Clubabend „Achtung: Datensicherheit“

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

- Handout zum Online-Vortrag des Frankfurter PresseClubs in Kooperation mit der Evangelischen Akademie Frankfurt
- Referent: Stefan Mey, Berlin, freier Technologjournalist, Journalistenbüro Schnittstelle
- Autor einer Broschüre zu digitaler Selbstverteidigung für Journalist*innen und eines Sachbuchs zum Darknet
- Kontakt: stefan-mey@posteo.de (Schlüssel-Signatur 4AFF287111E19A5B, zu finden auf keys.openpgp.org), Twitter @OmyDot

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 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

- Passwortmanager KeyPass für Windows, Download unter: XC: https://keepass.info/download.html
- Mac- und Linux-Nutzer*innen verwenden 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
- 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.

- Passwort-Manager im Browser: Die gängigen Internet-Browser verfügen auch über eingebaute Passwortspeicher. Wenn Sie sich mit Ihrem Browser auf einer Webseite anmelden, fragt Ihr Browser Sie meist, ob er das Passwort speichern soll. Diese Browser-Passwortmanager sind praktisch, sie gelten aber als nicht so sicher wie separate Programme. Der Grund: Das Passwort wird in einem Speicherbereich des Browsers abgelegt und dieser ist deutlich anfälliger für gezielte Attacken als separate Programme. Als Kompromiss für weniger wichtige Passwörter machen diese Browser-Passwortmanager aber durchaus Sinn. Im Firefox-Browser (siehe nächster Punkt) kommen Sie über folgenden Navigationspfad zum Passwortspeicher: Menü → Zugangsdaten und Passwörter.

(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

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

(5) Spam abwehren

- E-Mails sind das wichtigste Einfallstor für alle Arten von Cyberattacken.
- Besonders gefährlich ist Schad-Spam: Diese Spam-Mails versuchen, Schadprogramme auf Ihrem Gerät zu installieren. Diese Schadware kann 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.
- Schad-Spam geht mitunter sehr geschickt vor. Einen perfekten technischen Schutz gibt es nicht, vor allem, wenn es sich um individualisierten Spam handelt, der sorgfältig auf eine Person zugeschnitten ist. Oft handelt es sich aber um Massen-Spam, der gut zu erkennen ist. Der beste Schutz gegen Spam-Mails ist Wissen und ein gesunder Menschenverstand.
- 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.

(6) E-Mails verschlüsseln mit Thunderbird

- 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
- Anleitung von Thunderbird zur Einrichtung einer E-Mail-Adresse: 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:

- Jahre lang lief die Verschlüsselung in Thunderbird über die externe Erweiterung Enigmail, die Sie in Thunderbird installieren mussten. Letztes Jahr jedoch wurde die Verschlüsselung als Kernfunktion direkt in Thunderbird 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, klicken Sie auf Menü (die drei übereinander liegenden Striche rechts oben in Thunderbird) →Konten-Einstellungen → Ende-zu-Ende-Verschlüsselung. → Schlüssel erzeugen → Weiter → Sie lassen die Einstellungen, wie Sie sind, und klicken auf „Schlüssel erzeugen“ → und dann auf „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 den eigenen 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: siehe Exkurs zu Key-Servern* unten)
  - 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 einer*s anderen 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.

- ***Exkurs: Schlüssel per Key-Server bekannt machen:** Key-Server sind Datenbanken, auf die man seinen öffentlichen Schlüssel hochlädt, um ihn für andere auffindbar zu machen, und auf denen man nach öffentlichen Schlüsseln anderer sucht. Ich würde folgenden Key-Server empfehlen: https://keys.openpgp.org.
  - Damit Sie Ihren öffentlichen Schlüssels hochladen können, müssen Sie ihn zuerst aus Thunderbird heraus exportieren (Menü →Konten-Einstellungen → OpenPGP-Schlüssel verwalten → Klicken Sie Ihren Schlüssel an → Datei → Schlüssel in Datei exportieren → Speichern). Dann gehen Sie auf https://keys.openpgp.org → Hochladen → und laden die Schlüssel-Datei hoch. Die Datenbank schickt eine Bestätigigungsmail, dann ist Ihr öffentlicher Schlüssel auf key.openpgp.org auffindbar.
  - Schritt 2: Damit andere ihn leicht finden können, macht es Sinn, dass Sie die Signatur Ihres öffentlichen Schlüssels, die 16-stellige „Schlüssel-ID“, veröffentlichen. Die ID finden Sie so: Schlüsselverwaltung → die Zeile Ihres Schlüssels → Spalte Schlüssel-ID. Die 16-stellige Schlüssel-ID nennt Sie z. B. in Ihrer Mail-Signatur oder veröffentlichen sie auf Ihrer Webseite/ Ihrem Social-Media-Profil. Am besten schreiben Sie noch die verwendete Schlüsseldatenbank hinzu (key.openpgp.org), da verschiedene Datenbanken in Benutzung sind.

- 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“

Überblick: 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. 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

(Stufenmodell Messenger)

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

- 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

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/verschluesselt-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 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 Ubuntu 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.

Exkurs Crypto-Partys

- Nicht alles ist für Laien so leicht umzusetzen, wie es klingt. In vielen Städten gibt es „Crypto-Partys“, bei den IT-Aktivistinnen und -Aktivisten ehrenamtlich Informationen und konkrete Hilfestellung beim Umstieg auf Open-Source-Software bieten. Ein Überblick liefert die Webseite www.cryptoparty.in. In Frankfurt scheint es seit längerer Zeit allerdings keine Crypto-Partys mehr gegeben zu haben, auch nicht online). (siehe https://www.cryptoparty.in/frankfurt).

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