

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 gleichen 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.

Trotzdem gilt: ein verschlüsseltes Gerät ist viel sicherer als ein unverschlüsseltes. 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 Fingerabdrücke (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 wichtig, 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 Verlüsslungseinstellung 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

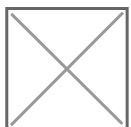
Einstellung für Verschlüsselung

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.



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 entsprechenden 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:

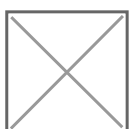


Wenn das der Fall ist, folge bitte dieser Anleitung weiter. Wenn das nicht der Fall ist springe zu "Verschlüsselung aktivieren (2. Schritt)".

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 Dialogfeld "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 Wiederherstellungsschlüssel 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 verschlüssele 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 kault 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 ungetestet, 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 befolgen.

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.



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



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.



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



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

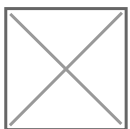


8. Im Dialogfeld „Encryption Options“ die bereits gesetzten Einstellungen bestätigen (AES, SHA-256).



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.

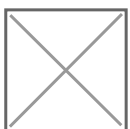


11. Wenn das Password unter 20 Zeichen lang ist, kann es sein, dass die folgende Fehlermeldung erscheint:



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:



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.

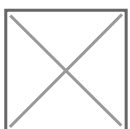
15. Aktiviere „Skip Rescue Disk verification“, da wir die Disk noch nicht so fertig einrichten, wie VeraCrypt das erwartet - wir machen das, wenn die Disk wirklich gebraucht würde. Dann „Next“.



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 weist dich nun darauf hin, dass der Computer neugestartet wird. Einmal bestätigen:



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



21. "PIM" einfach leerlassen, Enter drücken:



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



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:



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)