

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.