Half a Silver Bullet

Die zwei Capulcu-Broschüren und die Computersicherheit

> „Was müssen wir installieren, um sicher zu sein?“ – diese Frage hört oft, wer im weiteren Bereich der Linken was mit Rechnern macht. Und muss dann sagen: „So einfach ist das nicht“. In der Tat gibt es keine Silver Bullets, keine magischen Programme, die mensch runterlädt, um Bullen, Nazis, die Chefs, die Schlapphüte *und* facebook aus einem Rechner rauszuhalten. Tatsächlich haben wir früher im Wesentlichen gesagt: Vergesst es einfach ganz. Das revidieren wir, dank zweier Entwicklungen: Tails und der Dokumentation dazu von Capulcu.

Vorweg aber: Die Krawatten von Unisys, Thales, Cap Gemini und so fort, die Gesellen also, die den Unterdrückungsapparaten dieser Welt ihre EDV bauen, haben mit einem recht: „Sicherheit ist ein Prozess“. Ohne, dass sich in der Birne was tut, lesen euch Böse wie Nicht-ganz-so-Böse weiter wie ein Buch. Deshalb sollte, wer sich Tails installieren will, zunächst ein anderes Heft der Capulcus lesen: „Disconnect – keep the future unwritten“[1]. Das nämlich setzt einen Rahmen dafür, wie eine selbstbestimmte EDV-Nutzung – und die hängt als Voraussetzung wie Ziel eng mit der Sicherheit zusammen – aussehen könnte, und was wir an politischen Interventionen in dem Bereich noch recht weit oben auf der Todo-Liste haben.

Im ersten Capulcu-Heft[2] hingegen geht es technisch zu. Es ist in gewisser Weise ein erläutertes Handbuch zu Tails. Das wiederum ist ein komplettes Betriebssystem, das ihr auf üblichen Rechnern laufen lassen könnt, ohne das heißgeliebte Windows oder MacOS erst runterputzen zu müssen – und ein Betriebssystem, das bei der Wahrung der Privatsphäre hilft statt diese, wie sonst nur zu üblich, aktiv zu untergraben.

Den ersten Schritt dazu, das Runterladen von Tails nämlich, diskutiert die Broschüre in einem mehrseitigen Anhang. Dass etwas, das ihr auf eurem Telefon mit einem Wisch in den Appstore erledigt, hier so lange Worte braucht, mag erschrecken. Aber erstens liefert der Text Erklärungen für verschiedene Ausgangssysteme (ihr könnt von Windows, MacOS oder anderen Linuxen aus ein Tails-System bauen), und zweitens ist ein Download einer Software eigentlich grundsätzlich eine viel größere Sache als es der kleine Wisch suggerieren mag, denn wer Code auf eurem Rechner ausführen kann, hat ihn schon halb in der Hand. Natürlich: Smartphones haben Google oder Apple eh schon in der Hand, da erübrigen sich alle Skrupel. Bei Tails hingegen wollt ihr sicher sein, dass die Software, die ihr aus dem Netz bekommt, auch wirklich die ist, die sie vorgibt zu sein und nicht etwa den Bundestrojaner an Bord hat. Ihr werdet es schon ahnen: PGP hilft auch hier.

Wenn Tails endlich verifiziert auf eurer Platte liegt, müsst ihr noch dafür sorgen, dass euer Rechner den Kram auch ausführt – und wie er das tut. Dazu stellen die Capulcus drei Nutzungsszenarien vor, und das, was für euch relevant ist, wenn ihr eure RH-Mails und Unterstützungsfälle verantwortlich bearbeiten wollt, läuft bei ihnen als „c) Persistenz: Tails als Reise- und Alltagssystem“. Dabei läuft es auf einem USB-Stick, von dem ihr leicht Backups ziehen könnt und der auch an Urlaubsvertretungen (oder ähnlich) weitergegeben werden kann.

Insofern ist viel von den ersten zwanzig Seiten der Tails-Broschüre auch eine Sicherheitsstufe zu weit oben – selbstverständlich müsst ihr nicht nach jedem U-Fall mit Thermit an eure Datenträger heran. Bei all den Sicherheitsmaßnahmen ist immer zu fragen, welchen Angrifsszenarien ihr widerstehen wollt, und das sieht für U-Fall-Bearbeitung und BDV-Anträge eben anders aus als bei Planung direkter Abrüstungsmaßnahmen.

Die in diesem Bereich gegebenen Kurzeinführungen in alltägliche Tätigkeiten – Schlüssel verwalten, Mails austauschen, Chatten, Bilder verpixeln usf – sind aber trotz ihrer Tendenz zur Paranoia ausgesprochen le-

senswert, gerade auch, weil sie einen Vergleich geben zu euren augenblicklichen Praktiken und so bei der Einschätzung helfen mögen, ob ihr den Kram so weitermachen wollt.

Nun ist umgekehrt klar, dass die 30 Seiten der Broschüre nicht reichen können, um eine umfassende Einführung zu liefern in all die Dinge, die ihr mit Tails machen könnt. Die Capulcus liefern aber eine Übersicht über die üblichen Lösungen für Aufgaben von Office-Kram über Layout, Bild- oder Videobearbeitung bis hin zur Kontrolle von Dokument-Metadaten und anonymen Dokumenten-Austausch. Das sollte zumindest über die bei Linux-Neulingen nicht ungewöhnliche Verwirrung beim Erstkontakt („Wo isn hier mein Word? Und mein Photoshop?“) hinweghelfen, und für weiteres sind Verweise zu Programmdokus im Netz beigefügt.

Besonders hinweisen wollen wir kurz vor Schluss auf einen Punkt, der bei den Capulcus mehrfach betont wird: Zwar wird bei Tails der Netzwerkverkehr durch Tor recht zuverlässig anonymisiert (vgl. auch get connected in RHZ 4/07 und 2/08), aber wer durch diese Leitung erst, sagen wir, Aufrufe zu Scherbendemos verbreitet und gleich danach Freundschaftsanfragen auf Facebook macht, macht es den Rechnern jedenfalls sehr schwer mit der Anonymität. Deshalb: „Identitäten sauber trennen“ (lest es in der Broschüre nach).

Schaut also mal rein in die beiden Capulcu-Hefte. Wenn mehr von der RH-Arbeit über Tails liefe, könnten unsere Datenschutzbeauftragten ein gutes Stück besser schlafen. Und so schrecklich viel mühsamer als Computer an sich ist Tails auch nicht.

Datenschutzgruppe der Roten Hilfe Heidelberg

[1] https://capulcu.blackblogs.org/neue-texte/bandii/

[2] https://capulcu.blackblogs.org/neue-texte/bandi/