglichst kurz ein. - Besonders sensible Medien (Fotos und Videos) kannst Du auch so verschieben, dass diese nur einmal angesehen werden können⁹. - Aktiviere den 'Bildschirmschutz'¹⁰, innerhalb von Signal um Dich vor anderen Apps zu schützen, die den Bildschirminhalt versuchen mit zu lesen.

Signal gibt es auch für Android-Smartphones ohne Play Store¹¹ und für deinen PC¹².

8.4.2 Threema

Threema hat besonders im deutschsprachigen Raum eine recht große Verbreitung. Auch hier ist all eure Kommunikation Ende-zu-Ende verschlüsselt. Der Quelltext von Threema ist ebenfalls öffentlich zugänglich¹³. Trotzdem steht hinter dem Messenger eine Firma die von euch zur Nutzung einen einmaligen Betrag verlangt.

Aktuell größter Vorteil von Threema gegenüber der anderen gängigen Messengern ist die Tatsache, dass ihr nicht die Telefonnummer eures

⁶<https://support.signal.org/hc/de/articles/360007059792-Signal-PINs>

⁷<https://signal.org/blog/secure-value-recovery/>

⁸<https://support.signal.org/hc/de/articles/360007320771-Verschwindende-Nachrichten-festlegen-und-verwalten>

⁹<https://support.signal.org/hc/de/articles/360038443071-Einmalig-anzeigbare-Medien>

¹⁰<https://support.signal.org/hc/de/articles/360043469312-Bildschirmschutz>

¹¹<https://signal.org/android/apk/>

¹²<https://signal.org/de/download/>

¹³<https://github.com/threema-ch>

Kontaktes benötigt oder eures zum Betreiber hoch laden müsst. Zur Kontaktaufnahme genüg die Threema-ID¹⁴ des Gegenübers.

8.4.3 WhatsApp

WhatsApp nutzt seit ein paar Jahren¹⁵ die Ende-zu-Ende-Verschlüsselung von Signal. Trotzdem ist WhatsApp bei weitem nicht so sicher und vertrauenswürdig wie z. B. Signal. Deine Kommunikation ist zwar Ende-zu-Ende-verschlüsselt, aber Backups werden unverschlüsselt bei Apple bzw. Google gespeichert, wo sie abgerissen werden können. Zusätzlich wird euer komplettes Adressbuch im Klartext hochgeladen und von Facebook ausgewertet. Dein Profil, deine Gruppenmitgliedschaften und mehr werden außerdem im Klartext bei WhatsApp gespeichert.

Falls ihr nicht auf WhatsApp verzichten könnt, deaktiviert die Backups (und ratet das Euch Euren Kontakten). Sätzlich solltet ihr (wie bei Signal) die Sicherheitsnummern Eurer Kontakte überprüfen und die Benachrichtigung über eine Änderung der Nummer¹⁶ aktivieren. Aktiviert außerdem 2FA in den Einstellungen¹⁷.

8.4.4 Telegram

Telegram ist entgegen seines Rufes nicht zu empfehlen¹⁸. Die Chats sind nicht Ende-zu-Ende verschlüsselt, außer Du aktivierst es. Schlimmer noch, Telegram speichert die Nachrichten bei sich auf dem Server. Für Gruppen gibt es gar keine Verschlüsselung. Warum ein Anbieter für 'sichere' Kommunikation NutzerInnen so einem Risiko aussetzt ist nicht ganz klar. Daher sollte Telegram **nicht** genutzt werden.

¹⁴https://threema.ch/de/faq/threema_id

¹⁵<https://signal.org/blog/whatsapp-complete/>

¹⁶<https://faq.whatsapp.com/general/security-and-privacy/security-code-change-notification/?lang=de>

¹⁷<https://faq.whatsapp.com/general/security-and-privacy/account-security-tips/?lang=de>

¹⁸<https://gizmodo.com/why-you-should-stop-using-telegram-right-now-1782557415>

8.4.5 SMS

SMS Nachrichten solltest du, genau wie Telegram, **nicht** für deine Kommunikation nutzen. SMS haben keine Verschlüsselung und sind leicht ab zu hören.

8.4.6 Jabber/XMPP

Eine weitere Alternative ist das Protokoll Jabber/XMPP¹⁹ welches viele verteilte Server, statt eines Zentralen nutzt. Also im Prinzip so wie bei E-Mail. Leider gibt es verschiedene Apps mit unterschiedlichem Funktionsumfang, die wiederum unterschiedliche Arten der Verschlüsselung unterstützen. In der Praxis eine gute Methode für Anfänger um sich selbst ins Knie zu schießen. Zusätzlich funktioniert das alles auf Smartphones nicht reibungslos, besonders auf iPhones nicht. Falls Du doch einen Blick riskieren willst, dann nimm Conversations²⁰.

Pidgin, ein Programm das u. a. für Jabber/XMPP genutzt werden kann, gibt es ebenfalls für den PC und ist bei Tails²¹ bereits mit OTR für verschlüsselten Nachrichtenaustausch vorinstalliert. Was bei der manuellen Konfiguration von Pidgin zu beachten ist, z. B. Mitschnitte zu deaktivieren, erfährst du hier²².

8.4.7 Matrix

Matrix²³ ist ein weiteres Protokoll, dass ebenfalls über viele verteilte Server, statt einem zentralen funktioniert. Genauso wie bei Jabber/XMPP gibt es verschiedene Clients und die Möglichkeit der Ende-zu-Ende-Verschlüsselung. Wenn man auf stabil funktionierende Crypto Wert legt, sollte man sich

¹⁹<https://xmpp.org/software/clients.html>

²⁰<https://conversations.im/>

²¹https://github.com/beschlagnahmt-org/beschlagnahmt/blob/master/_posts/2000-01-01-190-anonym-im-netz.md#tails

²²<https://wiki.systemli.org/howto/jabber>

²³<https://matrix.org/>

momentan für Element²⁴ entscheiden, da sich bei den meisten anderen Apps die Ende-zu-Ende Verschlüsselung noch in einem experimentellen Zustand befindet.

²⁴<https://element.io/>

Kapitel 9

Telefonie

Genau wie SMS verfügen Festnetz- und Handy-Gespräche nicht über Ende-zu-Ende-Verschlüsselung¹, die vor mithören der Gespräche schützt. Es mag für eine Privatperson nicht ohne weiteres möglich sein ein Mobiltelefon abzuhören - so viel Crypto ist dann doch da - aber für staatliche Akteure oder deinen Mobilfunkanbieter ist das ganze kein Problem². Auch kommerzielle Anbieter von Internettelefonie wie Skype sind keine verlässliche Lösung. Allerdings kannst du mit den bereits erwähnten Apps 'Signal' oder 'Threema' Ende-zu-Ende-verschlüsselt über das Internet (Video-)telefonieren. Für Videokonferenzen, auch mit mehreren Teilnehmenden, ist ebenfalls Signal oder auch Jitsi³ eine Option. Jitsis Ende-zu-Ende-Verschlüsselung ist aber noch in der Erprobung⁴.

- △ Im aktivistischen Kontext ist von Telefonaten über Festnetz genau so abzuraten wie von Telefonaten mit dem Handy △

An dieser Stelle auch ein Hinweis zu alten Tastenhandys:

¹<https://de.wikipedia.org/wiki/Ende-zu-Ende-Verschl%C3%BCsselung>

²<https://de.wikipedia.org/wiki/Telekommunikations%C3%BCberwachung>

³<https://jitsi.org>

⁴<https://jitsi.org/blog/e2ee/>

Die Nutzung solcher Geräte kann durchaus Sinn machen. Bewegungsprofile können damit nicht so genau über Funkzellenabfragen erstellt werden, da sich die Geräte seltener mit dem Mobilfunknetz verbinden. Da die Geräte weniger Funktionen haben, liegen auch weniger Daten auf dem Gerät. Durch die weniger komplexen Betriebssysteme ist auch die Angriffsfläche deutlich geringer. Auf der anderen Seite ist es aber auch nicht möglich den des Geräts oder die getätigten Kommunikation zu verschlüsseln. Selbst die ohnehin unsichere Verschlüsselung durch das Mobilfunknetz ist bei diesen Geräten oft noch schlechter. Wenn du dir über diese Punkte bewusst bist und andere Vorteile für dich überwiegen, kannst du ein Tastenhandy nutzen. Ziehe jedoch nicht den Trugschluss, das Gerät wäre grundsätzlich sicherer nur weil es keinen großen Touchscreen hat.

Zivile Handfunkgeräte können über Verschlüsselung verfügen, in der Praxis ist das aber meistens nicht der Fall.

Kapitel 10

Passwörter

*

Ganz grob gesprochen werden Passwörter für 2 Zwecke verwendet, die aber auf den ersten Blick nicht für alle intuitiv unterscheidbar sind. Der Unterschied ist aber dennoch wichtig:

10.1 1. Daten entschlüsseln

Um ein verschlüsseltes Laufwerk oder eine verschlüsselte Datei zu entschlüsseln benötigst du ein Passwort. Damit eine Angreiferin (z.B. eine Ermittlungsbehörde oder ein Geheimdienst) dieses Passwort nicht durch schnelles ausprobieren aller möglichen Kombinationen erraten kann, muss es ausreichend lang sein. Gleichzeitig musst du diese Passwörter aber auswendig können, da es ein Fehler wäre, dieses auf einen Zettel zu notieren. Im Falle einer Durchsuchung hätten die Cops sonst leichtes Spiel beim Zugriff auf deine verschlüsselten Daten.

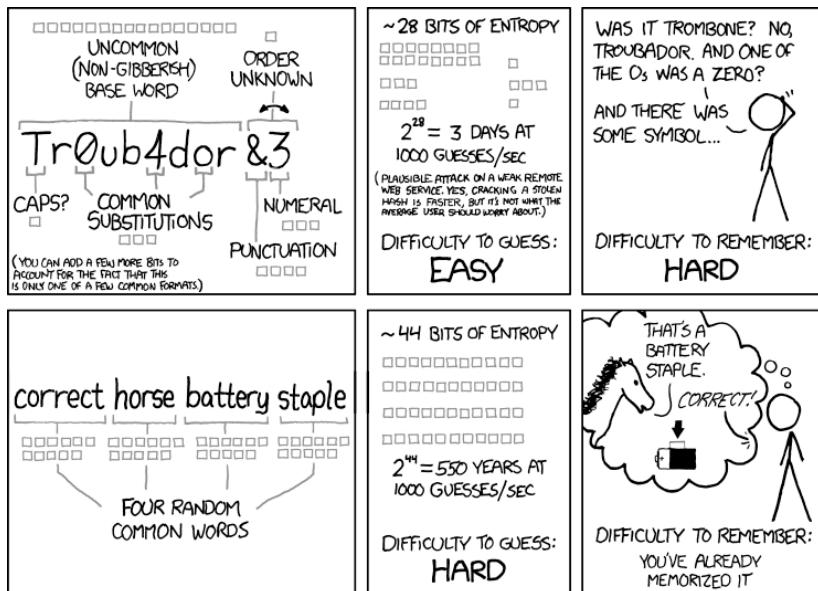
Also was machen?

Um ein solches sehr langes, aber dennoch vergleichsweise leicht zu merkendes Passwort zu generieren, hat sich ein Verfahren namens Di-

ceware¹ etabliert. Du lässt dir von einem Generator² mindestens **6** zufällige Wörter generieren, diese merkst Du Dir.

Wo anwenden?

Wie schon gesagt, dieses Verfahren nutzt du überall, wo es um Verschlüsselung von Daten geht. Das sind i.d.R. die Geräte-Verschlüsselung von deinem PC/Laptop, dein Passwortsafe, PGP-Key und verschlüsselte Container (z.B. von VeraCrypt). Die Anzahl der sogenannten Passphrasen, die du dir merken musst, sollte somit überschaubar sein.



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Achtung! Mindestens 6 Wörter verwenden!

¹<https://de.wikipedia.org/wiki/Diceware>

²<https://www.rempe.us/diceware/#german>

10.2 2. Anmeldung bei Diensten

Bei der Anmeldung bei Diensten (z.B. Webseiten) geht es nicht darum etwas zu entschlüsseln, sondern darum gegenüber den Dienst zu beweisen, dass Mensch ein gewisser Account gehört. Dieser Nachweis ist dein Passwort. Wichtig bei diesen Passwörtern ist deren Länge (damit diese niemand erraten kann) und deren Einzigartigkeit. Denn leider werden Diensten immer wieder mal die Passwort-Datenbanken geklaut und dann veröffentlicht. Ist dein Passwort in solch einer Liste und du hast es mehrfach verwendet, kann eine Angreiferin sich in all deine Accounts einloggen. Ob ein Passwort von dir schon mal veröffentlicht wurde, kannst du z.B. mit haveibeenpwned.com³ feststellen.

Natürlich kann sich keine:r zig verschiedene, elendig lange Passwörter merken. Deswegen gibt es sogenannte "Passwort-Manager" in denen du deine Passwörter abspeichern kannst. Eine Anleitung kannst du im Abschnitt "Passwort-Manager"⁴ finden.

10.3 Sonderfall Smartphones

Mit dem Entsperrpasswort bzw. der PIN deines Smartphones ist es eine etwas unangenehme Situation. Eigentlich könnte man hier eine kurze PIN nehmen, denn das Gerät verhindert ein schnelles Durchprobieren aller Möglichkeiten in dem es sich, bei mehreren Fehlversuchen, in immer längeren Abständen sperrt.

Aber, eine kurze PIN ist... - durch Fingerabdrücke auf dem Display⁵ leicht zu rekonstruieren - durch Überwachungskameras und andere Neugierige leicht ausspionierbar - Anfällig gegen Forensik-Geräte der Ermittlungsbehörden⁶, denn diese können oftmals Lücken in den Geräten nutzen und viele PINs automatisiert durchprobieren

³<https://haveibeenpwned.com/>

⁴[./passwort-manager/](#)

⁵<https://wifuture.de/news,57422.html>

⁶<https://www.cellebrite.com/de/>

Somit gilt: Gehe bei der Länge der PIN an deine absolute Schmerzgrenze der Praktibilität im Alltag! Besser wäre eine Passphrase, siehe oben.

Kapitel 11

Passwort-Manager

{: .no_toc }

*

Was bei einem Passwort wichtig ist haben wir erklärt und auch warum du bei jeden Dienst ein eizigartiges verwenden solltest. Um diese super sicheren Passwörter alle aufzubewahren brauchst du einen Passwort-Manager, außer du hast ein extrem gutes Gedächtnis. Da es bereits zu Datenlecks bei den kostenpflichtigen Anbietern kam, sollte die Wahl hierbei auf KeePassXC¹ fallen, denn die Anwendung ist Open Source, bewährt und nicht web-basiert. Wie du trotzdem die Vorzüge von Browser-integration und geräteübergreifender Synchronisation genießen kannst weiter unten.

11.1 Windows, Linux und MacOS

Das Prinzip ist denkbar einfach. Mensch lädt sich die Anwendung herunter, erstellt eine neue Datenbank, vergibt ein Hauptpasswort und kann damit beginnen, Logindaten für Webseiten und Dienste zu hinterlegen.

¹<https://keepassxc.org/>

Die Datenbank ist hierbei verschlüsselt. Das heißt: Solange niemensch dein Passwort knackt, bringt es der Person nichts im Besitz der Datei zu sein. Wichtig: Das Hauptpasswort wird selbstverständlich nicht in der Datenbank hinterlegt, du musst es dir also merken und es muss sicher sein. Wie Du ein möglichsts sicheres wählst, kannst du im Kapitel Passwörter² nachlesen. Solltest du nun einen neuen Eintrag in der Datenbank anlegen, kannst du dir ein zufälliges Passwort generieren lassen. Übernimm dieses bei das Passwortvergabe einfach in das Passwortfeld im Browser. Merken muss sich das zum Glück niemensch, du hast ja das Hauptpasswort.

11.1.1 Datenbank synchronisieren

Falls du bereits andere Passwortmanager genutzt hast, bist du in den Vorzug gekommen, auf mehreren Geräten auf deine Anmelddaten zugreifen zu können. Das können wir mit KeePassXC auch, vorausgesetzt du hast einen Cloudspeicher, auf dem du die Datenbank-Datei ablegen kannst. Verschiebe deinen Passwort-Safe einfach in ein Verzeichnis welche automatisch mit 'der Cloud' synchronisiert werden, wie z.B. Nextcloud oder auch Dropbox.

Wie wir bereits wissen ist es recht unbedenklich die Datenbank online zu lagern. Auch wenn auf deinen Cloudspeicher zugegriffen wird ist die Passwortdatenbank separat verschlüsselt.

11.1.2 Browser-Integration

Um die Bedienung über den Browser zu erleichtern gibt es für Firefox³ und Chrome⁴ das offizielle Addon "KeePassXC-Browser". Dieses kann Anmeldeformulare automatisch ausfüllen, Passwörter generieren oder Anmelddaten in der Datenbank ablegen.

² /passwort/

³ <https://addons.mozilla.org/en-US/firefox/addon/keepassxc-browser/>

⁴ <https://chrome.google.com/webstore/detail/keepassxc-browser/>

oboonakemofpalcgghocfoafidjkkk

1. Installiere KeePassXC-Browser
2. Aktiviere die Browser-Integration in den Einstellungen von KeePassXC
3. Wenn du ein Passwort eingibst bietet das Addon dir nun an es in KeePassXC zu speichern. Anders rum kannst du mit einem Knopfdruck gespeicherte Anmelddaten ausfüllen lassen, sofern du die zugehörige URL in jeweiligen Eintrag hinterlegt hast.

⚠ Tipp für zusätzliche Sicherheit ⚠ Schütze Deinen Passwort-Safe zusätzlich mit einem YubiKey / OnlyKey⁵, dann hast Du eine Two-Factor Authentication⁶. Das funktioniert auch in Verbindung mit den nachfolgend empfohlenen Smartphone-Apps.

11.2 Android und iOS

Auch für die beiden großen Smartphone Betriebssysteme gibt es kompatible Open Source Apps. Für Android empfehlen wir Keepass2Android⁷ und für iOS KeePassium⁸. Diese bieten grundsätzlich die gleiche Funktionalität wie KeePassXC, z.B. Synchronisation mit einem Online-Speicher und automatisches Befüllen von Anmeldeformularen.

⁵<https://keepassxc.org/docs/#faq-yubikey-howto>

⁶</two-factor-authentication/>

⁷<https://github.com/PhilippC/keepass2android>

⁸<https://keepassium.com/>

Kapitel 12

Glaubliche Abstreitbarkeit

Als Beschuldigte:r in einem Prozess kannst du dich auf dein Aussageverweigerungsrecht berufen um das Passwort geheim zu halten. Als Zeug:in wird das schon schwieriger. Mit der Argumentation dass du dich dadurch selbst belasten würdest und daher ebenfalls ein Aussageverweigerungsrecht hast, verrätst du möglicherweise mehr als dir lieb ist. Ein ähnliches Problem hast du wenn irgendwer versucht dir das Passwort mit Gewalt oder Erpressung zu entlocken. Für solche Fälle wurde das Konzept der "Glaublichen Abstreitbarkeit" oder "Plausible Deniability" entwickelt. Dein verschlüsselter Container oder dein verschlüsseltes System haben dabei zwei verschiedene Passwörter. Eines bringt dich in dein für schützenswerte Aktivitäten genutztes System, das andere in ein harmloses "Decoy-System" in dem keine sensiblen Daten gespeichert werden. Sollte nun irgendwer versuchen dich zur Herausgabe des Passworts zu zwingen kannst du einfach das Passwort für das Decoy-System nennen. Dein Gegenüber wird sich einloggen und das falsche System durchsuchen. Das noch mehr Daten existieren kann nicht erkannt werden. Die Software VeraCrypt die wir hier bereits angesehen haben unterstützt diese Funktion. Dort heißt das ganze „Hidden Volume“.



Um diese Funktion zu nutzen beginnst du mit einem unverschlüsselten System, installierst VeraCrypt wie zuvor beschrieben und verwendest dann die Funktion „Create Hidden Operating System“. Die optimale Größe der verschiedenen Partitionen sollte das Programm für dich aussuchen. Dann wird ein sogenanntes „Outer Volume“ erstellt. Dieses kannst du als weitere Sicherheitsebene betrachten, dein Decoy-System enthält nur harmlose Daten. Dein Outer-Volume enthält Daten die einen sensiblen Eindruck machen, die du aber preisgeben kannst falls du gezwungen werden sollst die versteckten Daten zu entschlüsseln. Der heiße Scheiß liegt stattdessen aber im Hidden-Volume, dessen Passwort du nie preisgibst. (Insgesamt gibt es also drei Passwörter.) VeraCrypt hat nun also das Outer-Volume erstellt und du befüllst es mit ein paar pseudosensiblen Daten. Das Programm wird dir sagen wie groß die Datenmenge sein darf, damit noch genug Platz für das Hidden-Volume ist in dem deine echten Geheimnisse aufbewahrt werden. Dieses wird im nächsten Schritt erstellt. Nun haben wir also ein Outer-Volume, ein Hidden-Volume und es fehlt nur noch das Decoy-System. Auf der Partition für das Decoy-System kannst du nun einfach eine neue Windows-Installation erstellen und diese mit der normalen Systemverschlüsselung von VeraCrypt verschlüsseln. Damit hast du dein Plausible-Deniability-System erfolgreich eingerichtet. Ja, das ist leider ziemlich kompliziert, kann dir aber in be-

stimmten Situationen von großem Nutzen sein. Weitere Informationen und Sicherheitshinweise findest auf der Seite von VeraCrypt. Eine Anleitung zu Plausible Deniability unter Linux findest du bei LinuxBrujo. Tricks wie diese können unter Umständen helfen dich in Verhörsituationen zu entlasten, aber selbstverständlich sind sie keine Garantie dass dein Gegeüber dir glaubt und ggf. auf die Anwendung von Gewalt verzichtet.

Links:

- Wikipedia - Gummischlauch-Kryptoanalyse¹
- VeraCrypt - Plausible Deniability²
- VeraCrypt - Hidden Operating System³
- LinuxBrujo - Plausible Deniability with LUKS⁴

¹https://de.wikipedia.org/wiki/Rubber-hose_cryptanalysis

²<https://www.veracrypt.fr/en/Plausible%20Deniability.html>

³<https://www.veracrypt.fr/en/VeraCrypt%20Hidden%20Operating%20System.html>

⁴<https://blog.linuxbrujo.net/posts/plausible-deniability-with-luks/>

Kapitel 13

Two-Factor Authentication

Deine Passwörter können aus verschiedenen Gründen dritten bekannt werden: - Eine Seite, auf der Du es benutzt hast wurde gehackt¹ - Dir hat irgendwer beim Eingeben über die Schulter geschaut² - Du hast als Passwort den Namenstag deiner Katze ausgewählt und irgendwer hat es geschafft das zu erraten³ - Dein Diensteanbieter wurde gezwungen das Passwort heraus zu geben⁴

Durch die, zuvor bereits erwähnte, Verwendung eines Passwortmanagers kannst du dich vor ein paar dieser Szenarien schützen.

Trotzdem macht “Two Factor Authentication” oder kurz “2FA” zusätzlich großen Sinn. Dabei installierst du z. B. eine App auf deinem Handy, die dir alle 30 Sekunden einen anderen kurzen Zahlencode anzeigt. Wenn du dich bei einem Dienst anmelden willst, bei dem Du 2FA aktiviert hast, gibst du nicht nur dein Passwort ein, sondern danach auch noch den Code von deinem Handy. Ohne den Code kommt keine:r rein, das Passwort alleine reicht nicht mehr. Es werden jetzt also zwei “Faktoren” ge-

¹<https://www.zeit.de/digital/datenschutz/2019-01/datenleak-email-passwoerter-internet-it-sicherheit>

²[https://en.wikipedia.org/wiki/Shoulder_surfing_\(computer_security\)](https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security))

³https://en.wikipedia.org/wiki/Brute-force_attack

⁴<https://netzpolitik.org/2020/bundesregierung-beschliesst-pflicht-zur-passwortherausgabe/>

prüft: Etwas das du weißt (das Passwort) und etwas das du besitzt (dein Handy mit der App).

Auf [twofactorauth.org⁵](https://twofactorauth.org) kannst du dich informieren, ob die Dienste die du nutzt 2FA anbieten und wie du es aktivieren kannst.

Eine weit verbreitete 2FA App ist "Authy⁶". Damit du nicht völlig aufgeschmissen bist falls du mal dein Handy verlierst, lagert Authy eine verschlüsselte Kopie deiner Datenbank auf deren Server. Diese kannst du von dort mit einem Passwort abrufen. Dieses Cloud-Backup ist trotzdem ein gewisses Risiko.

Eine alternative App ist 'andOTP⁷' (nur Android). Diese App speichert nichts in 'der Cloud⁸', du musst dich aber um die Backups selbst kümmern. Die App stellt dafür eine Möglichkeit bereit.

⁵<https://twofactorauth.org/>

⁶<https://www.authy.com/>

⁷<https://github.com/andOTP/andOTP>

⁸<https://fsfe.org/contribute/promopics/theresisnocloud-bluecolor-preview.png>

Kapitel 14

Phishing

Es klingt wie der billigste Trick der Welt, ist aber eine sehr verbreitete Methode um an fremde Zugangsdaten zu gelangen. Beim Phishing wird eine Seite perfekt nachgebildet und die Zielperson dazu gebracht sich auf der gefälschten Seite einzuloggen. Die Angreifer:innen können die Zugangsdaten dann lesen und sich auf der richtigen Seite einloggen. Die Nachbildungen können extrem realistisch sein, mit ein paar Tricks ist es sogar möglich, dass die Adresse genau gleich aussieht, zum Beispiel in dem Buchstaben aus dem kyrillischen Alphabet eingesetzt werden, die wie lateinische Buchstaben aussehen. Um sicher zu gehen bedenke immer, ob dich die Seite auf einem vertrauenswürdigen Weg erreicht hat oder ob dir irgendwer unter einem Vorwand einen Link geschickt hat, der dich zu dieser Login-Maske geführt hat. Am sichersten ist es wenn du Adressen immer selbst eintippst oder die Lesezeichenfunktion deines Browsers verwendest.



So

könnte eine Phishing Seite aussehen. Beachte die Auffälligkeiten die hier mit Kästen markiert sind.

Besonders weil die Behörden möglicherweise Spionage-Software auf deinem Rechner oder deinem Smartphone installieren wollen, solltest du darauf achten diese möglichst frei von Sicherheitslücken zu halten.

Daher hier nochmal ein paar Grundregeln: - Aktiviere automatische Updates. Ja, das kann nervig sein, aber ein gelegentlicher Neustart, wenn dies dir dein Gerät anzeigen, ist nichts gegen das stark erhöhte Risiko sich (staatliche) Schadsoftware ein zu fangen. Überprüfe auch Geräte wie z.B. deinen Router. - Nutze nur Geräte und Software, die noch mit Sicherheitsupdates versorgt werden. In Netz findest Du Informationen darüber wie lange Dein Windows¹, Linux, MacOS² oder iOS³ Sicherheitsupdates erhält. Bei Android-Smartphones ist es oft schwierig eine Aussage zu bekommen, ihr solltet aber kein Gerät benutzen, dessen Sicherheitspatch-

¹<https://support.microsoft.com/de-de/help/13853/windows-lifecycle-fact-sheet>

²<https://www.apple.com/de/macos/how-to-upgrade/>

³https://de.wikipedia.org/wiki/Versionsgeschichte_von_iOS#Aktuelle_Versionen

Level älter⁴ als 6 Monate ist. Vergiss auch hier nicht deine anderen Gerät z.B. deinen schon erwähnten Router. - Installiere nur Software aus vertrauenswürdigen Quellen. Neben den Webseiten der Entwickler:innen selbst, sind das der vorinstallierte App-Store Deines Betriebssystems. - Eine vertrauenswürdige Quelle bedeutet noch keine vertrauenswürdige Software. Frage dich immer ob du den Entwickler:innen vertrauen kannst, Open Source Software ist grundsätzlich vertrauenswürdiger. - Weniger ist mehr. Je weniger Software, Browser-Addons und Apps Du installiert hast, desto weniger Chancen hast du dir versehentlich Schadsoftware ein zu fangen. - Überlege dir welche Software-Tastatur du auf deinem Smartphone verwendest. Tastaturen von Drittanbietern können zwar praktisch sein, eine bösartige Tastatur kann aber die Nachrichten, die du in einem sicheren Messenger schreibst, abfangen bevor sie verschlüsselt werden. Auch die auf vielen Android-Geräten vorinstallierte Google-Tastatur 'GBoard' kann problematisch sein. Falls Du auf Nummer sicher gehen willst verwende OpenBoard⁵. - Nutze den Adblocker uBlock Origin⁶, denn Werbung ist nicht nur nervig, sondern kann auch ein Sicherheitsrisiko⁷ sein. - Klicke nicht auf Links in Messenger-Nachrichten von Unbekannten und in E-Mails. Gibt die URL händisch in deinen Browser ein oder nutze ein Lesezeichen. Es könnte sich um Phishing⁸ oder um einen Link zu Schadsoftware⁹ handeln. - Öffne keine E-Mail-Anhänge die du nicht erwartet hast, selbst wenn du glaubst den/die Absender:in zu kennen. Im Zweifelsfall ruf kurz an und frag, ob die Person dir wirklich etwas geschickt hat. - Schütze dein WLAN mit einer starken Passphrase (siehe Thema 'Passwörter'¹⁰), ändere zur Sicherheit das vom Hersteller voreingestellte Passwort. - Fahre deinen Rechner herunter anstatt ihn im Ruhezustand zu lassen, sonst lässt sich das Passwort deiner Plattenver-

⁴<https://www.tutonaut.de/android-version-und-sicherheitspatch-level herausfinden/>

⁵<https://github.com/dslul/openboard>

⁶<https://github.com/gorhill/uBlock/>

⁷<https://de.wikipedia.org/wiki/Malvertising>

⁸[phishing](#)

⁹https://www.vice.com/en_us/article/mbm5dp/human-rights-activist-allegedly-targeted-with-nso-malware-says-his-life-is-hellish

¹⁰[/passwort](#)

schlüsselung leicht auslesen. - Roote oder Jailbreak dein Smartphone nicht, du deaktivierst damit Sicherheitssysteme und verringest damit den Schutz vor Schadsoftware. - Surfe, wann immer möglich, über den Tor-Browser. Warum du das solltest findest du beim Thema Anonym im Netz¹¹. - Nutze keine gecrackte oder von Dritten manipulierte Software, diese kommt oft mit Schadsoftware.

Nur für Windows

- Lasse Windows Defender aktiviert
- Wenn du Microsoft Office benutzt: Deaktiviere die Makro-Funktion¹².

Weitere Tipps für Windows Nutzer:innen gibt es bei Decent Security¹³.

¹¹[/anonym-im-netz](#)

¹²https://www.vice.com/en_us/article/mbm5dp/human-rights-activist-allegedly-targeted-with-nso-malware-says-his-life-is-hellish

¹³<https://decentsecurity.com>

Kapitel 15

Anonym im Netz

*

Ganz grundlegend: Solltest du nicht wollen, dass ersichtlich ist was Du im Internet machst, musst Du einen Anonymisierungsdienst verwenden. Das Tool, welches Dir hierfür die besten Chancen bietet ist das 'Tor Netzwerk'. Es gibt noch andere Angebote die das selbe versprechen, diese sind aber entweder unsicherer (wie z. B. VPNs, mehr dazu weiter unten) oder weit weniger verbreitet (wie z. B. I2P¹ oder Freenet²) damit auch weniger von Fachleuten geprüft.

15.1 Tor

15.1.1 Funktionsweise

Bei der Verwendung von Tor wird dein Datenverkehr verschlüsselt über 3 Rechner (genannt Tor-Relays) freiwilliger BetreiberInnen umgeleitet, bis er dann vom Letzten an die von Dir aufgerufene Seite weitergeleitet

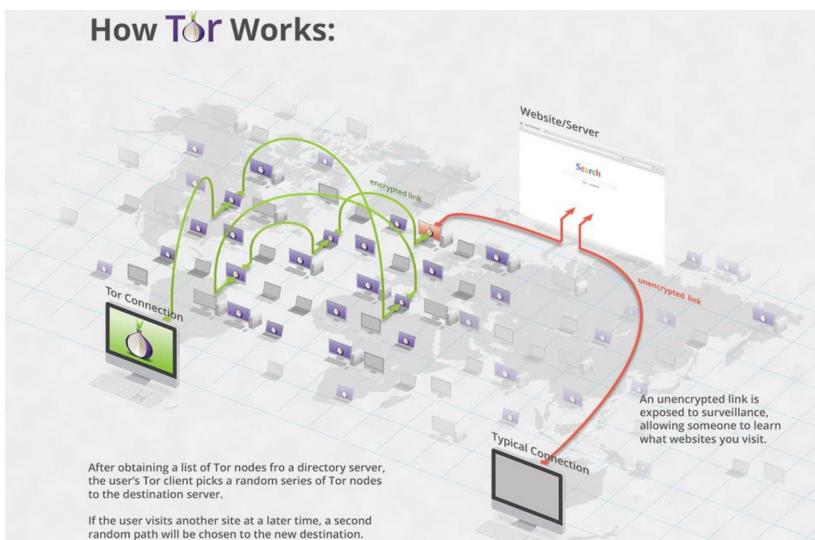
¹<https://geti2p.net/de/>

²<https://freenetproject.org/>

wird. Durch die Verwendung von diesen 3 Zwischenstationen ist sicher gestellt, dass niemand genug Informationen hat um die weitergeleitet Informationen Dir zu zu ordnen. Denn:

- Das erste Relay sieht nur, dass die Verbindung von dir kommt, aber nicht was über die Verbindung geht
- Das mittlere Relay sieht nur verschlüsselte Daten vom ersten Relay und gibt sie an ein anderes Relay weiter
- Das letzte Relay ('Exit-Relay') entschlüsselt und leitet nur Daten an die Zieladresse weiter, dessen Absender es aber nicht kennt

Das stellt den entscheidenden Vorteil gegenüber einem VPN dar, mehr dazu im Abschnitt zu VPNs.



Quelle: Edward Snowden auf Twitter³

³<https://twitter.com/Snowden/status/653587720598626304>

15.1.2 Tor Browser

Die einfachste Methode um Tor zu benutzen ist der Tor Browser⁴. Es gibt ihn so wohl für PCs, Android als auch für iOS⁵. Dieser ist ein angepasster Firefox, der jedoch den kompletten Verkehr durch das Tor Netzwerk leitet. Zusätzlich speichert der Browser selbst keine Daten dauerhaft auf deinem System. Die Verwendung des Tor Browser kann deinen Anonymität natürlich nicht gewährleisten, wenn Du auf den angesurften Seiten persönliche Daten preisgibst oder dich in rückverfolgbare Konten einloggst.

Grundsätzlich solltest du bedenken, dass mögliche Überwacher Deines Anschlusses sehen können dass du Tor benutzt. Ermittler bewerten verschlüsselten Datenverkehr, der bei Tor oder mit VPNs entsteht, in bösartiger Absicht gerne auch als "klandestines Verhalten" um weiteres "Futter" für ihre Ermittlungskonstruktionen zu haben. Allerdings, und das ist das wichtigste, können sie nicht sehen was du machst, denn die Verbindung ins Netzwerk ist verschlüsselt. Die Nutzung von Tor an sich macht dich nicht verdächtig, denn außer dir machen das alleine in Deutschland über 150.000 Menschen täglich⁶.

⚠ Wichtig ⚠

- Security Level⁷ mindestens 'Safer' besser 'Safest'
- Keine Addons installieren
- Einstellungen des Browsers nicht ändern

15.1.3 Betriebssysteme mit Tor-Integration

Um Deine Anonymität und IT-Sicherheit weiter ab zu sichern und Dich vor eigenen Fehlern zu bewaren gibt es zusätzlich spezielle Betriebs-

⁴<https://www.torproject.org/>

⁵<https://apps.apple.com/de/app/onion-browser/id519296448>

⁶<https://metrics.torproject.org/userstats-relay-country.html?country=de&events=off>

⁷<https://tb-manual.torproject.org/security-settings/>

systeme. Diese leiten wirklich allen Traffic über Tor und reden gar nicht auf andere Weise überhaupt mit dem Internet.

Tails

Tails⁸ kannst du dir herunterladen, mit dem mitgelieferten Installer auf einen USB-Stick übertragen und dann als sogenanntes "Live-System" auf deinem Rechner starten. Dazu steckst du den Stick ein und startest deinen Computer neu. Wenn während dem Start eine Meldung wie "Press F12 for Boot Menu" oder so ähnlich auftaucht drücke die entsprechende Taste und wähle im folgenden Menü deinen USB-Stick aus. Nun wird anstelle deines normalen Betriebssystems Tails gestartet werden. Wenn du fertig bist kannst du den Rechner herunterfahren und den USB-Stick entfernen, dann ist alles wieder beim Alten. Das ganze hat einen Aspekt der gleichzeitig Vor- und Nachteil ist: In Tails kannst du üblicherweise keine Daten dauerhaft speichern. Nach dem Herunterfahren ist alles verschwunden.

Wenn du mehr zu Tails wissen willst lies die offizielle Doku⁹ oder Capulcu über Tails (PDF)¹⁰ dazu. Letzere legt einen sehr hohen Sicherheitsstandard vor, der wahrscheinlich für viele nicht immer praktikabel ist, enthält aber definitiv eine Menge wertvoller Tipps.

Whonix

Whonix¹¹ funktioniert etwas anders als Tails. Für Whonix installierst du dir z. B. die Software VirtualBox mit der du virtuelle Maschinen betreiben kannst. Das ist quasi ein simulierter Computer der auf deinem richtigen Computer läuft. Dann lädst du dir die Whonix Images herunter und importierst diese in VirtualBox. Ja, richtig gehört, es sind zwei Images. Eins

⁸<https://tails.boum.org/>

⁹<https://tails.boum.org/doc/index.de.html>

¹⁰<https://capulcu.blackblogs.org/wp-content/uploads/sites/54/2019/01/Tails2019-01-27-A4.pdf>

¹¹<https://www.whonix.org/>

davon ist das Whonix-Gateway welches die Verbindung mit dem Internet aufbaut und dafür sorgt das alles nur über Tor geleitet wird. Das andere ist die Whonix-Workstation. Die benutzt du um deine Arbeit zu machen. Alles was innerhalb der Workstation passiert wird über Tor geleitet werden. Dort kannst du auch Dinge speichern, denke also daran das Host-System auf dem die beiden virtuellen Maschinen laufen komplett zu verschlüsseln. Du weißt ja jetzt wie das geht.

Bedenke, dass du bei Whonix kein „amnesisches“ System hast, also auch Spuren hinterlässt. Nutze Whonix daher nur auf verschlüsselten Geräten.

Qubes OS

Falls du schon etwas mehr technische Erfahrung hast und mit der Sicherheit mal so richtig auf die Kacke hauen willst, dann schau dir das Betriebssystem Qubes OS¹² an. Dieses arbeitet mit mehreren virtuellen Maschinen und bietet neben vielen anderen Sicherheits-Features auch eine Integration von Whonix an. Qubes OS läuft nicht auf jedem Rechner, daher lohnt vorab der Blick auf deren Liste der unterstützten Hardware¹³.

15.2 VPN

Ein VPN (Virtual Private Network) funktioniert technisch ähnlich wie Tor, hat aber einen entscheidenden Nachteil: Dein Internetverkehr wird nur an *eine einzige* Zwischeninstanz verschlüsselt übermittelt, nämlich den VPN-Provider. Das bedeutet: Du bist darauf angewiesen, dass dieser Anbieter nicht speichert, wer seine Nutzenden sind und welche Seiten diese aufrufen. Da dies nicht gewährleistet werden kann, solltest Du kei-

¹²<https://www.qubes-os.org/>

¹³<https://www.qubes-os.org/hcl/>

ne¹⁴ VPNs nutzen¹⁵. Denn die Anbieter müssen auf gerichtliche Anordnung diese Daten heraus geben und machen das auch¹⁶.



¹⁴<https://gist.github.com/joepie91/5a9909939e6ce7d09e29>

¹⁵<https://schub.wtf/blog/2019/04/08/very-precarious-narrative.html>

¹⁶https://www.theregister.com/2011/09/26/hidemyass_lulzsec_controversy/

Kapitel 16

IMSI Catcher und Stille SMS

Warum wird denn eigentlich immer dazu geraten zu Demos und Aktionen nur Zweithandys mitzunehmen?

Klar, die Cops können dir eventuell dein Haupthandy wegnehmen und Daten davon gewinnen. Doch es gibt noch andere Risiken, für die du das Handy nichtmal aus der Tasche genommen haben musst. Immer wieder kommt es vor das im Umfeld von Demos IMSI-Catcher aufgestellt werden. (Es ist möglich diese mit spezieller Software wie SnoopSnitch, Darshak oder AIMSICD zu erkennen.) IMSI-Catcher tun so als wären sie eine normale Basisstation im Handynetz und überreden Geräte in ihrem Umfeld dazu sich dort einzubuchen. Damit können die Cops feststellen welche Handynummern gerade in der Umgebung sind und so die anwesenden Personen feststellen. Mit dem Gerät können auch Telefonate abgehört werden. Dazu leitet der IMSI-Catcher das Gespräch mit seiner eigenen Nummer weiter. Wird der Catcher nicht in diesem Abhörmodus betrieben sind für die Personen im Umfeld oft Anrufe komplett blockiert. Das gilt auch für Notrufe. Aus diesem Grund ist es so wichtig ein Demo-Handy mit einer anonymen SIM-Karte¹ zu benutzen. Falls du Probleme hast eine anonyme SIM-Karte zu besorgen kann dir viel-

¹https://prepaid-data-sim-card.fandom.com/wiki/Registration_Policies_Per_Country#Europe

leicht die Gruppe Aktionssim² weiterhelfen. Tust du das nicht kann deine Nummer mit dem IMSI-Catcher ermittelt werden und die Cops müssen nur noch kurz beim Handyprovider anrufen um deinen Namen und deine Adresse herauszufinden. Somit haben sie einen eindeutigen Beweis, dass du auf der Demo anwesend warst. Eine weitere Methode ist die Funkzellenabfrage, dabei sparen die Behörden sich die Arbeit mit dem IMSI-Catcher und gehen direkt zu den Betreibern der Funkzellen und lassen sich von denen eine Liste aller eingebuchten Nummern geben. Auch hier sind Fälle bekannt geworden bei denen das Verfahren auf Demos eingesetzt wurde. In Berlin gibt es mittlerweile ein "Funkzellenabfragen-Transparenz-System³" mithilfe dessen du dich nach Abschluss der Ermittlungen benachrichtigen lassen kannst, falls du betroffen bist. In anderen Bundesländern gibt es das bisher noch nicht. Eine Ergänzung zur Funkzellenabfrage ist die sogenannte "Stille SMS", diese wird benutzt wenn die Cops deine Nummer haben und wissen wollen wo du gerade bist. Dazu senden sie eine spezielle SMS an dein Gerät welche dir nicht angezeigt wird. Du merkst von der ganzen Sache also gar nichts, dabei antwortet dein Handy aber der Funkzelle in die du gerade eingebucht bist. Dadurch lässt sich sehr einfach dein Aufenthaltsort herausfinden. Das Bundesamt für Verfassungsschutz versendete im ersten Halbjahr 2018 ganze 103.224 stille SMS, das BKA 30.988 und die Bundespolizei 50.654. Die Landesbehörden für Verfassungsschutz und die Polizeien der Bundesländer nutzen das Verfahren ebenfalls reichlich. Es ist von deutlich mehr als einer Millionen Ortungen pro Jahr auszugehen. Stille SMS können mit der bereits erwähnten App SnoopSnitch sichtbar gemacht werden.

²<https://aktionssim.blackblogs.org/>

³<https://fts.berlin.de/>



Bild: Ein IMSI-Catcher, Creative Commons BY-NC-SA 2.5 Canada. BC Civil Liberties Association

⚠ Fallstrick beim Demo-Handy ⚠

Wenn du dir ein sauberes Handy und eine anonyme Nummer besorgt hast schalte das Gerät niemals bei dir Zuhause oder an Orten an denen du dich oft aufhältst an. Damit wäre die Nummer und das Handy nicht mehr anonym. Schalte es erst an wenn du am Ort der Aktion bist. Lege die SIM-Karte nie in dein normales Handy (und andersrum). Schalte Aktionshandy und normales Handy nie am gleichen Ort ein. Überlege dir auch immer mal wieder die Nummer zu wechseln.

Links:

- Wikipedia - IMSI-Catcher⁴

⁴<https://de.wikipedia.org/wiki/IMSI-Catcher>

- SnoopSnitch⁵
- Darshak⁶
- AIMSIDC⁷
- Berliner Transparenzsystem⁸
- Wikipedia - Stille SMS⁹
- Statistik Stille SMS¹⁰

⁵<https://opensource.srlabs.de/projects/snoopsnitch>

⁶<https://github.com/darshakframework/darshak>

⁷<https://cellularprivacy.github.io/Android-IMI-Catcher-Detector/>

⁸<https://fts.berlin.de/>

⁹https://de.wikipedia.org/wiki/Stille_SMS

¹⁰<https://netzpolitik.org/2018/halbjahreswerte-fuer-stille-sms-imsi-catcher-und-funkzellenabfragen/>

Kapitel 17

OpSec

Das Wort “Opsec” steht für “Operations security” und bezeichnet eine Reihe von Vorgehensweisen um den Gegnern kritische Informationen vorzuenthalten. Ein Teil davon sind technische Maßnahmen wie sie hier beschrieben wurden, ein zweiter sehr wichtiger Teil sind Verhaltensregeln. Mache dir bewusst welche Informationen du geheim halten möchtest und wer sich für diese interessieren könnte. Rede nicht mit der Polizei, auch nicht wenn du glaubst clever zu sein und sie mit Lügen täuschen zu können. Auch Lügen können wichtige Informationen enthalten.

Vermeide es im Kontext von Aktionen Fotos oder Videos zu machen. Wenn es nicht anders geht denke daran das Material akribisch nach Details zu durchsuchen. Verpixele Gesichter, Markenlogos auf Kleidung, Schuhe, Gebäude im Hintergrund, Stromleitungen, persönliche Gegenstände und so weiter. Selbst die individuelle Gangart einer Person kann durch die Ganganalyse¹ dabei helfen Personen zu identifizieren. Prüfe auch ob dein Handy Standortdaten im Bild speichert und bereinige diese gegebenenfalls. Bei vielen Geräten ist das Speichern von Standortdaten die Standardeinstellung, vergiss diesen Schritt also auf keinen Fall. Du kannst auf Android dafür zum Beispiel die App „Scrambled Exif“ benutzen.

¹<https://de.wikipedia.org/wiki/Ganganalyse>

²<https://gitlab.com/juanitobananas/scrambled-exif>

zen.

Poste nicht in sozialen Netzwerken über deine Erlebnisse. Prahle niemals damit welchen Gruppen du angehörst, wen du kennst oder bei welchen Aktionen du dabei warst. Gehe nach einer Aktion nicht auf direktem Weg nach Hause sondern mach ruhig mal einen Umweg. Verwende während Aktionen Decknamen und Codes. Wenn nötig trage bei Aktionen Handschuhe. Bedenke auch das menschliche Körper echte Dreckschleudern sind und bei jeder Gelegenheit DNA hinterlassen. Bedenke, dass in der Öffentlichkeit überall Kameras sind, zum Beispiel an Bahnhöfen, im Umfeld von Geschäften und Kiosks und an Polizeiwachen. Software zur Gesichtserkennung ist keine Zukunftsmusik mehr und wird bereits überall auf der Welt eingesetzt, also bedecke wenn möglich dein Gesicht. Wenn du nicht alle Tipps zur Nutzung von Demohandys akribisch befolgt hast dann lasse dein Handy am besten zuhause.

Wenn du im Internet Anonymisierungstechnologie nutzt denke daran deine Identitäten voneinander zu trennen und nicht im anonymen Kontext Dinge zu schreiben oder Logins zu nutzen die dich deanonymisieren. Wenn du diese nutzen willst dann wechsel den Kontext, zum Beispiel indem du im Tor Browser auf „New Identity“ klickst oder das VPN wechselt.

Vergiss nicht das heutzutage fast jedes Telefon ein kleiner Computer mit Mikrofon ist. Bei privaten Gesprächen schalte das Gerät aus. Am besten nimmst du den Akku raus oder lagerst es irgendwo außer Hörweite. Bedenke bei Gesprächen auch das es in Autos³, Cafés, Restaurants, Kneipen und an vielen anderen Orten unerwünschte Zuhörer geben kann.

Das sind alles keine komplizierten Tipps, aber sie alle zu beachten ist nicht immer leicht, Reden macht nunmal Spaß. Bitte denke daran das diese Verhaltensregeln dich vor dem Knast bewahren können.

³<https://kontrapolis.info/823/>

```
[+] Tinder: Not Found!
[+] Telegram: Not Found!
[+] TradingView: Not Found!
[+] Trakt: Not Found!
[+] TrashboxRU: Not Found!
[+] Trello: Not Found!
[+] Typora: Not Found!
[+] Twitch: Not Found!
[+] Twitter: https://www.twitter.com/anonymaus1312
[+] Typeracer: Not Found!
[+] Ultimatum: Not Found!
[+] Utzschash: Not Found!
[+] VK: Not Found!
[+] VSCO: Not Found!
[+] Velonmania: Not Found!
[+] Vimeo: Not Found!
[+] Vladi: Not Found!
[+] Vimeo: Not Found!
[+] Virgpool: Not Found!
[+] VirusTotal: Not Found!
[+] WebHDFS: Not Found!
[+] We Heart It: Not Found!
[+] Webknode: Not Found!
[+] Whonix Forum: Not Found!
[+] WikiLeaks: Not Found!
[+] Wikipedia: Not Found!
[+] Wix: Not Found!
[+] WordPress: Not Found!
```

Software “sherlock” zum Aufspüren von Accounts in sozialen Netzwerken

Links:

- The Paddy Factor⁴
- Codes, What Are They Good For?⁵
- RHZ 2018/4 Schwerpunkt Tipps für Aktivismus (PDF)⁶

⁴<https://grugq.github.io/blog/2013/03/18/the-paddy-factor/>

⁵<https://grugq.github.io/blog/2013/12/21/codes-what-are-they-good-for/>

⁶<https://rote-hilfe.de/rote-hilfe-zeitung/heftarchiv?download=187:rote-hilfe-zeitung-4-2018>

Kapitel 18

Dienste und Anbieter

Hier wurde nun öfters erwähnt wie viel Vertrauen du den Menschen gegenüber bringen musst die zum Beispiel deinen Mailserver oder dein VPN betreiben. Um die Auswahl etwas leichter zu machen ist hier eine kleine Liste mit Anbietern. Recherchiere aber auch nochmal selbst wer am besten zu dir passt und trifft dann deine eigene Entscheidung.

(€) = Kostenpflichtig

(Inv) = Nur auf persönliche Anfrage oder Einladung

18.1 Mail

- Posteo¹ (€)
- Mailbox² (€)
- Riseup³ (Inv)
- Autistici⁴ (Inv)
- Systemausfall⁵ (Inv)

¹<https://posteo.de>

²<https://mailbox.org>

³<https://riseup.net>

⁴<https://autistici.org>

⁵<https://systemausfall.org>

- Systemli⁶ (Inv)
- so36⁷ (Inv)
- Anonymous Speech⁸ (€)
- Immerda⁹ (Inv)
- Dismail¹⁰ (XMPP Anmeldung)
- Disroot¹¹ (Free)
- Snopyta¹² (Free)

18.2 Matrix

- systemli.org¹³
- systemausfall.org¹⁴ (Inv)

18.3 Jabber/XMPP

- riseup.net¹⁵ (Inv)
- systemli.org¹⁶
- systemausfall.org¹⁷ (Inv)
- so36.net¹⁸ (Inv)

⁶<https://systemli.org>

⁷<https://so36.net>

⁸<https://anonymousspeech.com>

⁹<https://immerda.ch>

¹⁰<https://dismail.de>

¹¹<https://disroot.org>

¹²<https://snopyta.org>

¹³<https://systemli.org/service/matrix/>

¹⁴<https://systemausfall.org/dienste/matrix>

¹⁵<https://riseup.net>

¹⁶<https://systemli.org/service/xmpp/>

¹⁷<https://systemausfall.org>

¹⁸<https://so36.net>

18.4 Jitsi Meet

- meet.jit.si¹⁹ (Unterstützt E2E-Verschlüsselung)
- jitsi.rocks²⁰
- talk.snopyta.org²¹
- meet.systemli.org²²

18.5 BigBlueButton

- meeten.statt-drosseln.de²³
- senfcall.de²⁴
- bbb.daten.reisen/b²⁵

18.6 DNS

- Digitalcourage e.V.²⁶

Eine ausführliche Liste von Software und Anbietern findest du bei PrismBreak²⁷ und PrivacyTools²⁸.

¹⁹ <https://meet.jit.si>

²⁰ <https://jitsi.rocks>

²¹ <https://talk.snopyta.org>

²² <https://meet.systemli.org/>

²³ <https://meeten.statt-drosseln.de>

²⁴ <https://senfcall.de>

²⁵ <https://bbb.daten.reisen/b>

²⁶ <https://digitalcourage.de/support/zensurfreier-dns-server>

²⁷ <https://prism-break.org/de/>

²⁸ <https://www.privacytools.io/>

Kapitel 19

Resümee

Das wars. Hoffentlich konnte dir diese Seite helfen. Beachte aber das hier bei weitem nicht alles abgedeckt wurde, es handelt sich eher um einen Rundumschlag um auf einen halbwegs ordentlichen Sicherheitsstandard zu kommen. Wenn du einen Fehler gefunden oder einen Verbesserungsvorschlag hast, lass es uns wissen¹. Gerne kannst du direkt auf Github einen Verbesserungsvorschlag einreichen². Sollte dir das zu öffentlich sein, melde dich gerne per Mail³.

Falls du noch mehr zum Thema lesen willst empfehlen sich unter anderem die Kolumne „Get Connected“ der Datenschutzgruppe der RH Heidelberg⁴ und die Texte der Gruppe Capulcu⁵. Außerdem kannst du auf privacy-handbuch.de⁶ noch eine Menge detaillierterer Informationen zu Anonymisierung, Verschlüsselung und Schutz vor Tracking nachlesen. Viele weitere Anleitungen zum Thema in verschiedenen Sprachen findest du außerdem beim Projekt Surveillance Self-Defense⁷ der EFF.

¹<https://github.com/beschlagnahmt-org/beschlagnahmt/issues>

²<https://github.com/beschlagnahmt-org/beschlagnahmt/pulls>

³[/kontakt](#)

⁴<https://datenschutz.de/gc/>

⁵<https://capulcu.blackblogs.org/>

⁶<https://privacy-handbuch.de>

⁷<https://ssd.eff.org/>

Vielen Dank an alle die bei der Erstellung des Hefts und der Seite mitgeholfen haben und an alle die Ergänzungen einsenden und kommentieren. Solidarische Grüße an alle emanzipatorischen Gruppen und Einzelpersonen im Netz und in der analogen Welt.

