Warum "Verschlüsselung aktivieren" teilweise nicht mehr ausreicht

Es wird immer empfohlen: "Verschlüsselt eure Geräte". Das ist auch grundsätzlich richtig, allerdings reicht das nicht immer. Trotz Verschlüsselung kann die Polizei Geräte teilweise dennoch auslesen.

Linux und Mac

Für Linux und Mac(Book)s ist die Sache einfach: Nutzt die Festplattenverschlüsselung, die vom jeweiligen Betriebssystem mitgeliefert wird. Nutzt anständige Passwörter, dann kommt die Polizei nicht an eure Daten. Das gleiche gilt für externe Datentäger (externe Festplatten, USB-Sticks, SD-Karte), die mit Veracrypt verschlüsselt sind (Geräte ent/verschlüsseln mit Veracrypt)

Android & iPhones

Bei Smartphones sieht das leider ganz anders aus. Die Polizei nutzt Tools wie Cellebrite, um verschlüsselte Smartphones auszulesen. Cellebrite ist leider ziemlich gut darin. **Grundsätzlich solltet ihr davon ausgehen, dass Cellebrite eurer Telefon aufbekommt, gerade wenn ihr ein etwas älteres Gerät verwendet.** Mehr Einzelnheiten zum Thema: "Was bekommt Cellebrite auf" gibt es in diesem Vortrag.

Cellebrite nutzt zum Auslesen der Geräte Schwachstellen aus oder probiert alle Entsperrcodes aus (Bruteforce-Angriff). Es braucht Zeit, alle PINs auszuprobieren. Doch die Polizei hat die Zeit, da die beschlagnahmten Geräte über Jahre bei ihnen liegen. Das Gleiche gilt auch für das Ausnutzen von Schwachstellen: Gibt es gerade keine passende Schwachstelle, kann die Polizei einfach darauf warten, bis für das Telefon/Betriebssystem eine Schwachstelle bekannt wird.

TODO: was tun Trotzdem ist es empfehlenswert, ein komplexes Passwort (anstatt 6-stelliger PIN) für die Bildschirmsperre zu verwenden. Vielleicht gibt die Polizei nach ein paar Monaten auf. TODO: FMD, Cryptocam, Mooly

Das einzige, was die Polizei nicht aufbekommt, ist GrapheneOS. GrapheneOS ist ein auf Sicherheit ausgelegtes Betriebssystem, das auf Android basiert. Allerdings unterstützt GrapheneOS aktuell nur Google Pixel Geräte.

Windows

Die Verschlüsselung von Windows nennt sich Bitlocker. In den letzten Jahren sind immer wieder Schwachstellen bekannt geworden, durch die Bitlocker umgangen werden konnte. Ein paar Beispiele:

- die Bitpixie-Schwachstelle (wurde sehr lange nicht behoben)
- TPM-Sniffing-Angriff (Demo auf Youtube)
- auf dem 39C3 (Kongress vom Chaos Computer Club) gab es einen Vortrag, der gezeigt hat, wie man durch das Ausnutzen von einfachen Logik-Fehlern die Bitlocker-Verschlüsslung umgehen konnte

Die Zusammenfassung: **Die Windows-Verschlüsselung Bitlocker ist nicht zu empfehlen.** Es gibt allerdings Einstellungsmöglichkeiten, mit denen ihr die Bitlocker-Sicherheit deutlich erhöhen könnt.

Hintergrund: Wie funktioniert die Bitlocker-Verschlüsselung?

Moderne Laptops besitzen einen Sicherheitschip (TPM 2.0), der eure Festplatte beim Starten des Laptops automatisch entschlüsselt. Ihr müsst heutzutage kein Passwort eingeben, damit das Gerät entschlüsselt wird. Die PIN, die ihr dann beim Anmelden eingebt, ist nicht das Festplattenpasswort, sondern euer Benutzer*innen-Passwort (es kann ja mehrere Accounts auf dem Laptop geben). Dass ihr beim Starten kein Festplatten-Passwort eingeben müsst ist bequem, aber nicht besonders sicher.

Was tun mit dem Windows Laptop?

- auf Linux wechseln (gerade wenn euer Laptop mittlerweile sehr langsam geworden ist) :)
- Wenn ihr bei Windows bleiben wollt, könnt ihr
  - **Pre-Boot-Authentication aktivieren** - Dann nutzt Bitlocker weiterhin den TPM-Sicherheitschip, es muss aber eine PIN beim Start eingegeben werden (geht nicht auf Windows Home, nur auf Windows Pro/Education/Enterprise, Anleitung auf YouTube, Anleitung auf Deutsch, Anleitung auf Englisch)

- **Passwort nutzen** - Ihr könnt den TPM-Sicherheitschip auch einfach nicht nutzen und stattdessen ein sicheres Passwort setzen, mit dem eure Festplatte verschlüsselt ist (geht nicht auf Windows Home, nur auf Windows Pro/Education/Enterprise, TODO).
- den Laptop mit Veracrypt verschlüsseln (Anleitung)

Wenn ihr Windows nutzt

- Achtet bitte darauf, dass euer Bitlocker Recovery-Key nicht online im Microsoft Konto gespeichert ist (Anleitung zum Löschen)
- Schaut, dass ihr ein Backup von eurem Recovery-Key habt. Wenn der Laptop kaputt geht (z. B. Wasserschaden), aber die Festplatte noch geht (meistens der Fall), könnt ihr sie sonst nicht entschlüsseln und eure Daten sind futsch (TODO: Anleitung)

Version #1
Erstellt: 2026-03-24 12:49:02 UTC von RAZ Migration Bot
Zuletzt aktualisiert: 2026-03-24 12:49:02 UTC von RAZ Migration Bot