Digitale Selbstverteidigung

10 Tricks und Programme, mit denen Sie sich und Ihre Daten schützen können

- Handout zum Vortrag am 28.09.2021 in Görlitz
- Second Attempt e.V. & Rabryka, in Zusammenarbeit mit „Kontrovers vor Ort“ der Sächsischen Landeszentrale für politische Bildung
- Referent: Stefan Mey, Freier Journalist, Journalistenbüro Schnittstelle, Berlin,

Ich wünsche Ihnen viel Spaß bei der technischen Verteidigung ihres digitalen Lebens. Die Programme gelten als verlässlich und sicher. Was Sie damit machen, unterliegt aber natürlich Ihrer eigenen Verantwortung.

Entscheiden Sie einfach selbst, was Sie ausprobieren wollen. Und lassen Sie sich bitte nicht entmutigen: Je nach Ihren bisherigen IT-Erfahrungen wird Ihnen die Umsetzung leichter oder schwerer fallen. Sie müssen nicht alles auf einmal in Ihr digitales Leben einbauen. Jeder kleine Baustein der digitalen Selbstverteidigung bringt Sie weiter.

Gliederung

(1) Sichere und gut merkbare Passwörter erzeugen

- Nonsens-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. Beispielsatz: „Ein ganzes Brot kostet weniger als zwei halbe Brötchen, oder?“. Daraus leite ich folgendes Passwort ab: 1gBkwa2/2B,o? .
- Zusatz-Tipp: Wenn Sie wollen, können Sie die Methode auch noch „würzen“, sprich mit eigenen Regeln versehen und so noch komplexer machen. Zum Beispiel könnten Sie bei der Nonsens-Satz-Methode festlegen, dass Sie bei beim dritten Wort nicht den Anfangsbuchstaben, sondern das komplette Wort schreiben. Das „gewürzte“ Passwort würde dann lauten: 1gBrotkwa2/2B,o? .

(2) Passwortmanager

(Browser-Passwortmanager)

- Die gängigen Internet-Browser verfügen über eingebaute Passwortspeicher. Wenn Sie sich mit Ihrem Browser auf einer Webseite anmelden, fragt Ihr Browser Sie, ob er das Passwort speichern soll. Alle gängigen Browser verfügen über eingebaute Passwortmanager. Ich empfehle allgemein den Open-Source-Browser Firefox (siehe auch Abschnitt 3 „Spuren-arm surfen mit Firefox“). Im Firefox-Browser für PC kommen Sie über folgenden Navigationspfad zum Passwortspeicher: Menü → Passwörter. In der Firefox-App lautet der Pfad: Menü → Einstellungen → Zugangsdaten und Passwörter.
- Ein Master-Passwort können Sie so festlegen: Menü → Einstellungen → Datenschutz und Sicherheit → Häkchen bei „Hauptpasswort verwenden“. (Die Funktion gibt es z. Z. nur für Firefox auf PC.)
- So erstellen Sie eine Sicherheitskopie ihrer Passwörter: Menü → Zugangsdaten und Passwörter → Klick auf die drei Punkte rechts oben → Zugangsdaten exportieren → Exportieren → unter Umständen müssen Sie Ihr Geräte-Passwort eingeben → Speichern (Die Zugangsdaten werden nun als Tabelle gespeichert). Siehe auch https://support.mozilla.org/de/kb/exportieren-logindaten-firefox-lockwise. Zur Zeit ist das bequeme Exportieren der Passwörter aus dem Browser-eigenen Passwortmanager nur für Firefox auf PC möglich, nicht aber in der Firefox-App für Smartphones.

(Eigenständige Passwortmanager: KeePass-Programmfamilie)

- Für Windows: KeePass (https://keepass.info/download.html) oder KeePassXC https://keepassxc.org/download
- Für Mac und Linux: KeePassXC (https://keepassxc.org/download)
- Hilfebereich zu KeePass: https://keepass.info/help/base/index.html (englischsprachig)
- Offizielle Installationshilfe und Benutzerhandbuch von KeePassXC: https://keepassxc.org/docs/KeePassXC_GettingStarted.html und https://keepassxc.org/docs/KeePassXC_UserGuide.html
- KeePass-Programme 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. Eine Synchronisierung von Passwörtern zwischen PC und Smartphone ist möglich, aber etwas kompliziert.
- Achtung: Da Technik immer mal kaputt gehen und Software fehlerhaft sein kann, sollten Sie die Passwörter stets auch separat sichern, in einer Textdatei auf einer externen Festplatte oder auf einem Blatt Papier in der Wohnung. In KeePass und KeePassXC können Sie die Passwort-Liste bequem aus dem Programm heraus in verschiedenen Dateiformaten exportieren.

- KeePass und die verwandten Programme aus der KeePass-Familie sind Open Source, was ich bei einer solch wichtigen Programm-Art für wichtig halte. In puncto Usability und Funktionsumfang sind aber einige kommerzielle Programme besser. Wenn Sie sich auch andere PW-Manager anschauen wollen: Es gibt verschiedene detaillierte Tests. Zum Beispiel hat Stiftung Warentest im Januar 2020 Passwortmanager getestet: https://www.test.de/Passwort-Manager-im-Test-5231532-0/. Der Artikel steht hinter einer Paywall, die Süddeutsche Zeitung hat die drei Sieger aber zusammengefasst: https://www.sueddeutsche.de/digital/passwortmanger-test-stiftung-warentest-keepass-1.4774898. Alternativ gibt es einen Passwort-Manager-Test vom Computermagazin c't (ebenfalls Paid Content): https://www.heise.de/select/ct/2020/15/2003814272163299007.

(3) Spuren-arm surfen mit Firefox

- Download unter https://www.mozilla.org/de/firefox/new (verfügbar für PC und Smartphone)
- Automatische Suchvorschläge bei Eingaben in der Adresszeile abschalten (auf dem PC): Menü (drei übereinander liegende Striche rechts oben im Firefox) → Einstellungen → Suche → in Feld „Suchvorschläge anzeigen" Häkchen entfernen
- Cookies mit Schließen des Browsers löschen (auf dem PC): Menü → Einstellungen → Datenschutz & Sicherheit → Feld „Cookies und Website-Daten beim Beenden von Firefox löschen" anklicken
- Das sind die Navigationspfade für Firefox auf dem PC. Auf dem Smartphone unterscheiden sich die Pfade leicht, die Logik ist aber ähnlich.
- Exkurs: Podcast-Folge zur Problematik der Hintergrund-Datenströme in Webseiten und Apps: http://www1.stuttgart.de/stadtbibliothek/veranstaltungen/erwachsene/?id=2400.

(4) Anonym und Zensur-frei surfen

- Download für PC unter: https://www.torproject.org/de
- „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.
- Mit Tor können Sie nicht nur Überwachung erschweren, sondern auch Zensur aushebeln. Etwa, wenn Sie auf Reise in einem Land mit Internetzensur sind. Die Umgehung von Zensur funktioniert oft problemlos, allerdings nicht überall. Länder wie China blockieren einfach den Zugriff auf das komplette Tor-Netzwerk mit allen Verschleierungs-Knoten. Auch darauf hat Tor eine Antwort: versteckte „Bridge"-Knoten (siehe Erläuterung zu Brücken-Knoten im Tor-Benutzerhandbuch: https://tb-manual.torproject.org/de/circumvention).

(5) Spam abwehren

- E-Mails sind das wichtigste Einfallstor für alle Arten von Cyberattacken. Der beste Schutz gegen Spam-Mails ist Wissen und ein gesunder Menschenverstand. Es gibt zwei wichtige Typen von Spam:
- Phishing: Das sind E-Mails, die so tun, als kämen Sie von einer Bank, einem Webshop, sozialen Netzwerk oder sonstigem Onlinedienst. Die Mails imitieren das Layout der Original-Mails. Das Ziel der Cyberkriminellen ist, dass Sie auf einen Link in der Mail klicken, der Sie auf eine gefälschte Webseite führt, und dort die Zugangsdaten für Ihr Online-Banking, Ihr Profil bei einem Webshop oder sozialen Netzwerk angeben. Phishing-Mails arbeiten oft mit Täuschung und mit Druck. Es heißt beispielsweise, dass eine Unregelmäßigkeit in Ihrem Profil beobachtet wurde und dass Sie sich innerhalb von 24 Stunden einloggen müssen. Oft sind Phishing-Mails leicht zu enttarnen, weil sie grobe Rechtschreibfehler enthalten. Manche Mails imitieren das „Original“ aber virtuos. Falls Sie sich nicht sicher sind, ob die Mail echt ist oder nicht, hilft ein einfacher Trick: Klicken Sie nicht auf den Link in der Mail, um sich einzuloggen. Sondern öffnen Sie Ihren Browser und loggen sich bei Ihrem Online-Banking/Social Media/Ecommerce-Dienst ein. Falls es tatsächlich Handlungsbedarf gibt, wird Ihnen das dort angezeigt werden.
- Schad-Spam: Diese Spam-Mails versuchen, Schadprogramme auf Ihrem Gerät zu installieren. Diese Schadware kann dann viel Schaden anrichten, z.B. Ihren Rechner verschlüsseln und für die Entschlüsselung ein Lösegeld verlangen oder Ihr Gerät kapern und in ein „Bot-Netz“ eingliedern. Eine solche Schadware wird typischerweise auf zwei Arten verteilt: Sie klicken auf den Link in der Mail und „fangen sich“ beim Besuch der Webseite die Schadware ein. Oder die Schadware verbirgt sich im Anhang. Auch Schad-Spam geht mitunter sehr geschickt vor, und auch hier hilft gesundes Misstrauen: Seien Sie vorsichtig, auf Links in E-Mails zu klicken, wenn Sie den Absender nicht kennen und Ihnen irgendetwas komisch vorkommt. Und klicken Sie nicht auf Anhänge, wenn die Dateien im Anhang verdächtige Endungen haben, etwa .exe oder .zip.
- Spam-Mails arbeiten gern mit Emotionen. Die Mails setzen Sie unter Druck: Angeblich müssen Sie eine hohe Rechnung begleichen oder angeblich müssen Sie sich umgehend irgendwo einloggen, weil Ihr Konto gesperrt wurde. Oder die Mails locken Sie: mit der Aussicht auf ein unerwartetes Liebes-Abenteuer oder auf einen Job, mit dem Sie angeblich vom heimischen Schreibtisch aus mit sehr wenig Aufwand sehr viel Geld verdienen können.
- Hören Sie auf Ihr Bauchgefühl, wenn Ihnen etwas komisch vorkommt: beispielsweise, weil die E-Mail offensichtlich automatisiert übersetzt wurde, extrem unpersönlich ist oder inhaltlich keinen Sinn macht. Bevor Sie auf einen Link oder den Anhang klicken, atmen Sie einmal kurz durch und fragen sich, ob der Inhalt der Mail überhaupt plausibel ist. Im Zweifelsfall lassen Sie die Finger von der Mail.
- Fragen Sie sich bei Anhängen in einer E-Mail: haben Sie einen Anhang erwartet? Werden Sie misstrauisch, wenn der Anhang eine ungewöhnliche Endung, sprich ein Dateiformat hat, etwa .zip, .exe oder .msi.
- Falls Sie den Verdacht haben, bei der (angeblichen) E-Mail eines Finanzinstituts, eines Webshops, sozialen Netzwerks oder sonstigen Onlinedienstes könnte es sich um eine Phishing-Mail handeln, öffnen Sie einfach Ihren Browser, geben in die Adresszeile „ganz normal“ die Webadresse des Finanzinstituts, Webshops etc. ein und loggen sich dort ein. Falls die Mail tatsächlich „echt“ war und es Handlungsbedarf gibt, werden Sie das dann sehen.

(6) E-Mails verschlüsseln

- Die beste Lösung ist E-Mailverschlüsselung auf dem PC mithilfe des Open Source-Mailprogramms Thunderbird.
- Ich halte Thunderbird generell für eine sinnvolle Software. Sie können mithilfe von Thunderbird Mails aller E-Mail-Anbieter bequem auf Ihren Rechner kopieren, dort lesen und vom Rechner aus Mails verschicken. Sie können auch problemlos verschiedene E-Mail-Adressen in Thunderbird einbinden.
- Download unter https://www.thunderbird.net/de
- Ihre E-Mail-Adresse mit Thunderbird verknüpfen: Thunderbird starten → Menü (die drei übereinander liegenden Striche rechts oben in Thunderbird) → Konten-Einstellungen → Konten-Aktionen (Feld links unten) → E-Mail-Konto hinzufügen → ausfüllen: Ihr Name (geben Sie dem E-Mail-Konto einen Namen), E-Mail-Adresse, Passwort → Weiter → Fertig (lassen Sie die Voreinstellungen für‘s Erste, wie sie sind). (siehe auch https://support.mozilla.org/de/kb/automatisch-konto-konfigurieren)
- Falls die Einrichtung Ihrer E-Mail-Adresse nicht klappt, kann es sein, dass Sie sich zuerst bei Ihrem E-Mail-Anbieter einloggen und erlauben müssen, dass ein E-Mail-Programm auf ihre Mails zugreift. Konkret müssen Sie den Abruf von Mails über eine Technologie namens POP3/IMAP erlauben, die Thunderbird verwendet. Viele E-Mail-Anbieter haben Erklärtexte geschrieben, die Sie über eine Suchmaschine finden. Das ist zum Beispiel ein Erklärvideo des Anbieters Gmx: https://hilfe.gmx.net/pop-imap/einschalten.html#indexlink_help_pop-imap_einrichtung-mailprogramm-scheitert.
- Und nun zur E-Mail-Verschlüsselung: Jahrelang lief die Verschlüsselung in Thunderbird über die Erweiterung Enigmail, die Sie in Thunderbird installieren mussten. Letztes Jahr jedoch wurde die Verschlüsselung als Kernfunktion direkt in Thunderbird eingebaut. Zur Verschlüsselungsfunktion gibt es keine gute deutschsprachige Anleitung. Deswegen skizziere ich die wichtigsten Navigationspfade:
- **Schlüssel erzeugen**: Wenn Sie ein E-Mail-Konto eingerichtet haben, klicken Sie auf Menü (→ Konten-Einstellungen → Ende-zu-Ende-Verschlüsselung → Schlüssel erzeugen → Weiter → Sie lassen die Einstellungen, wie Sie sind, und klicken auf Schlüssel erzeugen → Bestätigen. Jetzt rechnet Thunderbird einige Sekunden und hat dann für Sie ein Schlüsselpaar erzeugt. Dass es geklappt hat, erkennen Sie an der Meldung „OpenPGP-Schlüssel erfolgreich erstellt.“
- **Anderen Ihren öffentlichen Schlüssel mitteilen** (3 Optionen)
  - (a) jemandem per Mail schicken: Verfassen → Sicherheit (obere Leiste) → Meinen öffentlichen Schlüssel anhängen → abschicken
  - (b) Sie könen ihren öffentlichen Schluss auch auf Ihre Webseite hochladen. Dafür müssen Sie ihn erst aus exportieren in ihr Dateisystem exportieren: Menü → Konten-Einstellungen → OpenPGP-Schlüssel verwalten → Klicken Sie Ihren Schlüssel an → Datei → Schlüssel in Datei exportieren → Speichern.
  - (c) auf Schlüssel-Server hochladen: Key-Server sind Datenbanken, auf die man seinen öffentlichen Schlüssel hochlädt, um ihn auffindbar zu machen. Ich würde folgenden Key-Server empfehlen: https://keys.openpgp.org. Damit Sie Ihren öffentlichen Schlüssels hochladen können, müssen Sie ihn zuerst exportieren (siehe unten Punkt). Dann gehen Sie auf https://keys.openpgp.org → Hochladen → und laden die Schlüssel-Datei hoch. Die Datenbank schickt eine Bestätigigungsmail und Ihr öffentlicher Schlüssel ist auf key.openpgp.org auffindbar. Nun können ihn andere finden und auf der Webseite schauen, ob ein Schlüssel für Ihre E-Mail-Adresse hinterlegt ist – und Sie können nach Schlüsseln anderer suchen. Zusätzlich können Sie Ihren Schlüssel in Ihrer E-Mail-Signatur, auf Ihrer Webseite oder Ihrem Social-Media-Profil bekannt machen, indem Sie dort die die 16-stellige „Schlüssel-ID“ veröffentlichen. Die ID finden Sie so: Schlüsselverwaltung → die Zeile Ihres Schlüssels → Spalte Schlüssel-ID. Am besten schreiben Sie noch die verwendete Schlüsseldatenbank hinzu (key.openpgp.org), da verschiedene Datenbanken in Benutzung sind.

- Sobald die andere Person Ihren Schlüssel in ihr eigenes E-Mail-Programm importiert hat, kann sie Ihnen verschlüsselte E-Mails schicken. Ihr Thunderbird-Programm entschlüsselt die Mails 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 anderer importieren:** rechter Mausklick auf Schlüssel im Anhang → Openpgp-Schlüssel importieren → im sich öffnenden Fenster (unten) Zeile „Akzeptiert (nicht verifiziert)“ anklicken (ansonsten weigert sich Thunderbird, den Schlüssel zu verwenden) → OK → OK
- **Verschlüsselte Mail schicken:** Verfassen → Sicherheit (obere Leiste) → Nur mit Schlüssel senden. Ab jetzt verschlüsselt Thunderbird alle Mails an die jeweilige Adresse.
- **Sicherheitskopie des eigenen Schlüssels erstellen:** Ihren privaten Schlüssel können Sie auch Thunderbird heraus exportieren und auf einem externen Datenträger sichern (für den Fall, dass Ihr Gerät einmal wegkommt oder unbrauchbar wird): Menü → Konten-Einstellungen → OpenPGP-Schlüssel verwalten → Klicken Sie Ihren Schlüssel an → Datei → Schlüssel in Datei exportieren → Speichern.
- **Ihren privaten Key optional mit Passwort schützen:** Standardmäßig ist die Textdatei mit Ihren privaten Schlüssel nicht extra mit einem Passwort geschützt. Der private Schlüssel ist eigentlich dadurch schon sehr sicher, dass er auf dem Computer liegt, auf denen niemand sonst Zugriff habt. Sie können optional allerdings ein Master-Passwort einrichten. Das verschlüsselt separat Ihren privaten Schlüssel (und auch alle gespeicherten Passwörter für E-Mail-Adressen.) Der Navigationspfad lautet: Menü → Einstellungen → Datenschutz & Sicherheit → anklicken: Master-Passwort verwenden.

Exkurs: Mail-Verschlüsselung jenseits von Thunderbird auf PC

- *Die beste Lösung für Mailverschlüsselung ist Thunderbird auf dem PC, egal ob Windows, Mac oder Linux. Man kann aber auch auf anderen Geräten und in anderen Kontexten verschlüsseln. Diese Lösungen sind alle miteinander kompatibel, da sie die gleiche Technologie (Openpgp) verwenden. (Nicht kompatibel ist allerdings die S/MIME-Verschlüsselung, die Outlook und Apple Mail eingebaut haben.)*
- *Für das E-Mail-Programm Outlook gibt es die Software gpg4win, die vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) in Auftrag gegeben wurde. Link: www.gpg4win.org*
- *Für Apple Mail nennt die Seite openpgp.org/software die kostenpflichtige österreiche Software GPGtools.org.*
- *Mailvelope, eine Erweiterung für Firefox, Google Chrome und Microsoft Edge ermöglicht E-Mail-Verschlüsselung direkt im Browser. Das allerdings gilt als nur mittel-sicher. Der Private Key liegt im Browser-Speicher, was Angriffe leichter macht, als wenn der Private Key separat in einer Datei auf dem Rechner liegt. Link: www.mailvelope.com*
- *Für Android-Smartphones empfiehlt sich die App K-9 Mail zusammen mit dem Verschlüsselungsprogramm OpenKeyChain. Links: https://k9mail.app, www.openkeychain.org.*
- *Für iOS gibt es keine einheitliche Empfehlung. Die Seite www.openpgp.org/software schlägt drei Apps vor: iPG Mail, Canary Mail und Safe Easy Privacy, die jedoch zum Teil kostenpflichtig und nicht Open Source sind.*

(7) Smartphone-Einstellungen

- Die Navigationspfade bei Android-Smartphones unterscheiden sich leicht je nach Gerätehersteller. Beim Marktführer Samsung lautet der Navigationspfad: Einstellungen → Google → Google-Konto verwalten – 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“). Weiter unten finden Sie die Einstellmöglichkeiten für personalisierte Werbung.
- Auf iPhones können Sie die komplette iCloud manuell deaktivieren, über: Einstellungen → Apple-ID, iCloud iTunes oder App-Store (ganz oben, direkt unter Nutzernamen) → Abmelden. Die Abwahl und Auswahl einzelner Datenkategorien ist möglich über: Einstellungen → Apple-ID → iCloud. (siehe https://mobilsicher.de/ratgeber/icloud-datenschutz-funktionen-hacks#toc3 und https://mobilsicher.de/ratgeber/icloud-konfigurieren.
- Podcast-Folge Überblick „Das Smartphone als Datenschleuder“: http://www1.stuttgart.de/stadtbibliothek/veranstaltungen/erwachsene/?id=2011

(8) Messenger-Apps

(Stufenmodell Messenger)

- unterste Stufe: Whatsapp, Facebook Messenger, iMessage, Telegram
- mittlere Stufe: Signal, Wire
- Top-Position: Threema
  (auch interessant, aber technisch komplizierter sind: Briar (Kommunikation läuft über Darknet Adressen/ Element (Sie können optional eine eigene Datenbank einstellen)/ Delta-Chat (Kommunikation läuft über E-Mail-Adressen)
- Detaillierte Porträts der und anderer Messenger auf Mobilsicher.de: https://mobilsicher.de/ratgeber/verschluesselt-kommunizieren-per-app
- Detaillierte und sehr technische Porträts einzelner Messenger auf der Webseite von Mike Kuketz: https://www.kuketz-blog.de/die-verrueckte-welt-der-messenger-messenger-teil1

Exkurs F-Droid (App-Store für Open-Source-Apps)

• Für Android (für iPhones leider nicht) gibt es einen alternativen Appstore nur für Open-Source-Apps: F-Droid. So installieren sie ihn: mit der Browser-App auf https://f-droid.org gehen → Klick auf F-Droid herunterladen → herunterladen → öffnen → Sie sehen ein Dialogfenster mit der Meldung, dass Sie aus Sicherheitsgründen keine Apps aus unbekannter Quelle installieren dürfen → Klick auf Einstellungen → Schieberegler „Aus dieser Quelle zulassen“ auf „an“ → zurück zu F-Droid-Fenster → installieren → öffnen

• Am Schluss deaktivieren Sie wieder die Möglichkeit, dass das Gerät Programme installiert, die der Browser heruntergeladen hat, prinzipiell ist das eine sinnvolle Sicherheitseinstellung: Einstellungen → Apps → Browser-App auswählen → in Zeile „Unbekannte Apps installieren“ steht „Zugelassen“, Klick darauf → Schieberegler auf „aus“

• Link Anleitung F-Droid-Installation mit Screenshots: https://mobilsicher.de/ratgeber/so-installieren-sie-den-app-store-f-droid.

(9) Texte verschlüsseln

- 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 anklicken. Sie werden dann nach einem Passwort gefragt. Das Dokument lässt sich im Anschluss 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). Einsteiger*innen würde ich Linux Mint empfehlen.
- 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-Betriebsystem 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.

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