Festplattenverschlüsselung

- Allgemeines zur Festplattenvollverschlüsselung
- Android Gerät verschlüsseln
- Windows verschlüsseln mit Bitlocker
- Windows verschlüsseln mit Veracrypt
- macOS verschlüsseln
- Festplattenvollverschlüsselung mit Ubuntu Installation

Allgemeines zur Festplattenvollverschlüsselung

Wenn du Fragen zur Verschlüsselung hast, kannst du dich gerne bei uns melden. Schreibe dazu einfach eine E-Mail an it-support@raz-ev.org

Risiken

Wenn du deine Festplatte verschlüsselst und das Passwort vergisst, gilt: Alle deine Daten sind weg - niemand kann sie wieder retten. Du musst dir dieses Risikos bewusst sein.

Lasst uns kurz unterscheiden:

- Auf deinem Gerät sind Daten von deinem Engagement bei der Letzte Generation (LG)
- Vielleicht sind darauf auch ganz persönliche, private Daten (Kinderfotos, Steuererklärung, ...)

Wenn du deine privaten Daten, also die Daten, die nicht zu LG gehören, sichern willst, kannst du sie auch unverschlüsselt auf eine externe Festplatte oder mit einem Dienst wie Dropbox speichern. Der Grund, warum wir Laptops verschlüsseln, ist es, dich und andere vor den Konsequenzen der Arbeit mit der LG zu schützen und zu verhindern, dass die Polizei die Orga stören kann. Deine privaten Daten sind dein Bier und deine Verantwortung. Sie mitzuverschlüsseln ist aber vermutlich der einfachste Weg.

Wenn du Angst hast, dein Passwort zu vergessen, kannst du es aufschreiben und **so schnell wie möglich einer vertrauenswürdigen Person übergeben, die nichts mit der LG zu tun hat.** Im Zweifel auch Verwandte, wobei Eltern besser ausgeklammert werden sollten. Nochmal: **Das Passwort muss so schnell es geht aus deiner Wohnung und von deinem Körper weg.**

Manchmal gibt es auch sogenannte Wiederherstellungsschlüssel (z.B. bei Macbooks) - diese sind eine Art spezielles Passwort, das vom Verschlüsselungstool generiert wird und genutzt werden kann, um deine Festplatte zu entschlüsseln. Wenn du dir sicher bist, dass du dein Passwort nicht vergisst, kannst du die Wiederherstellungsschlüssel einfach löschen und vergessen. Ansonsten gelten die gleiche Regeln wie beim Passwort oben: So schnell wie möglich an eine

vertrauenswürdige Person außerhalb der LG geben.

Unabhängig von der Verschlüsselung solltest du dir Gedanken um Backups (Sicherheitskopien) machen. Die Frage ist nicht, ob Festplatten kaputt gehen, sondern wann. Mach dir also vorher Gedanken, welche Daten dir wichtig sind und wie du sie sichern möchtest. Auch das Gerät, auf das du sie sicherst (USB-Stick, externe Festplatte, Dateien in Dropbox), sollte natürlich verschlüsselt sein.

Angriffe auf Festplattenverschlüsselung

Wenn der Computer hochgefahren und gesperrt ist, kann mit einem etwas aufwändigen und nicht immer erfolgreichen Angriff die Verschlüsselung geknackt werden. Der Angriff ist durchaus filmreif, hier eine Demonstration für Windows und hier für Mac.

D.h., wenn der Laptop Gefahr läuft, von der Polizei genommen zu werden, muss er heruntergefahren werden. Wenn es eilt, kann man ihn durch 10-sekündiges Drücken auf den Aus-Knopf auch auf die harte Tour ausschalten. Auch alle Handys, Tablets etc. mit LG-Daten dürfen nicht im Standby bleiben, wenn die Polizei klingelt:

> Standby, Ruhezustand, "Energie sparen", Zuklappen etc. sind leider nicht sicher.

Trotzem gilt: ein verschlüsseltes Gerät ist viel sicherer als ein unerschlüsseltes. Ein Gerät kann ja auch verloren/geklaut werden. Durch die Verschlüsselung sollte euer Gerät nicht langsamer werden.

Biometrische Entsperrungsmerkmale

Bei iPhones und Androids kannst du dir überlegen, die biometrischen Entsperrungsmerkmale zu deaktivieren. Die Polizei kann deinen Finger auf den Homebutton/Fingerabdruckscanner drücken oder das Smartphone vor dein Gesicht halten - das ist aber bei der LG bislang noch nie vorgekommen.

Oder deine Fingerabrdrücke (die sie jetzt ja haben) in eine Attrappe gießen, die sie zum Entsperren nehmen, hier ein Beispiel: Kraken Security Labs Bypasses Biometric Security With $5 In Materials. Das geht theoretisch auch (mit Aufwand) mit deinem Gesicht.

Davon abgesehen hinterlässt dein Fingerabdruck Fett auf dem Sensor, manchmal reicht es, das Fett einfach z.B. mit Anhauchen zu erwärmen.

Die Eingabe von Passwörtern lässt sich jedoch ausspähen, sodass eine gute Variante ist, dass du sehr gut lernst, wie du das biometrische Entsperren in der Hosentasche und über Nacht deaktivieren kannst - damit es in brenzligen Situationen klappt.

Passwörter

Es ist immens wichtig, dass die Passwörter sehr gut gewählt werden und nicht erratbar sind. Zusätzlich ist es äußerst wichtg, dass das Passwort nicht wiederverwendet wird, insbesondere nicht für Onlinedienste wie z.B. Google Mail etc. Außerdem dürfen Passwörter niemals aufgeschrieben und irgendwo "versteckt" werden - das findet die Polizei ziemlich sicher bei einer Hausdurchsuchung. Wenn Angreifende die Festplatte in die Hände kriegen, können sie versuchen, das Passwort herauszufinden, in dem sie automatisiert verschiedene Möglichkeiten durchprobieren. Mit einem herkömmlichen Gamer-PC können zwischen 6.432 und 457.500 Passwörter **pro Sekunde** getestet werden (je nachdem, wie die Platte verschlüsselt wurde) - die Polizei kann sich im Zweifel noch leistungsfähigere Systeme anschaffen, um den Durchsatz weiter zu erhöhen.

Da komplizierte Passwörter schwer zu merken sind, empfehlen wir den Einsatz eines sogenannten Diceware-Passworts. Das sind einfach mehrere **zufällig** ausgewählte Wörter aus einem (deutschen) Wörterbuch mit Leerzeichen getrennt (man kann aber auch andere Trennzeichen verwenden). Hier ein Beispiel:

> speerwerfen gehrock aluminium rotkohl saugt

Unter der Annahme, dass der Angreifende weiß, dass ein Diceware-Passwort verwendet wurde, dass es fünf Wörter lang ist und dass er das Wörterbuch kennt, aus dem das Passwort generiert wurde (in diesem Fall enthält es ~7.000 Wörter), müssen durchschnittlich 14.215.144.014.964.850.000 Passwörter durchprobiert werden, bis das richtige gefunden wurde. Mit den oben genannten Zahlen reden wir hier von einem Aufwand zwischen 985.266 und 70.080.730 Jahren.

Wir empfehlen speziell für die Festplattenverschlüsselung ein Passwort mit vier Wörtern. Hier liegt der Aufwand zwischen 126 und 9.012 Jahren. Bitte benutze das folgende Tool, um das Passwort zu generieren: https://dice.itsnow.biz/

Wenn du das Passwort nicht magst, kannst du einfach so lange ein neues würfeln bis es dir angenehm ist.

Bei Androids und iPhone gelten aus technischen Gründen etwas andere Regeln. Für diese Geräte empfehlen wir eine **zufällig** gewählte Zahlenkombination von mindestens 6 Zeichen. Normale kompliziertere Passwörter sind natürlich auch erlaubt.

Android Gerät verschlüsseln

Grundsätzlich sind alle Smartphones, die mit **Android 6.0 oder höher** laufen standardmäßig **verschlüsselt** und das lässt sich auch nicht ausschalten.

Verschlüsselungsstatus herausfinden

Wollt ihr auf Nummer sicher gehen, lässt sich das oft in den Systemeinstellungen nachgucken. Leider ist die Menustruktur sehr unterschiedlich, abhängig von Android-Version und Gerätehersteller und manchmal die Verlüsselungseinstellung nicht ganz leicht zu erkennen.

So kann die Einstellung z.B. hier liegen:

- `Einstellungen » Sicherheit & Standort » Verschlüsselung & Anmeldedaten » Verschlüsselung`
  oder
- `Einstellungen » Sicherheit » Weitere Einstellungen » Verschlüsselung & Anmeldedaten » Speichertyp Hardwaregestützt`
  oder
- `Einstellungen » Tab Allgemein » Sicherheit » Gerät verschlüsseln`

android-verschluesseln-einstellungen.png
Einstellung für Verschlüsselung
Android 8.0

Bei einigen Androidversionen/Geräteherstellern ist die Verschlüsselung in den Einstellungen gar nicht mehr aufgeführt.

Mit etwas technischen Einsatz bekommt ihr den Verschlüsselungsstatus in jedem Fall über die Kommandozeile mit der Android Debugging Bridge (ADB) heraus. Dazu muss das Gerät über USB mit dem Computer verbunden werden, ADB auf dem Computer installiert und USB-Debbuging aktiviert werden. Eine Anleitung dazu findet ihr hier.

Danach liefert der Befehl `adb shell getprop ro.crypto.state` die Information, ob das Gerät verschlüsselt ist.

android-verschluesseln-adb.png

Das Kommandozeilentool ADB kann den Verschlüsselungsstatus auslesen

Was tun bei Android < 6.0?

Android ist seit der Version 4.0 mit Verschlüsselung ausgestattet, diese wird in 4.0 und 5.0 aber nicht standardmäßig aktiviert. Das könnt ihr über die Einstellungen ähnlich wie oben beschrieben nachholen.

Solltet ihr noch ein Androidgerät < 4.0 haben, nehmt gerne Kontakt zu uns aus der IT-AG auf. Dazu könnt ihr eine Mail an it-support@letztegeneration.org schicken.

SD-Karte/USB-Stick verschlüsseln

Habt ihr sensible Daten auf einer SD-Karte und/oder USB-Sticks abgelegt, solltet ihr darüber nachdenken, diese zu verschlüsseln. Am einfachsten verschlüsselt ihr eure SD-Karte/USB-Sticks mit Veracrypt. Eine Anleitung findest du auf Youtube: https://www.youtube.com/embed/HSeoekvGocs

Windows verschlüsseln mit Bitlocker

Diese Anleitung beschreibt, wie du einen Computer mit Windows verschlüsseln kannst. Es ist immens wichtig, dass du dir auch die allgemeinen Informationen zum Thema Festplattenverschlüsselung durchliest.

Wir empfehlen aktuell die in Windows integrierte Verschlüsselung, die “Bitlocker” genannt wird.

Bitlocker funktioniert nur auf Pro und Enterprise Editionen von Windows. In dieser Anleitung wird beschrieben, wie du herausfindest, welche Edition du hast und wie du sie umwandeln kannst.

Wenn dein Gerät verschlüsselt ist, lies bitte auch diesen wichtigen Hinweis.

Ist die Verschlüsselung schon aktiv?

Es kann gut sein, dass dein Rechner schon verschlüsselt ist. Um das herauszufinden, drücke die Windows-Taste auf der Tastatur und gebe "Bitlocker" ein. Dann:

- kommt eine Bing-Suche, wenn deine installierte Windows-Edition nicht ausreicht (siehe unten für mehr Details)
- falls Bitlocker unterstützt wird, klicke auf das Bitlocker-Symbol. Dann siehst du
  - den Text „Bitlocker deaktiviert“, wenn nichts verschlüsselt ist
  - „aktiviert“, wenn deine Festplatte bereits verschlüsselt ist

Windows-Edition herausfinden

1. Windowstaste und X gleichzeitig drücken
2. Menüpunkt „System“ auswählen.
3. Unter der Überschrift „Windows Spezifikationen“ steht die Windows-Edition. Wenn da steht „Windows 10 Home“ dann folge bitte weiter dieser Anleitung. Wenn da “Windows 10 Pro” oder „Windows 10 Enterprise“ steht kannst du zu „Verschlüsselung aktivieren (1. Schritt)“ springen.

   windows_version.png

Windows-Edition ändern

Bitte einen entsprechenen Key kaufen. Die IT-AG kann dich dabei unterstützen.

Verschlüsselung aktivieren (1. Schritt)

1. Windowstaste drücken, “Bitlocker” eingeben und “Bitlocker verwalten” anklicken.

2. Nun kann es sein, dass du die folgende Meldung erhältst:

Wenn das der Fall ist, folge bitte dieser Anleitung weiter. Wenn das nicht der Fall ist springe zu “Verschlüsselung aktivieren (2. Schritt)”.

Verschlüsselung aktivieren (TPM-Fehler beheben)

Um diesen Fehler zu beseitigen bitte folgendes tun:

1. “Abbrechen” klicken.
2. Windowstaste zusammen mit R drücken und in das Dialogfelg "gpedit.msc" und Enter drücken.

2. Links folgendes auswählen: “Administrative Vorlagen”, “Windows Komponenten”…

3. … “Bitlocker-Laufwerksverschlüsselung”, “Betriebssystemlaufwerke”.

4. Auf der rechten Seite “Zusätzliche Authentifizierung beim Start anfordern” doppelklicken:

5. Im folgenden Dialogfeld sicherstellen, dass links oben “Aktiviert” ausgewählt ist und weiter unten “BitLocker ohne kompatibles TPM zulassen […]”. Danach auf OK drücken.

6. Das Gruppenrichtlinienfenster schließen.

7. Im Bitlocker-Fenster nochmal “Bitlocker aktivieren” anklicken.

8. Laufwerke sollten nur mit Passwort entsperrt werden, entsprechendes anklicken:

9. Jetzt ein Kennwort vergeben. Bitte lies dir unseren allgemeinen Hinweise zum Thema Verschlüsselung durch - das ist wichtig, damit dein Computer auch wirklich geschützt ist.

Verschlüsselung aktivieren (2. Schritt)

1. Windows zwingt dich nun, Wiederherstellungsschlüssel für die Festplatte zu speichern - auch wenn du das gar nicht willst. Lies dir bitte zum Thema Wiederhestellungsschlüssel unsere allgemeinen Hinweise zum Thema Verschlüsselung durch. Speichere den Wiederherstellungsschlüssel auf keinem Fall in deinem Microsoft-Konto oder auf einem USB-Stick! Wähle stattdessen “Wiederherstellungsschlüssel drucken”. Hinweis: es kann sein, dass hier weitere Optionen angezeigt werden, die nicht auf dem Screenshot unten zu sehen sind.

1. Wähle als Drucker “Microsoft Print to PDF”.

1. Vergebe einen Namen und speichere die PDF auf dem Desktop.

Wenn du die Wiederherstellungsschlüssel nicht an einen vertrauenswürdigen Menschen geben willst, dann lösche sie gleich wieder. Halte dich ansonsten an die Regeln aus den allgemeinen Hinweisen zur Verschlüsselung.

Klicke auf “Weiter”.

Wähle im folgenden Dialogfenster “Gesamtes Laufwerk verschlüsseln”, dann “Weiter”:

1. Den Verschlüsselungsmodus auf “Neuer Verschlüsselungsmodus” lassen, “Weiter” klicken:

   Verschlüsselungsmodus

1. “Bitlocker-Systemüberprüfung ausführen" muss ausgewählt sein, wieder “Weiter” drücken:

   Jetzt verschlüsseln bestätigen

1. Und nun den Computer “Jetzt neu starten”.

1. Der Computer wird jetzt verschlüsselt. Das dauert eine Weile, er kann jedoch dabei weiter verwendet werden, wobei er am Anfang etwas langsam sein kann. Wenn Bitlocker dir ein weiteres Festplattenlaufwerk zum Verschlüsseln anbietet, dann verschlüssle auch das.

Siehe auch

VeraCrypt ist eine Alternative zum Verschlüsseln von Windows. Der Vorteil ist, dass keine Pro-Lizenz von Windows nötig ist. Leider birgt die Verschlüsselung bei VeraCrypt das Risiko, dass durch das Verschlüsseln der Rechner unwiederbringlich unbenutzbar wird. Daher ist es wichtig, vor dem Verschlüsseln des Rechners ein Backup zu machen.

wichtiger Hinweis: Recovery Key im Microsoft Account

Es gibt einen Recovery Key, mit dem die Festplatte entschlüsselt werden kann. Den brauchst du, wenn dein Laptop kautt ist, du die Festplatte ausbauen möchtest und an einen anderen Rechner anschließt/einbaust und von da auf deine Daten zugreifen möchtest. Dieser Recovery/Wiederherstellungs-Key ist bei vielen im Microsoft Account gespeichert. Wenn ihr den Laptop verschlüsselt werdet ihr danach gefragt, wo ihr den Recovery-Key speichern wollt. Eine Option ist "in der Microsoft Cloud". Wir empfehlen, den Key auszudrucken und an einem Sicheren Ort zu verwahren (Freunde/Familie, auf jeden Fall außerhalb der Wohnung).

Falls die Polizei euren Rechner beschlagnahmt und die Festplatte verschlüsselt ist, kann die Polizei nicht auf die Daten zugreifen. Theoretisch kann sie aber bei Microsoft fragen, ob ihr den Recovery

Key bei ihnen gespeichert habt (wir wissen nicht, ob das passiert).

Dementsprechend empfehlen wir, zu schauen, ob ihr den bei Microsoft gespeichert habt. Wenn ja, dort bitte löschen. Hier gibt's zwei Anleitungen, um den den Recovery Key im Microsoft Account zu löschen (bislang ungetetstet, gerne Rückmeldung geben):

1. How to find your BitLocker recovery key -> im Video ist ein löschen/delete Button zu sehen
2. Ansonsten ist der Key wohl auch im OneDrive zu finden, siehe dazu:
   - https://www.thewindowsclub.com/delete-bitlocker-recovery-key-from-onedrive-in-windows-10

Prozessvorschlag für die Verschlüsselung ist demnach:

- beim Verschlüsseln neuer Systeme mit Bitlocker: den Recovery Key nicht im Microsoft Account speichern, sondern ausdrucken/aufschreiben und nicht-LG-Menschen geben
- wenn Menschen schon verschlüsselte Windows-Rechner haben: checken, ob der Recovery Key im Microsoft Account hinterlegt ist; wenn ja: löschen

Windows verschlüsseln mit Veracrypt

Windows verschlüsseln mit VeraCrypt

Wir empfehlen die Verschlüsselungsart VeraCrypt nur in technischen Ausnahmefällen. Bitte nutze wenn möglich BitLocker.

Bitte lies dir im Vorfeld **unbedingt** die allgemeinen Hinweise zum Thema Verschlüsselung durch.

Wenn du auf deinem Computer mehrere Betriebssysteme hast, bitte kontaktiere die IT-AG. Wenn du nur Windows benutzt und nichts von einem weiteren Betriebssystem weißt, kannst du die Anleitung einfach befolgeden.

1. VeraCrypt herunterladen:
   https://github.com/veracrypt/VeraCrypt/releases/download/VeraCrypt_1.26.24/VeraCrypt_Setup_x64_1.26.24.msi
2. VeraCrypt installieren. Dabei gibt es nichts besonderes zu beachten.
3. VeraCrypt starten, z.B. über das StartMenü.
4. Im Menü oben „*System > Encrypt System Partition/Drive*“ auswählen.

   veracrypt_system2.png

5. Im Dialogfeld „Type of System Encryption“ „Normal“ auswählen.

   veracrypt_system3.png

6. Im Dialogfeld „Area to Encrypt“ wenn möglich „Encrypt the whole drive“ auswählen. Manchmal ist das aus technischen Gründen nicht möglich, dann eben „Encrypt Windows System Partition“ auswählen.

   bios_vs_gpt.png

7. Sollte nun die folgende Fehlermeldung erscheinen, diese mit „Ja“ bestätigen.

recovery_partition.png

8. Bei „Number of Operating Systems“ „Single-boot“ auswählen.

8. Im Dialogfeld „Encryption Options“ die bereits gesetzten Einstellungen bestätigen (AES, SHA-256).

9. Im Dialogfeld „Passwort“ ein Passwort vergeben. An dieser Stelle nochmal der wichtige Verweis zum Dokument Allgemeinen Hinweise zum Thema Verschlüsselung. Mit diesem Passwort steht und fällt ob dich die Verschlüsselung schützt.

10. Alle anderen Optionen nicht aktivieren.

11. Wenn das Password unter 20 Zeichen lang ist, kann es sein, dass die folgende Fehlermeldung erscheint:

bruteforce.png

Wenn das gewählte Passwort den Regeln aus Allgemeinen Hinweise zum Thema Verschlüsselung entspricht, kann diese Meldung mit „Ja“ ignoriert werden.

12. Im Dialogfeld „Collecting Random Data“ muss solange die Maus durch die Gegend bewegt werden, bis der Balken unten voll & grün ist.

Das sieht dann so aus:

randomness.png

13. Nach einem Klick auf „Next“ erscheint das Dialogfeld „Keys Generated“, das mit „Next“ weitergeklickt werden kann:

14. VeraCrypt möchte nun eine sogenannte Rescue Disk erstellen. Das ist entweder ein USB-Stick oder eine CD. In sehr seltenen Fällen kann es passieren, dass der Teil von VeraCrypt kaputt geht, der deine Festplatte entschlüsselt - du könntest dann deinen Computer nicht mehr starten, da deine Platte nicht mehr entschlüsselt werden kann.

Wenn jemand diese Rescue Disk in die Finger bekommt kann dieser Mensch nicht deinen Computer entschlüsseln - es wird immer noch das Passwort benötigt.

Die Rescue-Disk stellt dir VeraCrypt als sogenanntes Image zur Verfügung, das kann auf einen USB-Stick ausgerollt werden oder auf eine CD gebrannt. Wir raten dir, dass du das erstmal einfach nur auf einen (oder mehrere) USB-Sticks kopierst. Solltest du in die Verlegenheit kommen, das zu brauchen, kannst du dich bei der IT melden.

15. Aktiviere „Skip Rescue Disk verification“, da wir die Disk noch nicht so fertig einrichten, wie VeraCrypt das erwartet - wir machen das, wenn die Disk wirklich gebraucht würde. Dann „Next“.

16. Als „Wipe Mode“ „None“ einstellen. Dann „Next“.

17. VeraCrypt möchte nun testen, ob dein Computer ohne Probleme verschlüsselt werden kann. Dabei werden noch keine Daten verschlüsselt - wenn der Test erfolgreich war fragt dich VeraCrypt nochmal. Einmal „Test“ klicken.

18. Im nächsten Fenster dann „OK“ klicken:

19. VeraCrypt weißt dich nun darauf hin, dass der Computer neugestartet wird. Einmal bestätigen:

test_restart.png

20. Nach dem Neustart fragt dich VeraCrypt nach deinem Passwort, nach der Eingabe Enter drücken:

boot_password.png

21. “PIM” einfach leerlassen, Enter drücken:

boot_password_2.png

22. Dann entschlüsselt VeraCrypt deine Platte (die allerdings bei diesem ersten Neustart noch nicht verschlüsselt ist, das ist nur ein Test):

boot_password_3.png

23. Nach dem Neustart meldet VeraCrypt mit sehr hoher Wahrscheinlichkeit, dass der Test erfolgreich war. Mit Klick auf „Encrypt“ kann es losgehen:

24. Das will Windows aber noch einmal freigegeben haben, einmal „Ja“ klicken:

encrypt_admin.png

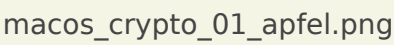
25. Dein Computer wird jetzt verschlüsselt! Du kannst ihn ganz normal weiterbenutzen während das passiert, es könnte nur etwas langsamer als sonst sein. Du kannst ihn sogar herunterfahren - allerdings gibt es dann ggf. noch Teile, die nicht verschlüsselt sind.

macOS verschlüsseln

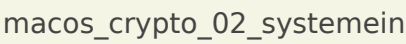
> UPDATE 10/2023: Die Polizei kann die Verschlüsselung nicht umgehen und beißt sich die Zähne daran aus.

In der Regel sind aktuelle Macbooks schon verschlüsselt. Ob das der Fall ist, kann man so nachprüfen:

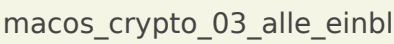
Zuerst links oben auf den Apfel klicken.


macos_crypto_01_apfel.png

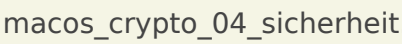
Dann auf “Systemeinstellungen” klicken.


macos_crypto_02_systemeinstellungen.png

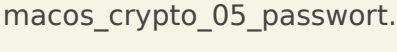
Dann einmal zur Sicherheit auf den Button mit den 4x3 Punkten klicken:


macos_crypto_03_alle_einblenden.png

Dann auf “Sicherheit” klicken. Manchmal heißt das auch “Sicherheit & Privatsphäre”.


macos_crypto_04_sicherheit.png

Unter dem Reiter “Allgemein” zuerst prüfen, dass “Passwort erforderlich” aktiviert ist und auf “5 Minuten” eingestellt ist. Wenn nicht entsprechend ändern. **ES IST IMMENS WICHTIG, EIN GUTES PASSWORT ZU WÄHLEN**. Bei macOS ist das Passwort zum Entsperren des Macs auch das Passwort, mit dem die Festplatte verschlüsselt wird. Siehe dazu die Wikiseite "Allgemeines zum Thema Festplatten-Verschlüsselung".


macos_crypto_05_passwort.png

Dann auf “FileVault” klicken.

Wenn da “FileVault ist für die Festplatte Macintosh aktiviert” steht, ist die Verschlüsselung an. Manchmal heißt die Festplatte auch anders.

macos_crypto_06_verschlüsselung_aktiviert.png

Wenn die Verschlüsselung nicht aktiviert ist, sieht das so aus:

macos_crypto_07_verschlüsselung_deaktiviert.png

Zum Aktivieren der Verschlüsselung auf das Schloß klicken und das Passwort eingeben:

macos_crypto_08_passwort_eingeben.png

Im nächsten Fenster ist es wichtig, “Wiederherstellungsschlüssel erstellen [...]” auszuwählen – die Polizei kann sich sonst die Unterstützung von Apple holen, um die Festplatte zu entschlüsseln.

macos_crypto_09_key_icloud.png

Den Wiederherstellungsschlüssel abschreiben **UND EINER VERTRAUENSWÜRDIGEN PERSON GEBEN, DIE NICHTS MIT LG ZU TUN HAT**. Vorzugsweise Freunde, bei Familie die Eltern zur Sicherheit aussparen (stattdessen Tante, Cousine, Onkel, etc.). Es ist immens wichtig, dass der Wiederherstellungsschlüssel SO SCHNELL ES GEHT aus eurem Wohnraum und von eurem Körper weg verschwindet. Wer risikobereit ist, kann den Schlüssel auch ignorieren und vergessen. Er hilft euch die Festplatte zu entschlüsseln, wenn ihr euer Passwort vergisst.

macos_crypto_10_wiederherstellungskey.png

Nun wird die Festplatte verschlüsselt, währenddessen kann der Mac einfach weiterbenutzt werden.

macos_crypto_11_verschlüsselung_in_progress.png

Weitere Links

https://github.com/drduh/macOS-Security-and-Privacy-Guide

Festplattenvollverschlüsselung mit Ubuntu Installation

Festplattenvollverschlüsselung bei Ubuntu Neuinstallation

Schritte

1. Erstelle ein USB Stick mit Ubuntu
2. Starte dein Computer von den USB Stick
3. Ubuntu Installation mit Festplattenvollverschlüsselung

1. Erstelle in Bootable USB Stick

2. Starte den Computer vom USB-Stick

> Dieser Schritt ist leider sehr herstellerabhängig. Die Hersteller haben unterschiedliche Methoden um beim Start des Computers in das Boot Menü zu

> kommen. Gängige Tasten sind ESC, F2, F10, F12 oder F11. Im Zweifel die Marke/Modell des Computers suchen. z.B “Lenovo T480p Boot menu key” oder mal alle Tasten drücken ;-)

Beispiel mit Dell Laptop

3. Setup Guide mit Festplattenvollverschlüssel (bis 4:45)

veracrypt

Veracrypt installieren auf Windows/Linux/Mac

Einführung Veracrypt

Veracrypt ist ein Tool, mit dem Festplatten oder USB-Sticks verschlüsselt/entschlüsselt werden können. Veracrypt ist quelloffen (Open Source) und existiert für alle Betriebssysteme (Windows, Linux und Mac). Diese Seite erklärt, wie du Veracrypt installierst und die Sprache auf Deutsch stellst.

> Eventuell ist Veracrypt bereits auf deinem Gerät installiert. Du kannst in deinem Startmenü einfach mal nach Veracrypt suchen. {.is-info}

Installation

Die Installation hängt von eurem Betriebssystem ab.

Veracrypt auf Windows installieren

1. Geh dazu auf die Webseite von Veracrypt (leider nur auf Englisch verfügbar): https://veracrypt.io/en/Downloads.html
2. Im Abschnitt "Windows", kannst du die Installations-Datei herunterladen. Das ist der erste Download-Link in der Windows-Liste: *EXE Installer (x64 and ARM64): VeraCrypt Setup 1.xx.xx.exe*"
3. Wenn du die Datei heruntergeladen hast, befindet sie sich im Downloads Ordner. Führe die Datei mit einem Doppelklick aus.
4. Es startet sich der Installations-Assistent. Den musst du durchklicken. Dabei gibt es eigentlich nichts besonderes zu beachten
5. Anschließend findest du Veracrypt im Startmenü

Falls du Probleme damit hast, kannst du dir auch dieses Video anschauen, das die Installation zeigt: https://www.youtube.com/watch?v=h1Fth3invJI

Veracrypt auf Linux (Ubuntu/Mint) installieren

Leider befindet befindet sich Veracrypt bei Linux (egal ob Ubuntu oder Mint) nicht in den offiziellen Paketquellen. Das heißt, du kannst nicht einfach die Software-Verwaltung öffnen und Veracrypt installieren.

Du installierst Veracrypt am Besten mit diesen Befehlen auf der Kommandozeile:

1. Terminal/Kommandozeile öffnen (suche im Startmenü nach einer Anwendung Namens "Terminal")
2. Gebe anschließend die folgenden drei Befehle ein. Du wirst dabei nach deinem Benutzer:innen-Passwort gefragt Du kannst die Befehle auch kopieren. Das Einfügen im Terminal geht mit *Strg + Shift + V* .

```
sudo add-apt-repository ppa:unit193/encryption -y
```

```
sudo apt update
```

```
sudo apt install -y veracrypt
```

3. Wenn alles geklappt hat, solltest du ab jetzt Veracrypt im Startmenü finden.

Falls du Probleme hattest: In diesem Video siehst du, wie jemand diese Schritte ausführt: https://www.youtube.com/watch?v=hqbVFiUGH9I

Veracrypt auf Mac installieren

Die nachfolgenden Schritte sind für MacOS Monterey 12 und neuer. Auf einem Mac musst du zwei Programme installieren: "macFUSE" (ein Hilfsprogramm, das Veracrypt im Hintergrund nutzt) und Veracrypt selbst.

1. Gehe auf die Webseite von Veracrypt: https://veracrypt.io/en/Downloads.html
2. Dort findest du in der Liste "macOS"
3. Öffne den "macFUSE" Link in einem neuen Tab. Rechts kannst du "macFUSE 5.x.x" herunterladen

4. Downloade Veracrypt von der Veracrypt Webseite. Klicke dazu auf "VeraCrypt_1.xx.xx.dmg" (auch in der macOS Liste
5. Nun musst du beide Installations-Datein ausführen und installieren. Es ist wichtig, dass du macFUSE als erstes installierst.

Wenn du Probleme dabei hattest, kannst du dir auch dieses Video anschauen: https://www.youtube.com/watch?v=8epKaZqznVI

Wie geht's weiter?

- Sprache in Veracrypt auf Deutsch stellen
- Festplatte/USB-Stick mit Veracrypt verschlüsseln
- Festplatte/USB-Stick mit Veracrypt entschlüsseln/benutzen
- Veracrypt Passwort ändern

Sprache einstellen - Veracrypt auf Deutsch stellen

Sprache einstellen - Veracrypt auf Deutsch stellen

Leider lässt sich Veracrypt nur auf Windows auf Deutsch stellen. Auf Linux und Mac musst du leider mit der englisch-sprachigen Version arbeiten.

Zunächst startest du die Veracrypt Anwendung.

Veracrypt in englischer Sprache

Als nächstes gehst du oben in der Menüleiste auf 'Settings' und anschließend auf "Langauge".

Menüleiste

Anschließend wählst du die gewünscht Sprache aus.

Auswahl der deutschen Sprache

Nach einem Klick auf "OK" hast du Veracrypt auf Deutsch umgestellt.

04_veracrypt_2025-10-14_18-16-38_006.png

Wie geht's weiter?

- Festplatte/USB-Stick mit Veracrypt verschlüsseln
- Festplatte/USB-Stick mit Veracrypt entschlüsseln/benutzen
- Veracrypt Passwort ändern

veracrypt

Festplatte/USB-Stick mit Veracrypt verschlüsseln

Festplatte/USB-Stick mit Veracrypt verschlüsseln

Diese Anleitung beschreibt, wie du einen externen Datenträger verschlüsseln kannst. Ein externer Datenträger ist zum Beispiel eine externe Festplatte oder ein USB-Stick. Die Verschlüsselung muss nur einmalig eingerichtet werden. Wie du deinen verschlüsselten Datenträger entschlüsseln/benutzen kannst, wird hier beschrieben.

Vorbereitung: Folgende Dinge solltest du vorbereitet haben

> - **Mach zunächst ein Backup deiner Dateien. Beim Verschlüsseln/Formatieren des Datenträgers gehen alle Dateien verloren.**
>   - Wenn dein Datenträger eine NTFS-Partition enthält, können die Dateien auch "in-place" verschlüsselt werden. Heißt die existierenden Dateien werden verschlüsselt ohne dass sie vorher gebackuped werden müssen...

    - Ob das bei dir geht, siehst du am einfachsten, wenn du der Anleitung folgst und die entsprechende Option ("in-place Verschlüsselung) bei dir auftaucht.
- Du musst Veracrypt installiert haben (Anleitung)
- Du kannst in Veracrypt die Sprache auf Deutsch stellen, wenn dir das lieber ist
- Du brauchst einen externen Datenträger, den du verschlüsseln möchtest
- Du musst dir ein gutes Passwort überlegen
- Die Verschlüsselung benötigt Zeit - wie viel hängt von der Größe des Datenträgers und der Art der Formatierung ab (mehr dazu unten) {.is-info}

Anleitung: Verschlüsselung mit Veracrypt einrichten

Nachdem du Veracrypt gestartet hast, gehst du in der Menüleiste auf "Volume" und anschließend auf "Neues Volume erstellen".

Menüleiste Neues Volume erstellen

In dieser Anleitung verschlüsseln wir den gesamten Datenträger. Wähle "Partition bzw. Laufwerk verschülsseln".

Laufwerk verschlüsseln

Wähle im nächsten Schritt "Standard-VeraCrypt-Volume", um ein normales Veracrypt Volume zu erstellen.

Standard Veracrypt Volume auswählen

> Meistens enthalten Datenträger eine einzige Partition. Dein Datenträger kann aber auch mehrere Partitionen oder gar keine Partition haben. Du kannst Partitionen auch vergrößern, verkleinern oder löschen. Dies wird allerdings nicht in dieser Anleitung erklärt. Der USB-Stick, der hier verschlüsselt wird, enthält

> keine Partition. Letztendlich ist egal, ob dein Datenträger eine Partition hat (und du die verschlüsselst) oder der gesamte Datenträger (ohne Partition) verschlüsselt wird. {.is-info}

> Die Warnung (siehe unten) weißt dich darauf hin, dass Betriebssysteme die Festplatte in Zukunft nicht erkennen (da sie verschlüsselt ist) und dir vorschlagen, diese zu formatieren (da keine Partitionstabelle/Partitionen exisitieren). Du solltest darauf achten, nicht versehentlich deinen Datenträger zu formatieren, wenn du die Festplatte einsteckst. Das passiert aber auch nicht nebenbei, du würdest es aktiv mitbekommen und müsstest dies explizit bestätigen. {.is-warning}

Bestätige die Warnung mit "Ja" (gesamtes Gerät verschlüsseln), um mit der Verschlüsselung fortzusetzen. Wenn du eine Partition verschlüsselst, wird diese Warnung bei dir nicht erscheinen.

Bestätigen, dass kompletter Datenträger verschlüsselt werden soll

---

Klicke auf "Datenträger". Es öffent sich dann ein neues Fenster, in dem du den Datenträger auswählen kannst, den du verschlüsseln möchtest.

Datenträger auswählen, der verschüsselt werden soll

In diesem Fenster (siehe unten) wählst du den Datenträger aus, den du verschlüsseln möchtest.

> Die Spalte "Größe" hilft dir, deinen Datenträger in der Liste zu finden. {.is-info}

> Wenn dein Datenträger keine Partition enthält, wähle den Datenträger aus (wie hier im Bild). Wenn der Datenträger eine Partition enthält, wähle die Partition aus. {.is-info}

Laufwerk bzw Partition auswählen

Im nächsten Schritt hast du zwei Optionen. Im Normalfall wählst du "verschlüsseltes Volume erstellen und formatieren". Dabei gehen (später, wenn du "Formatieren" klickst) alle Dateien auf dem Datenträger verloren. Deshalb ist es wichtig, dass du die Dateien vorher backupst.

> Wenn der Datenträger eine NTFS-Partition enthält, kannst du die Partition "in-place" verschlüsseln. Dadurch gehen die bereits gespeicherten Dateien nicht verloren. Der Vorgang dauert sehr lange. {.is-info}

Datenträger formatieren

Bei den Verschlüsselungseinstellungen kannst du die Standardeinstellungen lassen wie sie sind und auf "Weiter" klicken.

Verschlüsselungseinstellungen

Hier wird dir nochmal zur Überprüfung angezeigt, wie groß der ausgewählte Datenträger ist. In unserem Beispiel sind es 3.75 GB.

> Es ist normal, dass die Größe kleiner ist, als du sie vielleicht erwartest. {.is-info}

Fahre fort mit "Weiter".

Volume Größe überprüfen

Überlege dir nun ein sicheres Passwort und gib es zwei mal ein.

> Für das Passwort kannst du dir fünf zufällige Wörter ausdenken. Mach dir noch Gedanken zur Groß- und Kleinschreibung und dem Trennzeichen. Im unserem Beispiel sind alle Wörter klein geschrieben und durch ein Leerzeichen getrennt. {.is-info}

> Wenn du das Passwort vergisst, sind deine Daten für immer verloren! Speichere deshalb dein Passwort am Besten gleich in deinem Passwort-Manger ab. Das gilt vorallem für Datenträger, die du selten nutzt. {.is-warning}

> Du kannst das Passwort auch später wieder ändern. {.is-info}

Passwort eingeben

Wenn im nächsten Schritt die Festplatte formatiert wird, gehen alle Daten auf dem Datenträger verloren. Dies musst du hier bestätigen.

> Mach unbedingt vorher ein Backup von den Daten, wenn sich auf dem Datenträger aktuell noch von Daten befinden. Am Ende des Einrichtungs-Assistenten hast du einen verschlüsselten, aber leeren Datenträger. {.is-warning}

Wenn du deine Daten gebackuped hast, klicke auf "Ja".

Bestätigung Datenträger wird formatiert

Im nächsten Schritt kannst du das Dateisystem auswählen.

> **Welches Dateisystem soll ich auswählen?** Benutzt du ausschließlich Windows, dann wähle "NTFS". Ansonsten wähle "exFAT" aus. "exFAT" wird von allen gängigen Betriebssystemen unterstützt (Windows, Linux, Mac). {.is-info}

Dateisystem auswählen

Im gleichen Fenster kannst du rechts oben die Art der Formatierung auswählen (siehe Bild unten).

> **Welche Formatierung soll ich auswählen?**
>
> - Wähle "Schnellformatierung", wenn auf dem Datenträger vorher nichts gespeichert war (z. B. neu gekauft). Die Schnellformatierung ist meist in wenigen Minuten erledigt.
> - Wähle "Vollformatierung", um alle bisher unverschlüsselten Dateien zu überschreiben. Die Vollformatierung benötigt sehr lange. {.is-info}

> Erklärung: Nach der Aktivierung/Einrichtung der Verschlüsselung werden alle Dateien, die du neu speicherst, verschlüsselt auf dem Datenträger gespeichert. Wenn du allerdings vorher unverschlüsselte Daten auf dem Datenträger gespeichert hattest, solltest du die "Vollverformatierung" nutzen. Dabei wird der komplette Datenträger mit Nullen (00000...) beschrieben, um zwar gelöschte (durch die Formatierung), aber noch wiederherstellbare Dateien zu überschreiten. {.is-info}

>

> Bewege deine Maus in dem Fenster. Das gibt Veracrypt mehr Zufall (Entropie) und sorgt für eine bessere Verschlüsselung (siehe Mitte unten im Fenster). {.is-info}

Vollformatierung auswählen

Klicke anschließend auf "Formatieren", um die Verschlüsselung/Formatierung zu starten. Dir wird auch angezeigt, wie lange der Vorgang noch etwa dauert.

Formatierung Verschlüsselung wird eingerichtet

Herzlichen Glückwunsch! Dein Datenträger wurde erfolgreich verschlüsselt.

Die Verschlüsselung wurde erfolgreich eingerichtet

Du kannst den Einrichtungs-Assisten nun beenden.

> Wie du deinen verschlüsselten Datenträger nun verwenden/entschlüsseln kannst, erfährst du in der Anleitung hier. {.is-info}

Der Assistent kann beendet werden

veracrypt

Festplatte/USB-Stick mit Veracrypt entschlüsseln/benutzen

Festplatte/USB-Stick mit Veracrypt entschlüsseln/benutzen

Diese Anleitung zeigt dir, wie du mit Veracrypt deinen bereits verschlüsselten Datenträger (externe Festplatte oder USB-Stick) mit Veracrypt entschlüsseln/benutzen kannst.

Hinweise

> - Du brauchst drei Dinge: Veracrypt, den Datenträger und das Passwort
> - Falls du Veracrypt noch nicht installiert hast, gibt es hier eine Anleitung.
> - Dein Datenträger muss bereits verschlüsselt sein. Das ist ein einmaliger Vorgang. Falls das noch nicht passiert ist, gibt es hier eine passende Anleitung. {.is-info}

Anleitung

> Die Bezeichnungen in Veracrypt sind etwas verwirrend:
>
> - "Einhängen" (im englischen "Mount") bedeutet das Entsperren/Entschlüsseln eines Datenträgers
> - "Trennen" (im englischen "Unmount") beendet die Entschlüsselung. Das nutzt du, wenn du mit deinen Arbeiten fertig bist und du den Datenträger entfernen möchtest. {.is-info}

Als erstes startest du Veracrypt. Mit einem Klick auf "Datenträger" öffnet sich ein neues Fenster, in dem du den Datenträger auswählen kannst, den du entschlüsseln möchtest.

Veracrypt Fenster

Hier wählst du den Datenträger aus und klickst auf "OK".

Datenträger auswählen

> Die Spalte "Größe" hilft, dir deinen Datenträger zu finden. {.is-info}

> Wenn dein Datenträger eine Partition enthält, wähle die Partition und nicht den Datenträger aus. Der Datenträger im Screenshot enthält keine Partitionen. {.is-info}

(leider kein Screenshot) Als nächstes wählst noch einen leeren Laufwerksbuchstaben aus. Dazu klickst du auf eine der leeren Zeilen (in der Mitte des Fensters). Um die Festplatte zu entschlüsseln, gehe links unten auf Einhängen (im englischen "Mount"). Es öffnet sich ein neues Fenster, in dem du dein Passwort eingeben musst.

Hier kannst du dein Passwort eingeben und klickst auf "OK".

Passwort eingeben

Die Entschlüsselung dauert ein paar Sekunden. Unter Linux wirst du hier nochmal nach deinem Benutzer*innen-Passwort gefragt.

04_veracrypt_2025-10-14_18-38-31_029.png

So sieht das Veracrypt-Fenster aus, wenn die Entschlüsselung erfolgreich war. Der Datenträger ist nun entschlüsselt und steht im Datei-Explorer als Laufwerksverzeichnis (A:) zur Verfügung (siehe ganz links in der Splate (LW=Laufwerk)).

Datenträger ist entschüsselt

> Tipp: mit einem Doppelklick auf den entschlüsselten Datenträger (der blauen Zeile im Screenshot) öffnet sich der Datei-Explorer und zeigt dir deine entschlüsselten Dateien an. {.is-info}

> Unter Linux gibt es keine Laufwerksbuchstaben. Dort wird der entschlüsselte Datenträger aber ebenfalls als "virtuelle Festplatte" im Dateisystem eingehängt. {.is-info}

Öffne im Datei-Explorer den "Arbeitsplatz" oder "Dieser PC". Dein verschlüsselter Datenträger wird als "virtuelle Festplatte" angezeigt (wie oben beschrieben als Laufwerksbuchstabe A). Dort findest du alle Dateien, die sich auf dem Datenträger befinden. Alle Sachen, die sich dort befinden, speichert Veracrypt verschlüsselt auf dem Datenträger.

Entschlüsselten Datenträger im Datei-Explorer anzeigen

Wenn du mit deinen Arbeiten fertig bist und den Datenträger entfernen möchtest, kannst du auf "Alle Datenträger trennen" (im englischen "Unmount all" klicken.

> Deine Daten sind zu jedem Zeitpunkt verschlüsselt gespeichert. Auch wenn du die Festplatte/USB-Stick einfach raus ziehst. Das "Aushängen/Trennen" wird aber empfohlen. Damit entfernst du den Datenträger sauber. {.is-info}

Datenträger wieder aushängen

Gut gemacht :)

veracrypt

Veracrypt Passwort ändern

Veracrypt Passwort ändern

Hinweise

> - Du brauchst drei Dinge: Veracrypt, den Datenträger und das Passwort
> - Falls du Veracrypt noch nicht installiert hast, gibt es hier eine Anleitung.
> - Dein Datenträger muss bereits verschlüsselt sein. Das ist ein einmaliger Vorgang. Falls das noch nicht passiert ist, gibt es hier eine passende Anleitung. {.is-info}

Anleitung

1. Als erstes startest du Veracrypt
2. Entschlüssele/Entsperre deinen Datenträger (Anleitung zum Entschlüsseln),
3. Wähle den entschlüsselten Datenträger aus (die blaue Zeile im Screenshot),
4. Gehe in der Menüleiste auf "Volume", dann auf "Volume-Passwort ändern". Es öffnet sich ein neues Fenster.

Veracrypt Menüleiste

Als nächstes kannst du das Passwort ändern. Dazu gibst du einmal das aktuelle und zwei mal das neue Passwort ein. Bestätige mit einem Klick auf "OK.

Passwort ändern Dialog

Zur Verbesserung der Verschlüsselung (Zufall/Entropie) sollst du nun den Mauszeiger innerhalb des Fensters bewegen. Unten im Fenster befindet sich ein Ladebalken, bei dem du den Fortschritt sehen kannst. Klicke auf "Fortsetzen".

Entropie - Maus bewegen

Das Passwort wird geändert. Unter Linux wirst du hier nochmal nach deinem Benutzer*innen-Passwort gefragt. Der Vorgang sollte nur ein paar Sekunden dauern.

Ladebalken - Passwort wird geändert

Das Passwort wurde erfolgreich geändert.

Dialog - Passwort wurde geändert

Allgemeines zur Festplattenvollverschlüsselung

Wenn du Fragen zur Verschlüsselung hast, kannst du dich gerne bei uns melden. Schreibe dazu einfach eine E-Mail an it-support@raz-ev.org

Risiken

Wenn du deine Festplatte verschlüsselst und das Passwort vergisst, gilt: Alle deine Daten sind weg - niemand kann sie wieder retten. Du musst dir dieses Risikos bewusst sein.

Lasst uns kurz unterscheiden:

- Auf deinem Gerät sind Daten von deinem Engagement bei der Letzte Generation (LG)
- Vielleicht sind darauf auch ganz persönliche, private Daten (Kinderfotos, Steuererklärung, ...)

Wenn du deine privaten Daten, also die Daten, die nicht zu LG gehören, sichern willst, kannst du sie auch unverschlüsselt auf eine externe Festplatte oder mit einem Dienst wie Dropbox speichern. Der Grund, warum wir Laptops verschlüsseln, ist es, dich und andere vor den Konsequenzen der Arbeit mit der LG zu schützen und zu verhindern, dass die Polizei die Orga stören kann. Deine privaten Daten sind dein Bier und deine Verantwortung. Sie mitzuverschlüsseln ist aber vermutlich der einfachste Weg.

Wenn du Angst hast, dein Passwort zu vergessen, kannst du es aufschreiben und **so schnell wie möglich einer vertrauenswürdigen Person übergeben, die nichts mit der LG zu tun hat.** Im Zweifel auch Verwandte, wobei Eltern besser ausgeklammert werden sollten. Nochmal: **Das Passwort muss so schnell es geht aus deiner Wohnung und von deinem Körper weg.**

Manchmal gibt es auch sogenannte Wiederherstellungsschlüssel (z.B. bei Macbooks) - diese sind eine Art spezielles Passwort, das vom Verschlüsselungstool generiert wird und genutzt werden kann, um deine Festplatte zu entschlüsseln. Wenn du dir sicher bist, dass du dein Passwort nicht vergisst, kannst du die Wiederherstellungsschlüssel einfach löschen und vergessen. Ansonsten gelten die gleiche Regeln wie beim Passwort oben: So schnell wie möglich an eine

vertrauenswürdige Person außerhalb der LG geben.

Unabhängig von der Verschlüsselung solltest du dir Gedanken um Backups (Sicherheitskopien) machen. Die Frage ist nicht, ob Festplatten kaputt gehen, sondern wann. Mach dir also vorher Gedanken, welche Daten dir wichtig sind und wie du sie sichern möchtest. Auch das Gerät, auf das du sie sicherst (USB-Stick, externe Festplatte, Dateien in Dropbox), sollte natürlich verschlüsselt sein.

Angriffe auf Festplattenverschlüsselung

Wenn der Computer hochgefahren und gesperrt ist, kann mit einem etwas aufwändigen und nicht immer erfolgreichen Angriff die Verschlüsselung geknackt werden. Der Angriff ist durchaus filmreif, hier eine Demonstration für Windows und hier für Mac.

D.h., wenn der Laptop Gefahr läuft, von der Polizei genommen zu werden, muss er heruntergefahren werden. Wenn es eilt, kann man ihn durch 10-sekündiges Drücken auf den Aus-Knopf auch auf die harte Tour ausschalten. Auch alle Handys, Tablets etc. mit LG-Daten dürfen nicht im Standby bleiben, wenn die Polizei klingelt:

> Standby, Ruhezustand, "Energie sparen", Zuklappen etc. sind leider nicht sicher.

Trotzem gilt: ein verschlüsseltes Gerät ist viel sicherer als ein unerschlüsseltes. Ein Gerät kann ja auch verloren/geklaut werden. Durch die Verschlüsselung sollte euer Gerät nicht langsamer werden.

Biometrische Entsperrungsmerkmale

Bei iPhones und Androids kannst du dir überlegen, die biometrischen Entsperrungsmerkmale zu deaktivieren. Die Polizei kann deinen Finger auf den Homebutton/Fingerabdruckscanner drücken oder das Smartphone vor dein Gesicht halten - das ist aber bei der LG bislang noch nie vorgekommen.

Oder deine Fingerabrdrücke (die sie jetzt ja haben) in eine Attrappe gießen, die sie zum Entsperren nehmen, hier ein Beispiel: Kraken Security Labs Bypasses Biometric Security With $5 In Materials. Das geht theoretisch auch (mit Aufwand) mit deinem Gesicht.

Davon abgesehen hinterlässt dein Fingerabdruck Fett auf dem Sensor, manchmal reicht es, das Fett einfach z.B. mit Anhauchen zu erwärmen.

Die Eingabe von Passwörtern lässt sich jedoch ausspähen, sodass eine gute Variante ist, dass du sehr gut lernst, wie du das biometrische Entsperren in der Hosentasche und über Nacht deaktivieren kannst - damit es in brenzligen Situationen klappt.

Passwörter

Es ist immens wichtig, dass die Passwörter sehr gut gewählt werden und nicht erratbar sind. Zusätzlich ist es äußerst wichtg, dass das Passwort nicht wiederverwendet wird, insbesondere nicht für Onlinedienste wie z.B. Google Mail etc. Außerdem dürfen Passwörter niemals aufgeschrieben und irgendwo "versteckt" werden - das findet die Polizei ziemlich sicher bei einer Hausdurchsuchung. Wenn Angreifende die Festplatte in die Hände kriegen, können sie versuchen, das Passwort herauszufinden, in dem sie automatisiert verschiedene Möglichkeiten durchprobieren. Mit einem herkömmlichen Gamer-PC können zwischen 6.432 und 457.500 Passwörter **pro Sekunde** getestet werden (je nachdem, wie die Platte verschlüsselt wurde) - die Polizei kann sich im Zweifel noch leistungsfähigere Systeme anschaffen, um den Durchsatz weiter zu erhöhen.

Da komplizierte Passwörter schwer zu merken sind, empfehlen wir den Einsatz eines sogenannten Diceware-Passworts. Das sind einfach mehrere **zufällig** ausgewählte Wörter aus einem (deutschen) Wörterbuch mit Leerzeichen getrennt (man kann aber auch andere Trennzeichen verwenden). Hier ein Beispiel:

> speerwerfen gehrock aluminium rotkohl saugt

Unter der Annahme, dass der Angreifende weiß, dass ein Diceware-Passwort verwendet wurde, dass es fünf Wörter lang ist und dass er das Wörterbuch kennt, aus dem das Passwort generiert wurde (in diesem Fall enthält es ~7.000 Wörter), müssen durchschnittlich 14.215.144.014.964.850.000 Passwörter durchprobiert werden, bis das richtige gefunden wurde. Mit den oben genannten Zahlen reden wir hier von einem Aufwand zwischen 985.266 und 70.080.730 Jahren.

Wir empfehlen speziell für die Festplattenverschlüsselung ein Passwort mit vier Wörtern. Hier liegt der Aufwand zwischen 126 und 9.012 Jahren. Bitte benutze das folgende Tool, um das Passwort zu generieren: https://dice.itsnow.biz/

Wenn du das Passwort nicht magst, kannst du einfach so lange ein neues würfeln bis es dir angenehm ist.

Bei Androids und iPhone gelten aus technischen Gründen etwas andere Regeln. Für diese Geräte empfehlen wir eine **zufällig** gewählte Zahlenkombination von mindestens 6 Zeichen. Normale kompliziertere Passwörter sind natürlich auch erlaubt.

Android Gerät verschlüsseln

Grundsätzlich sind alle Smartphones, die mit **Android 6.0 oder höher** laufen standardmäßig **verschlüsselt** und das lässt sich auch nicht ausschalten.

Verschlüsselungsstatus herausfinden

Wollt ihr auf Nummer sicher gehen, lässt sich das oft in den Systemeinstellungen nachgucken. Leider ist die Menustruktur sehr unterschiedlich, abhängig von Android-Version und Gerätehersteller und manchmal die Verlüsselungseinstellung nicht ganz leicht zu erkennen.

So kann die Einstellung z.B. hier liegen:

- `Einstellungen » Sicherheit & Standort » Verschlüsselung & Anmeldedaten » Verschlüsselung`
  oder
- `Einstellungen » Sicherheit » Weitere Einstellungen » Verschlüsselung & Anmeldedaten » Speichertyp Hardwaregestützt`
  oder
- `Einstellungen » Tab Allgemein » Sicherheit » Gerät verschlüsseln`

android-verschluesseln-einstellungen.png
Einstellung für Verschlüsselung
Android 8.0

Bei einigen Androidversionen/Geräteherstellern ist die Verschlüsselung in den Einstellungen gar nicht mehr aufgeführt.

Mit etwas technischen Einsatz bekommt ihr den Verschlüsselungsstatus in jedem Fall über die Kommandozeile mit der Android Debugging Bridge (ADB) heraus. Dazu muss das Gerät über USB mit dem Computer verbunden werden, ADB auf dem Computer installiert und USB-Debbuging aktiviert werden. Eine Anleitung dazu findet ihr hier.

Danach liefert der Befehl `adb shell getprop ro.crypto.state` die Information, ob das Gerät verschlüsselt ist.

android-verschluesseln-adb.png

Das Kommandozeilentool ADB kann den Verschlüsselungsstatus auslesen

Was tun bei Android < 6.0?

Android ist seit der Version 4.0 mit Verschlüsselung ausgestattet, diese wird in 4.0 und 5.0 aber nicht standardmäßig aktiviert. Das könnt ihr über die Einstellungen ähnlich wie oben beschrieben nachholen.

Solltet ihr noch ein Androidgerät < 4.0 haben, nehmt gerne Kontakt zu uns aus der IT-AG auf. Dazu könnt ihr eine Mail an it-support@letztegeneration.org schicken.

SD-Karte/USB-Stick verschlüsseln

Habt ihr sensible Daten auf einer SD-Karte und/oder USB-Sticks abgelegt, solltet ihr darüber nachdenken, diese zu verschlüsseln. Am einfachsten verschlüsselt ihr eure SD-Karte/USB-Sticks mit Veracrypt. Eine Anleitung findest du auf Youtube: https://www.youtube.com/embed/HSeoekvGocs

Windows verschlüsseln mit Bitlocker

Diese Anleitung beschreibt, wie du einen Computer mit Windows verschlüsseln kannst. Es ist immens wichtig, dass du dir auch die allgemeinen Informationen zum Thema Festplattenverschlüsselung durchliest.

Wir empfehlen aktuell die in Windows integrierte Verschlüsselung, die “Bitlocker” genannt wird.

Bitlocker funktioniert nur auf Pro und Enterprise Editionen von Windows. In dieser Anleitung wird beschrieben, wie du herausfindest, welche Edition du hast und wie du sie umwandeln kannst.

Wenn dein Gerät verschlüsselt ist, lies bitte auch diesen wichtigen Hinweis.

Ist die Verschlüsselung schon aktiv?

Es kann gut sein, dass dein Rechner schon verschlüsselt ist. Um das herauszufinden, drücke die Windows-Taste auf der Tastatur und gebe "Bitlocker" ein. Dann:

- kommt eine Bing-Suche, wenn deine installierte Windows-Edition nicht ausreicht (siehe unten für mehr Details)
- falls Bitlocker unterstützt wird, klicke auf das Bitlocker-Symbol. Dann siehst du
  - den Text „Bitlocker deaktiviert“, wenn nichts verschlüsselt ist
  - „aktiviert“, wenn deine Festplatte bereits verschlüsselt ist

Windows-Edition herausfinden

1. Windowstaste und X gleichzeitig drücken
2. Menüpunkt „System“ auswählen.
3. Unter der Überschrift „Windows Spezifikationen“ steht die Windows-Edition. Wenn da steht „Windows 10 Home“ dann folge bitte weiter dieser Anleitung. Wenn da “Windows 10 Pro” oder „Windows 10 Enterprise“ steht kannst du zu „Verschlüsselung aktivieren (1. Schritt)“ springen.

Windows-Edition ändern

Bitte einen entsprechenen Key kaufen. Die IT-AG kann dich dabei unterstützen.

Verschlüsselung aktivieren (1. Schritt)

1. Windowstaste drücken, “Bitlocker” eingeben und “Bitlocker verwalten” anklicken.

2. Nun kann es sein, dass du die folgende Meldung erhältst:

Wenn das der Fall ist, folge bitte dieser Anleitung weiter. Wenn das nicht der Fall ist springe zu “Verschlüsselung aktivieren (2. Schritt)”.

Verschlüsselung aktivieren (TPM-Fehler beheben)

Um diesen Fehler zu beseitigen bitte folgendes tun:

1. “Abbrechen” klicken.
2. Windowstaste zusammen mit R drücken und in das Dialogfelg "gpedit.msc" und Enter drücken.

2. Links folgendes auswählen: “Administrative Vorlagen”, “Windows Komponenten”…

3. … “Bitlocker-Laufwerksverschlüsselung”, “Betriebssystemlaufwerke”.

4. Auf der rechten Seite “Zusätzliche Authentifizierung beim Start anfordern” doppelklicken:

5. Im folgenden Dialogfeld sicherstellen, dass links oben “Aktiviert” ausgewählt ist und weiter unten “BitLocker ohne kompatibles TPM zulassen […]”. Danach auf OK drücken.

6. Das Gruppenrichtlinienfenster schließen.

7. Im Bitlocker-Fenster nochmal “Bitlocker aktivieren” anklicken.

8. Laufwerke sollten nur mit Passwort entsperrt werden, entsprechendes anklicken:

9. Jetzt ein Kennwort vergeben. Bitte lies dir unseren allgemeinen Hinweise zum Thema Verschlüsselung durch - das ist wichtig, damit dein Computer auch wirklich geschützt ist.

Verschlüsselung aktivieren (2. Schritt)

1. Windows zwingt dich nun, Wiederherstellungsschlüssel für die Festplatte zu speichern - auch wenn du das gar nicht willst. Lies dir bitte zum Thema Wiederhestellungsschlüssel unsere allgemeinen Hinweise zum Thema Verschlüsselung durch. Speichere den Wiederherstellungsschlüssel auf keinem Fall in deinem Microsoft-Konto oder auf einem USB-Stick! Wähle stattdessen “Wiederherstellungsschlüssel drucken”. Hinweis: es kann sein, dass hier weitere Optionen angezeigt werden, die nicht auf dem Screenshot unten zu sehen sind.

1. Wähle als Drucker “Microsoft Print to PDF”.

1. Vergebe einen Namen und speichere die PDF auf dem Desktop.

Wenn du die Wiederherstellungsschlüssel nicht an einen vertrauenswürdigen Menschen geben willst, dann lösche sie gleich wieder. Halte dich ansonsten an die Regeln aus den allgemeinen Hinweisen zur Verschlüsselung.

Klicke auf “Weiter”.

Wähle im folgenden Dialogfenster “Gesamtes Laufwerk verschlüsseln”, dann “Weiter”:

1. Den Verschlüsselungsmodus auf “Neuer Verschlüsselungsmodus” lassen, “Weiter” klicken:

Verschlüsselungsmodus

1. “Bitlocker-Systemüberprüfung ausführen" muss ausgewählt sein, wieder “Weiter” drücken:

Jetzt verschlüsseln bestätigen

1. Und nun den Computer “Jetzt neu starten”.

1. Der Computer wird jetzt verschlüsselt. Das dauert eine Weile, er kann jedoch dabei weiter verwendet werden, wobei er am Anfang etwas langsam sein kann. Wenn Bitlocker dir ein weiteres Festplattenlaufwerk zum Verschlüsseln anbietet, dann verschlüssle auch das.

Siehe auch

VeraCrypt ist eine Alternative zum Verschlüsseln von Windows. Der Vorteil ist, dass keine Pro-Lizenz von Windows nötig ist. Leider birgt die Verschlüsselung bei VeraCrypt das Risiko, dass durch das Verschlüsseln der Rechner unwiederbringlich unbenutzbar wird. Daher ist es wichtig, vor dem Verschlüsseln des Rechners ein Backup zu machen.

Windows verschlüsseln mit Veracrypt

Windows verschlüsseln mit VeraCrypt

Wichtig: Bitte lies dir im Vorfeld unbedingt die allgemeinen Hinweise zum Thema Verschlüsselung durch.

Wenn du auf deinem Computer mehrere Betriebssysteme hast, bitte kontaktiere die IT-AG. Wenn du nur Windows benutzt und nichts von einem weiteren Betriebssystem weißt, kannst du die Anleitung einfach befolgeden.

1. VeraCrypt herunterladen: https://veracrypt.io/en/Downloads.html (leider nur auf Englisch verfügbar, mehr Informationen zur Installation findest du hier)
2. VeraCrypt starten, z.B. über das Startmenü.
3. Im Menü oben „*System > Encrypt System Partition/Drive*“ auswählen.

veracrypt_system2.png

5. Im Dialogfeld „Type of System Encryption“ „Normal“ auswählen.

veracrypt_system3.png

6. Im Dialogfeld „Area to Encrypt“ wenn möglich „Encrypt the whole drive“ auswählen. Manchmal ist das aus technischen Gründen nicht möglich, dann eben „Encrypt Windows System Partition“ auswählen.

bios_vs_gpt.png

7. Sollte nun die folgende Fehlermeldung erscheinen, diese mit „Ja“ bestätigen.

recovery_partition.png

8. Bei „Number of Operating Systems“ „Single-boot“ auswählen.

8. Im Dialogfeld „Encryption Options“ die bereits gesetzten Einstellungen bestätigen (AES, SHA-256).

9. Im Dialogfeld „Passwort“ ein Passwort vergeben. An dieser Stelle nochmal der wichtige Verweis zum Dokument Allgemeinen Hinweise zum Thema Verschlüsselung. Mit diesem Passwort steht und fällt ob dich die Verschlüsselung schützt.

10. Alle anderen Optionen nicht aktivieren.

11. Wenn das Password unter 20 Zeichen lang ist, kann es sein, dass die folgende Fehlermeldung erscheint:

bruteforce.png

Wenn das gewählte Passwort den Regeln aus Allgemeinen Hinweise zum Thema Verschlüsselung entspricht, kann diese Meldung mit „Ja“ ignoriert werden.

12. Im Dialogfeld „Collecting Random Data“ muss solange die Maus durch die Gegend bewegt werden, bis der Balken unten voll & grün ist.

Das sieht dann so aus:

randomness.png

13. Nach einem Klick auf „Next“ erscheint das Dialogfeld „Keys Generated“, das mit „Next“ weitergeklickt werden kann:

14. VeraCrypt möchte nun eine sogenannte Rescue Disk erstellen. Das ist entweder ein USB-Stick oder eine CD. In sehr seltenen Fällen kann es passieren, dass der Teil von VeraCrypt kaputt geht,

der deine Festplatte entschlüsselt - du könntest dann deinen Computer nicht mehr starten, da deine Platte nicht mehr entschlüsselt werden kann.

Wenn jemand diese Rescue Disk in die Finger bekommt kann dieser Mensch nicht deinen Computer entschlüsseln - es wird immer noch das Passwort benötigt.

Die Rescue-Disk stellt dir VeraCrypt als sogenanntes Image zur Verfügung, das kann auf einen USB-Stick ausgerollt werden oder auf eine CD gebrannt. Wir raten dir, dass du das erstmal einfach nur auf einen (oder mehrere) USB-Sticks kopierst. Solltest du in die Verlegenheit kommen, das zu brauchen, kannst du dich bei der IT melden.

15. Aktiviere „Skip Rescue Disk verification“, da wir die Disk noch nicht so fertig einrichten, wie VeraCrypt das erwartet - wir machen das, wenn die Disk wirklich gebraucht würde. Dann „Next“.

16. Als „Wipe Mode“ „None“ einstellen. Dann „Next“.

17. VeraCrypt möchte nun testen, ob dein Computer ohne Probleme verschlüsselt werden kann. Dabei werden noch keine Daten verschlüsselt - wenn der Test erfolgreich war fragt dich VeraCrypt nochmal. Einmal „Test“ klicken.

18. Im nächsten Fenster dann „OK“ klicken:

19. VeraCrypt weißt dich nun darauf hin, dass der Computer neugestartet wird. Einmal bestätigen:

test_restart.png

20. Nach dem Neustart fragt dich VeraCrypt nach deinem Passwort, nach der Eingabe Enter drücken:

boot_password.png

21. “PIM” einfach leerlassen, Enter drücken:

boot_password_2.png

22. Dann entschlüsselt VeraCrypt deine Platte (die allerdings bei diesem ersten Neustart noch nicht verschlüsselt ist, das ist nur ein Test):

boot_password_3.png

23. Nach dem Neustart meldet VeraCrypt mit sehr hoher Wahrscheinlichkeit, dass der Test erfolgreich war. Mit Klick auf „Encrypt“ kann es losgehen:

24. Das will Windows aber noch einmal freigegeben haben, einmal „Ja“ klicken:

encrypt_admin.png

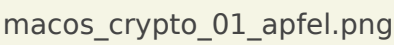
25. Dein Computer wird jetzt verschlüsselt! Du kannst ihn ganz normal weiterbenutzen während das passiert, es könnte nur etwas langsamer als sonst sein. Du kannst ihn sogar herunterfahren - allerdings gibt es dann ggf. noch Teile, die nicht verschlüsselt sind.

macOS verschlüsseln

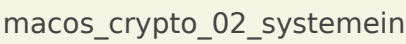
> UPDATE 10/2023: Die Polizei kann die Verschlüsselung nicht umgehen und beißt sich die Zähne daran aus.

In der Regel sind aktuelle Macbooks schon verschlüsselt. Ob das der Fall ist, kann man so nachprüfen:

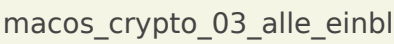
Zuerst links oben auf den Apfel klicken.


macos_crypto_01_apfel.png

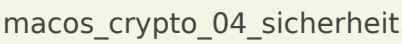
Dann auf “Systemeinstellungen” klicken.


macos_crypto_02_systemeinstellungen.png

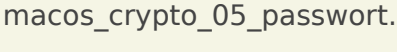
Dann einmal zur Sicherheit auf den Button mit den 4x3 Punkten klicken:


macos_crypto_03_alle_einblenden.png

Dann auf “Sicherheit” klicken. Manchmal heißt das auch “Sicherheit & Privatsphäre”.


macos_crypto_04_sicherheit.png

Unter dem Reiter “Allgemein” zuerst prüfen, dass “Passwort erforderlich” aktiviert ist und auf “5 Minuten” eingestellt ist. Wenn nicht entsprechend ändern. **ES IST IMMENS WICHTIG, EIN GUTES PASSWORT ZU WÄHLEN**. Bei macOS ist das Passwort zum Entsperren des Macs auch das Passwort, mit dem die Festplatte verschlüsselt wird. Siehe dazu die Wikiseite "Allgemeines zum Thema Festplatten-Verschlüsselung".


macos_crypto_05_passwort.png

Dann auf “FileVault” klicken.

Wenn da “FileVault ist für die Festplatte Macintosh aktiviert” steht, ist die Verschlüsselung an. Manchmal heißt die Festplatte auch anders.

macos_crypto_06_verschlüsselung_aktiviert.png

Wenn die Verschlüsselung nicht aktiviert ist, sieht das so aus:

macos_crypto_07_verschlüsselung_deaktiviert.png

Zum Aktivieren der Verschlüsselung auf das Schloß klicken und das Passwort eingeben:

macos_crypto_08_passwort_eingeben.png

Im nächsten Fenster ist es wichtig, “Wiederherstellungsschlüssel erstellen [...]” auszuwählen – die Polizei kann sich sonst die Unterstützung von Apple holen, um die Festplatte zu entschlüsseln.

macos_crypto_09_key_icloud.png

Den Wiederherstellungsschlüssel abschreiben **UND EINER VERTRAUENSWÜRDIGEN PERSON GEBEN, DIE NICHTS MIT LG ZU TUN HAT**. Vorzugsweise Freunde, bei Familie die Eltern zur Sicherheit aussparen (stattdessen Tante, Cousine, Onkel, etc.). Es ist immens wichtig, dass der Wiederherstellungsschlüssel SO SCHNELL ES GEHT aus eurem Wohnraum und von eurem Körper weg verschwindet. Wer risikobereit ist, kann den Schlüssel auch ignorieren und vergessen. Er hilft euch die Festplatte zu entschlüsseln, wenn ihr euer Passwort vergisst.

macos_crypto_10_wiederherstellungskey.png

Nun wird die Festplatte verschlüsselt, währenddessen kann der Mac einfach weiterbenutzt werden.

macos_crypto_11_verschlüsselung_in_progress.png

Weitere Links

https://github.com/drduh/macOS-Security-and-Privacy-Guide

Festplattenvollverschlüsselung mit Ubuntu Installation

Festplattenvollverschlüsselung bei Ubuntu Neuinstallation

Schritte

1. Erstelle ein USB Stick mit Ubuntu
2. Starte dein Computer von den USB Stick
3. Ubuntu Installation mit Festplattenvollverschlüsselung

1. Erstelle in Bootable USB Stick

2. Starte den Computer vom USB-Stick

> Dieser Schritt ist leider sehr herstellerabhängig. Die Hersteller haben unterschiedliche Methoden um beim Start des Computers in das Boot Menü zu

> kommen. Gängige Tasten sind ESC, F2, F10, F12 oder F11. Im Zweifel die Marke/Modell des Computers suchen. z.B “Lenovo T480p Boot menu key” oder mal alle Tasten drücken ;-)

Beispiel mit Dell Laptop

3. Setup Guide mit Festplattenvollverschlüssel (bis 4:45)

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)