

Digitale Selbstverteidigung

10 Möglichkeiten, wie Sie sich und Ihre Daten schützen können

Digitales Handout zum Vortrag zu Digitaler Selbstverteidigung

09.09.2020, BayernLab Traunstein

Referent: Stefan Mey, Freier Journalist, Berlin

Ich wünsche Ihnen viel Spaß bei der technischen Verteidigung ihres digitalen Lebens. Die Links, die Anweisungen und die Programme habe ich sorgfältig geprüft. Was Sie damit machen, unterliegt aber natürlich Ihrer eigenen Verantwortung.

Gliederung

- (1) Sichere Passwörter erzeugen
- (2) Passwortmanager (KeepassXC)
- (3) Spuren-arm surfen (Firefox)
- (4) Anonym und Zensur-frei surfen (Tor-Browser)
- (5) E-Mail-Programm nutzen (Thunderbird)
- (6) E-Mails verschlüsseln (OpenPGP/Thunderbird)
- (7) Smartphone-Datenflüsse einschränken
- (8) Gute Messenger nutzen (Threema, Signal, Briar)
- (9) Texte verschlüsseln (LibreOffice)
- (10) Alternative PC-Betriebssysteme (Linux Mint oder Linux Ubuntu)

(1) Sichere und merkbare Passwörter erzeugen

Nonsense-Satz-Methode: Sie denken sich einen unsinnigen, absurden oder lustigen Satz aus. Die Anfangsbuchstaben der Wörter bzw. die Zahlen, Satzzeichen und Sonderzeichen ergeben Ihr Passwort. Mein Beispielsatz war: „**Ein ganzes Brot kostet weniger als zwei halbe Brötchen, oder?**“. Daraus leite ich folgendes Passwort ab: **1gBkwa2/2B,o?** . Das Passwort sollte aus mindestens 13 Elementen bestehen und Großbuchstaben, Kleinbuchstaben, Zahlen sowie Satz/Sonderzeichen enthalten.

Zusatz-Tipp: Sie können die Methode auch noch „würzen“, sprich mit eigenen Regeln versehen. Zum Beispiel können Sie sich sagen, dass Sie bei all Ihren Passwörtern jeweils beim dritten Wort nicht den Anfangsbuchstaben, sondern das komplette Wort schreiben. In unserem Fall würde das Passwort dann lauten: **1gBrotkwa2/2B,o?**

(2) Passwortverwaltung mit KeyPassXC (PC)

- Passwortmanager KeePassXC: <https://keepassxc.org/download>
- gute Anleitung: https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/dossiers/sicherheit/keepass/1_installation/index.html. (Die Anleitung bezieht sich auf KeePass. KeePassXC ist eine Abwandlung dieses Ursprungsprogramms, weil KeyPass leider nicht für Mac-Geräte verfügbar ist. Die Logik der beiden Schwesterprogramme ist aber identisch, deswegen hilft die Anleitung auch beim Verständnis von KeyPassXC).
- Anmerkungen zum Download-Prozess: Beim Download von KeePassXC gibt es zwei kleine Tücken ... Windows: Klicken Sie auf das Windows-Symbol. Es gibt zwei unterschiedliche Pakete für 64-Bit und 32-Bit-Systeme. Die meisten Windows-PCs haben 64 Bit. Den Bit-Typen Ihres PCs ermitteln Sie folgendermaßen: klicken Sie auf das Windows-Feld rechts unten auf Ihrem Bildschirm → dann auf das Zahnrad-Symbol, es öffnet sich das Einstellungsmenü → auf „System“ klicken → dann in der linken Spalte auf „Info“, dann sehen Sie in der Zeile „Systemtyp“ die Bit-Angabe. Klicken Sie dann auf der KeePassXC-Webseite auf das Feld „MSI Installer“, für Ihre 64-Bit bzw. 32-Bit-Version. ... Mac: Klicken Sie auf das Apple-Symbol und auf das Feld Binary Bundle, passend zu Ihrer Mac-Version (macOS 10.13+ oder macOS 10.12 "Sierra").
- Passwortmanager auf dem Smartphone: Empfehlenswert ist für Android die App Keepass2Android und für iOS die App KeePassium. Für KeePass2Android gibt es eine gute Anleitung: <https://mobilsicher.de/ratgeber/so-gehts-passwort-manager-keepass2android-nutzen>.

(3) Spuren-arm surfen mit Firefox

- Download unter <https://www.mozilla.org/de/firefox/new>
- Funktion Privater Modus: Navigationspfad: klicken Sie auf das Burger-Menü (Drei-Striche-Symbol rechts oben im Browser) - Neues Privates Fenster (s. <https://support.mozilla.org/de/kb/privater-modus>)
- Cookies mit Schließen des Browsers löschen, Navigationspfad: Burger-Menü – Einstellungen – Datenschutz & Sicherheit - „Cookies und Website-Daten beim Beenden von Firefox löschen“ anklicken
- Erweiterung „Firefox Multi-Account Containers“: Installation über folgenden Navigationspfad: Burger-Menü – Addons – Erweiterungen – Name eingeben – Zu Firefox hinzufügen (Direkt-Link zum Addon: <https://addons.mozilla.org/de/firefox/addon/multi-account-containers>).
- Firefox gibt es auch auf dem Smartphone, s. <https://www.mozilla.org/de/firefox/mobile/>. Allerdings funktioniert ist die Erweiterung Multi-Account Contains-Addon in den Browser-Apps leider nicht verfügbar.

- Achtung: Die Erweiterung „Firefox Multi-Account Containers“ stellt die Firefox-Mutterorganisation Mozilla direkt. Prinzipiell sollten Sie allerdings zurückhaltend bei der Installation von Addons sein. Es gibt Addons, die sich über den Verkauf von Daten finanzieren. Ein auf den ersten Blick nützliches Addon, das Ihnen eine verbesserte Browser-Darstellung oder das Ausblenden von störender Werbung verspricht, kann faktisch zur Schadware im Browser werden und seinerseits Daten über Sie ausleiten. Von Mozilla geprüfte Addons sind mit einem orangefarbenen „Empfohlen“-Symbol gekennzeichnet.

(4) Anonym und Zensur-frei surfen mit dem Tor-Browser

- Download unter: <https://www.torproject.org/de>
- allgemeines „Benutzerhandbuch“ des Tor Projects: <https://tb-manual.torproject.org/de>
- Wenn Sie auf das grüne Schloss links neben dem Adressfeld klicken, sehen Sie die Tor-Verschleierungs-Route. Über das Feld „Neuer Kanal für diese Seite“ können Sie sich eine neue Route erzeugen lassen.
- Tor auf dem Smartphone: In den App-Stores werden viele angebliche Tor-Browser-Apps angeboten. Zu empfehlen sind nur folgende zwei Apps:
 - (Android) Tor Browser for Android: <https://play.google.com/store/apps/details?id=org.torproject.torbrowser&hl=de>
 - (iOS) OnionBrowser von Mike Tigas: <https://itunes.apple.com/de/app/onion-browser/id519296448?mt=8>
- Im Vergleich mit PCs sind Smartphones erheblich größere Datenschleudern. Wenn es Ihnen um Anonymität geht, sollten Sie Tor deshalb lieber auf dem PC nutzen.

(5) E-Mail-Programm nutzen (Thunderbird)

- Download unter <https://www.thunderbird.net/de>
- Anleitung von Thunderbird: <https://support.mozilla.org/de/kb/automatisch-konto-konfigurieren>
- Die gängigen E-Mail-Anbieter haben oft auch Erklärtex te zur Einrichtung von Thunderbird geschrieben, z.B.: <https://www.telekom.de/hilfe/festnetz-internet-tv/e-mail/e-mail-konto/e-mail-adresse-t-online.de-in-mozilla-thunderbird-einrichten> (T-online), <https://hilfe.web.de/pop-imap/imap/thunderbird.html> (Web.de) oder <https://posteo.de/hilfe/wie-richte-ich-posteo-in-thunderbird-manuell-ein> (Thunderbird)
- Falls die Einrichtung Ihrer E-Mail-Adresse in Thunderbird nicht klappt, kann es sein, dass Sie sich zuerst noch einmal bei Ihrem E-Mail-Anbieter einloggen und erlauben müssen, dass Thunderbird auf ihre Mails zugreift. Auch dafür bieten die meisten E-Mail-Anbieter Erklärtex te, die Sie meist gut über eine Suchmaschine finden. Das ist zum Beispiel der Erklärtex t von Gmx.de: https://hilfe.gmx.net/pop-imap/einschalten.html#indexlink_help_pop-imap_einrichtung-mailprogramm-scheitert
- Wichtig: am besten lassen Sie bei der Einrichtung alle Einstellungen so, wie sie sind. Standardmäßig ist eine Technologie namens „IMAP“ voreingestellt. Die sorgt dafür, dass Thunderbird Nachrichten vom E-Mail-Anbieter abrufen, sie aber dort lässt. Das bedeutet, dass Sie sie auch weiterhin über den Browserzugriff online lesen können.
- Wenn Sie manuell auf „Pop3“ umstellen, können Sie einstellen, dass Thunderbird neue Mails herunterlädt und dann automatisch beim E-Mail-Anbieter löscht. Das ist insofern Daten-sparender, da die Mails dann nur noch auf Ihrem Rechner gespeichert sind. Es bedeutet aber: Sie können die heruntergeladenen E-Mails dann nicht mehr online lesen, sie existieren nur noch auf Ihrem Rechner. (Sie können allerdings einstellen, dass auch bei Pop3 Mails noch 30 Tage beim Mail-Provider verbleiben und erst dann gelöscht werden.)

- Vor allem, wenn Sie sich dafür entscheiden, dass Ihre E-Mails nach dem Abruf durch Thunderbird beim Mail-Anbieter gelöscht werden, ist es wichtig, dass Sie sich regelmäßig auf externen Datenträgern Back-ups Ihrer Thunderbird-Dateien machen. Falls Ihr Rechner nämlich mal verloren oder komplett crasht, wären ansonsten alle Ihre E-Mails weg. Das Sichern Ihrer Thunderbird-Dateien geht zum Glück sehr gut. Hier wird erklärt wie:

<https://support.mozilla.org/de/kb/thunderbird-daten-auf-neuen-rechner-uebertragen>

(6) E-Mails verschlüsseln mit Thunderbird

- Die beste Lösung ist E-Mailverschlüsselung im Open Source-Mailprogramm Thunderbird.
- Jahre lang lief die Verschlüsselung in Thunderbird über die externe Erweiterung Enigmail, die Sie in Thunderbird installieren mussten. Gerade befinden wir uns in einer Übergangsphase, die Verschlüsselung wurde vor kurzem als Kernfunktion direkt in Thunderbird eingebaut. Wenn Sie unter <https://www.thunderbird.net/de> das Programm Thunderbird herunterladen, bekommen Sie die Software-Version No. 78.2.1. In diese Version ist die Verschlüsselungsfunktion erstmal für alle eingebaut.

- Zur neuen Verschlüsselungsfunktion gibt es momentan noch keine gute Anleitung. Deswegen skizziere ich kurz die wichtigsten Navigationspfade:

- **Schlüssel erzeugen:** Wenn Sie ein E-Mail-Konto eingerichtet haben und in der linken Spalte das Konto anklicken, sehen Sie (ab Version 78.2), das Feld „Ende-zu-Ende-Verschlüsselung“. Das klicken Sie an. → Sie finden dort den Punkt „Add Key“ und klicken ihn an. (Momentan ist das Menü noch nicht auf Deutsch übersetzt. Später dürfte der Punkt „Schlüssel hinzufügen“ oder ähnlich lauten.) → Sie klicken auf „Continue“ („Weiter“). → Sie lassen die Einstellungen, wie Sie sind, und klicken auf „Generate Key“ („Schlüssel erzeugen“) → und dann auf „Confirm“ („Bestätigen“). Jetzt hat Thunderbird für Sie ein Schlüsselpaar erzeugt.

- **Anderen den eigenen, öffentlichen Schlüssel mitteilen:** Sie klicken auf „Verfassen“ und schreiben eine Mail → Sie klicken auf das Feld „S/Mime“ und wählen in der sich öffnenden Leiste den Punkt „Meinen öffentlichen Schlüssel anhängen“ → Sie schicken die Mail an die von Ihnen angegebene E-Mail-Adresse. → Sobald die Person Ihren Schlüssel in ihr eigenes E-Mail-Programm importiert hat, kann sie Ihnen verschlüsselte E-Mails schicken. Ihr Thunderbird-Programm entschlüsselt die dann automatisch für Sie. Wenn Sie sich einmal anschauen wollen, wie eine verschlüsselte E-Mail aussieht, loggen Sie sich auf der Webseite Ihres E-Mail-Anbieters ein. Sie werden sehen: Im noch nicht entschlüsselten Zustand besteht die Mail nur aus unverständlichem Zeichensalat.

- **Den öffentlichen Schlüssel einer*s anderen importieren:** Wenn Sie eine Mail mit einem öffentlichen Schlüssel erhalten haben, müssen Sie ihn importieren. Sie machen einen Rechtsklick auf die, sich im Anhang befindliche, Datei mit der Endung .asc. → Sie wählen den Punkt „Import Openpgp Key“ aus. → Sie klicken zweimal im sich öffnenden Dialogfenster auf „OK“. Nun haben Sie den öffentlichen Schlüssel der*des anderen importiert. → Dann müssen Sie dem Schlüssel noch Ihr Vertrauen aussprechen. Erst dann verwendet Thunderbird ihn. Klicken Sie dafür wieder in der linken Spalte auf Ihre E-Mail-Adresse. → Wählen Sie den Punkt „Ende-zu-Ende-Verschlüsselung“ aus. → Klicken Sie auf das Feld „OpenPGP Key Manager“. → Klicken Sie mit der rechten Maustaste auf den Schlüssel, den Sie importiert haben. → Klicken Sie auf „Key Properties“ (später heißt der Punkt vermutlich „Schlüssel-Eigenschaften“). → In dem Reiter „Your Acceptance“ („Ihr Vertrauen“), geben Sie an, inwiefern Sie darauf vertrauen, dass der Schlüssel tatsächlich zur jeweiligen E-Mail-Adresse gehört und nicht etwa ein Betrugsversuch ist. Thunderbird verwendet den Schlüssel nur, wenn Sie angeben, dass Sie den Schlüssel akzeptieren und eines der beiden Felder auswählen: „Yes, but I have not verified that it is the correct key.“ oder „Yes, I’ve verified in

person this key has the correct fingerprint.“ → Ab jetzt können Sie der jeweiligen Person eine verschlüsselte E-Mail schicken. Dazu teilen Sie Thunderbird einmal mit, dass die Mails an die Person ab jetzt immer verschlüsselt werden sollen. Wenn Sie eine Mail schreiben (auf „Verfassen“ klicken), wählen Sie im sich öffnenden Mail-Fenster das Feld „S/Mime“ an → und dann den Punkt „Nur mit Verschlüsselung senden“. Über den gleichen Navigationspfad können Sie Thunderbird auch anweisen, nicht zu verschlüsseln. (Der Punkt heißt dann „Nicht verschlüsseln“.)

- **Den eigenen privaten Schlüssel auf dem Rechner verschlüsseln:** Den privaten Schlüssel („Private Key“), mit dem Thunderbird an Sie gerichtete verschlüsselte Mails wieder entschlüsseln kann, hat Thunderbird im Programm-Ordner auf Ihrem Rechner abgelegt. Dieser Private Key ist alleine schon dadurch gesichert, dass niemand einfach so an die Inhalte auf Ihrem Rechner kommt.

Sie können aber noch ein zusätzliches „Master-Passwort“ einrichten, das Sie jedes Mal eingeben müssen, sobald Sie Thunderbird starten. Dieses Master-Passwort verschlüsselt Ihren Private Key. Auch wenn Sie dann Ihren Rechner verlieren oder er Ihnen gestohlen wird, ist Ihr Private Key sicher. Das ist eine zusätzliche Sicherheitsmaßnahme. Ihr Private Key ist aber schon dadurch gesichert, dass er lokal auf Ihrem Rechner liegt. So können Sie ein Master-Passwort festlegen: Gehen Sie ins Menü von Thunderbird (Klick auf das das „Burger-Symbol“ mit den drei übereinander liegenden Strichen. → auf Einstellungen“ → auf „Datenschutz & Sicherheit“ → Machen Sie im Feld „Passwörter“ ein Häkchen in das Feld „Master-Passwort verwenden“ → Sie denken sich ein Master-Passwort aus, geben es zweimal im sich öffnenden Dialogfenster ein und klicken auf „OK.“ → Ab jetzt müssen Sie (und gegebenenfalls Leute, die unbefugten Zugriff auf Ihren Rechner haben) jedes Mal beim Start von Thunderbird das Master-Passwort eingeben. → Achtung: Wenn Sie das Passwort vergessen, können Sie Thunderbird zwar neu einrichten, Sie haben aber keinen Zugriff mehr auf Ihren Private Key. Mails, die mit dem zum Private Key gehörigen öffentlichen Schlüssel verschlüsselt wurden, können Sie dann nicht mehr entschlüsseln. Unter Punkt Eins schlage ich Ihnen eine Methode vor, um ein sicheres und gut merkbares Passwort zu erzeugen. Sie können sich das Passwort auch zusätzlich auf ein Blatt Papier schreiben, das Sie sicher und gut auffindbar in Ihrer Wohnung verwahren.

- Weiterführende Anleitungen: Eigentlich gibt es jede Menge detaillierte Anleitungen zur Mail-Verschlüsselung in Thunderbird im Netz. Die beziehen sich aber alle noch auf die „alte“ Vorgehensweise mithilfe der externen Programmiererweiterung Thunderbird. Da die neue Verschlüsselungsfunktion gerade erst eingeführt wird, gibt es noch keine guten Anleitungen dazu. Wenn Sie mehr wissen wollen, suchen Sie in den nächsten Wochen über eine Suchmaschine nach Anleitungen zu „Thunderbird Verschlüsselung“ oder „Thunderbird OpenPGP“ und achten Sie darauf, dass die Artikel aktuell sind und sich auf die neue Verschlüsselung beziehen.

- Für die „alte“ Verschlüsselungsmethode mit Enigmail gibt es eine gute Anleitung. Die ist zwar nicht mehr aktuell. Die Lektüre könnte sich aber trotzdem lohnen, da Sie dort viele weitere Hintergründe zum Prinzip der Mail-Verschlüsselung finden. Und die Logik der Verschlüsselung ist beim alten wie beim neuen Verfahren identisch.

https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/dossiers/sicherheit/email/gnupg/enigmail.html

In Kürze: Mail-Verschlüsselung jenseits von Thunderbird auf PC

- Die beste Lösung ist E-Mailverschlüsselung im Open Source-Mailprogramm Thunderbird.
- Momentan läuft die Verschlüsselung in Thunderbird über die Erweiterung Enigmail. Sie installieren das Addon über folgenden Navigationspfad in Thunderbird: Burger-Menü rechts oben – Addons – Addons - „Enigmail“ in das Suchfeld eingeben – Zu Thunderbird hinzufügen. Gute

Anleitung für Enigmail: https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/dossiers/sicherheit/E-Mail/gnupg/install_enigmail.html

- Achtung: Thunderbird befindet sich gerade in einer Umbruchphase. Zur Zeit verschlüsseln Sie Ihre Mails in Thunderbird mit der Erweiterung Enigmail. Ende August wird die Thunderbird-Version 78.2 erscheinen, ab der wird der Umgang mit Erweiterungen komplett anders sein. Enigmail wird dann nicht mehr funktionieren. Thunderbird arbeitet daran, E-Mailverschlüsselung nahtlos in das Mailprogramm zu integrieren, siehe <https://blog.thunderbird.net/2019/10/thunderbird-enigmail-and-openpgp>. Mit Veröffentlichung der Thunderbird-Version No. 78.2 wird die aktuelle Version (No. 68) noch drei weitere Monate mit Updates versorgt werden und somit sicher sein. Somit müssen Sie nicht sofort umsteigen, sondern können sich drei Monate Zeit dafür lassen. Dieses Wiki zur Version 78 wird kontinuierlich von Thunderbird aktualisiert: <https://wiki.mozilla.org/Thunderbird:OpenPGP:2020>.
- Die Grundfunktionalität der E-Mail-Verschlüsselung bleibt gleich. Nur die Navigation wird sich verändern (und vermutlich erheblich vereinfachen)

(7) Smartphone-Einstellungen

- Die Navigationspfade bei Android-Smartphones unterscheiden sich leicht je nach Gerätehersteller. Beim Marktführer Samsung lautet der Navigationspfad: Einstellungen – Google-Konto – Daten & Personalisierung. Dort finden Sie die Zeilen „Web- & App-Aktivitäten“, „Standortverlauf“ und „Youtube-Verlauf“. Wenn Sie auf die Kategorien tippen, können Sie über einen Schieberegler die Datenübertragung abschalten („pausieren“).
- Auf iPhones können Sie die komplette iCloud manuell deaktivieren, über: Einstellungen → Apple-ID, iCloud iTunes oder App-Store (ganz oben, direkt unter Nutzernamen) → Abmelden. Einzelne iCloud-Einstellungen sind möglich über: Einstellungen → Apple-ID → iCloud. (siehe <https://mobilsicher.de/ratgeber/icloud-datenschutz-funktionen-hacks#toc3> und <https://mobilsicher.de/ratgeber/icloud-konfigurieren>).

(8) Messenger-Apps (Smartphone)

- Stufenmodell Messenger
- unterste Stufe: Whatsapp, Facebook Messenger, iMessage, Telegram
- mittlere Stufe: Threema, Wire, Signal
- oberste Stufe: Briar

Detaillierte Portraits dieser und weitere Messenger finden Sie auf der Webseite des Medienprojekts Mobilsicher sowie auf der Webseite des Privacy-Handbuchs:

<https://mobilsicher.de/ratgeber/verschluesst-kommunizieren-per-app> und https://www.privacy-handbuch.de/handbuch_74.htm

(9) Texte verschlüsseln mit LibreOffice

- LibreOffice ist ein Open-Source-Programmpaket, vergleichbar mit Microsoft Office. Es enthält u.a. ein Textprogramm, ein Tabellenprogramm und ein Präsentationsprogramm. Download unter: <https://de.libreoffice.org>
- Wenn Sie ein Textdokument speichern (mit Strg+S oder über den Navigationspfad Datei – Speichern) können Sie im sich öffnenden Fenster den Punkt „Mit Kennwort speichern“ auswählen. Sie werden dann nach einem Passwort gefragt. Das Dokument lässt sich im Anschluss dann nur öffnen, nachdem man dieses Passwort eingegeben hat.

(10) Alternative PC-Betriebssysteme

- Gut funktionierende alternative PC-Betriebssysteme sind Linux Mint und Linux Ubuntu.

(<https://linuxmint.com> und <https://ubuntu.com>)

- Wenn Sie sie nutzen wollen, haben sie verschiedene Möglichkeiten. Bei allen drei Optionen brauchen Sie einen USB-Stick, auf den Sie zuvor Linux installiert haben.

→ Option Eins: Das Linux-Betriebssystem befindet sich nur auf einem USB-Stick, von dem aus Sie es starten. Das macht allerdings nur für eine Testphase Sinn, da Sie keine Dateien speichern können.

→ Option Zwei: Sie wählen die „Dual Boot“-Variante. Über den Partitionsmanager auf Ihrem Rechner schränken Sie den Platz etwas ein, den Ihr altes Betriebssystem zur Verfügung hat und stellen einen Festplatten-Bereich für das Linux-Betriebssystem bereit. Im Anschluss installieren Sie Linux Mint oder Linux Ubuntu von Ihrem USB-Stick und wählen die Option, Linux neben Windows bzw. Mac zu installieren. Sie können dann in Zukunft beim Hochfahren des Rechners wählen, ob der Rechner das Windows/Mac- oder das Linux-Betriebssystem starten soll.

→ Option Drei: Sie ersetzen Ihr altes Windows- oder Mac-Betriebssystem und spielen, von dem USB-Stick aus, Linux Mint oder Linux Ubuntu auf Ihren Rechner.

Bei Option Drei ersetzt Linux Ihr als Betriebssystem komplett mit allen Dateien. Sie müssen sich deswegen vorher ein Back-up Ihrer Daten erstellen. Und auch bei den anderen beiden Optionen sollten Sie zuvor Ihre Daten gesichert haben. Linux Mint und Linux Ubuntu auszuprobieren und zu nutzen, ist sehr sicher. Gerade wenn Sie noch wenig IT-Know-how haben und Änderungen am Betriebssystem vornehmen, kann jedoch immer etwas schiefgehen.

Auf ein Linux-Betriebssystem umzusteigen, ist keine Raketenwissenschaft. Es ist dennoch deutlich komplexer, als ein „normales“ Programm zu installieren. Sie müssen immer wieder kleine Einstellungen vornehmen, mit denen IT-Laien oft nicht vertraut sind. Wenn Sie die Suchbegriffe „Linux Mint installieren“ oder „Linux Ubuntu installieren“ in eine Suchmaschine eingeben, finden Sie gute, allgemein verständliche Anleitungen. Lesen Sie sich vielleicht zwei oder drei der Anleitungen durch und legen Sie los.

Wenn Sie das Gefühl haben, dass Sie gar nicht durchblicken und wenn Sie in Ihrem Bekannten- oder Familienkreis Personen mit mehr IT-Know-how haben, fragen Sie die vielleicht einfach um Rat. Außerdem gibt es in einigen Städten „Cryptopartys“, bei den IT-Aktivist*innen ehrenamtlich Informationen und konkrete Hilfestellung beim Umstieg auf Open-Source-Software bieten. Eine Auflistung von Städten und Terminen finden Sie unter <https://www.cryptoparty.in>

So. Schön, dass Sie bis hierhin durchgehalten haben. :-) Das waren die zehn Programme und Tricks, die Ihnen bei Ihrer digitalen Selbstverteidigung helfen. Ich wünsche Ihnen viel Spaß und Erfolg dabei. Stefan Mey
