BitLocker

- Windows verschlüsseln mit Veracrypt
- Welche Windows Version nutze ich?
- Ist mein Laptop schon verschlüsselt?
- Windows mit BitLocker verschlüsseln
- Pre-Boot Authentication in BitLocker aktivieren
- Wie kann ich meinen BitLocker Wiederherstellungsschlüssel (Recovery Key) sichern?
- Grundlegende Informationen zur Windows Festplattenverschlüsselung

Windows verschlüsseln mit Veracrypt

Windows verschlüsseln mit VeraCrypt

Diese Anleitung ist etwas veraltet. Die Screenshots passen nicht mehr ganz, allerdings funktioniert die Anleitung als Ganzes schon noch.

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.

Welche Windows Version nutze ich?

Welche Windows Version nutze ich?

> Grundlegende Informationen zur Festplattenverschlüsselung unter Windows findest du hier. {.is-info}

1. Suche im Startmenü nach `Systeminformationen` und klicke auf der rechten Seite auf `Öffnen` .

1-startmenü-systeminformationen.png

2. Auf der rechten Seite steht, welche Windows Version du installiert hast. Aktuell ist Windows 11. Eventuell hast du dort noch Windows 10 stehen. Du solltest auf jeden Fall immer das neuste und aktuellste Windows nutzen.

2-dialog-systeminformationen.png

Zur Version: Hier ist "Windows Pro" installiert. Daneben gibt es z. B. noch "Windows Home" und "Windows Enterprise".

> Wenn du Windows Home nutzt, solltest du deinen Laptop mit Veracrypt verschlüsseln oder auf Windows Pro/Enterprise upgraden. Warum wird dir hier erklärt. {.is-danger}

>

- Auf dieser (englischsprachigen) Webseite wird beschrieben, wie du (kostenlos) auf Windows Pro upgraden kannst.
- Man kann auch den offiziellen Weg gehen und Geld dafür bezahlen. Hier ist ein Artikel mit mehr Informationen dazu.
- Bei Fragen kannst du dich natürlich auch immer an it-support@raz-ev.org wenden. {.is-info}

Weiterführende Links

- Ist mein Laptop bereits verschlüsselt?
- Windows mit BitLocker verschlüsseln

Ist mein Laptop schon verschlüsselt?

Ist mein Laptop bereits verschlüsselt?

> Grundlegende Informationen zur Festplattenverschlüsselung unter Windows findest du hier. {.is-info}

Suche im Startmenü nach `Bitlocker` (unter Windows Home `Geräteverschlüsselung`) und klicke rechts auf `Öffnen`.

1-startmenü-bitlocker.png

Unverschlüsselter Laptop

In diesem Beispiel ist die Festplatte nicht verschlüsselt. Hier steht: `C: BitLocker deaktiviert`.

2-bitlocker-dialog-unverschlüsselt.png

> Mit C: ist deine Festplatte gemeint. Es kann auch sein, dass du mehrere Festplatten hast. Oder dass du eine Festplatte hast, die aber unterteilt ist (in Partitionen). Dann steht da C: und D:. Du solltest schauen, dass wirklich alle Partitionen verschlüsselt sind! {.is-warning}

Hier findest du die Anleitung zum Aktivieren von BitLocker.

Verschlüsselter Laptop (ohne Pre-Boot Authentication)

Wenn dein Laptop vollständig verschlüsselt ist, sieht das folgendermaßen aus (`BitLocker aktiviert`).

3-bitlocker-verschlüsselt.png

Um Pre-Boot Authentication zu aktiviern, folge dieser Anleitung.

Verschlüsselter Laptop (mit Pre-Boot Authentication)

In diesem Beispiel ist der Laptop verschlüsselt (`C: Bitlocker aktiviert`) und zusätzlich Pre-Boot Authentication aktiviert. Das siehst du an der Option `wie das Laufwerk beim Start entsperrt werden soll`.

6-bitlocker-einstellungen.png

Bei aktivierter Pre-Boot Authentication musst du beim Start des Laptops noch ein zusätzliches Passwort eingeben. So sieht das dann aus:

pre-boot-authentication.jpeg

Windows mit BitLocker verschlüsseln

Mit dieser Anleitung kannst du deinen Laptop mit BitLocker verschlüsseln.

> Grundlegende Informationen zur Festplattenverschlüsselung unter Windows findest du hier. {.is-info}

> Bevor du mit der Verschlüsselung startest: Bitte hänge deinen Laptop ans Stromkabel und installiere als erstes alle Windows-Updates. {.is-info}

1. Öffne zunächst die BitLocker Einstellungen, indem du im Startmenü nach `BitLocker` suchst und rechts auf `Öffnen` klickst.

   > Wenn du Windows Home nutzt gibt es bei dir kein BitLocker. Wie du das herausfinden kannst, steht hier. Du findest stattdessen im Startmenü `Geräteverschlüsselung`. Obwohl die Installation weitgehend gleich ist, gibt es wichtige Unterschiede, die du hier nachlesen kannst. {.is-info}

1-startmenü-bitlocker.png

2. In unserem Beispiel ist BitLocker deaktiviert (Festplatte nicht verschlüsselt). Auf der rechten Seite kannst du `BitLocker aktivieren`.

1-bitlocker-deaktiviert.png

Laptop ohne TPM (Sicherheitschip)

Wenn dein Laptop keinen Sicherheitschip (TPM) enthält, bekommst du an dieser Stelle folgende Fehlermeldung: `Auf diesem Gerät kann kein TPM verwendet werden. Der Administrator muss für die Richtlinie "Zusätzliche Authentifizierung beim Start anfordern" für Betriebssystemvolumes die Option "BitLocker ohne kompatibles TPM zulassen" festlegen`

.

Wenn die Fehlermeldung bei dir kommt, nutze bitte diese Anleitung und springe runter zu `Anleitung: BitLocker ohne TPM aktivieren`.

Keine Fehlermeldung bekommen? Hier geht's weiter!

3. Als nächstes sollst du deinen Wiederherstellungsschlüssel sichern. Was der Wiederherstellungsschlüssel ist wird hier erklärt. Am besten speicherst du ihn in eine Datei, kopierst ihn dann in deinen Passwort-Manager und löscht die Datei dann von deinem Laptop.

   > Du kannst den Wiederherstellungsschlüssel `in eine Datei speichern`. Allerdings erlaubt es Windows dir nicht, die Datei auf die Festplatte vom Laptop zu speichern. Das ist eine Sicherheitsvorkehrung, da du den Wiederherstellungsschlüssel benötigst, wenn dein Laptop nicht mehr startet. Du kannst ihn z. B. auf einem USB-Stick speichern (unbedingt danach löschen!). Alternativ kannst du ihn auch drucken. Du kannst ihn dann wirklich drucken oder kannst das "in Datei drucken"-Feature nutzten. Du müsstest einen "virtuellen" Drucker auswählen können, mit dem du den Wiederherstellungsschlüssel in eine Datei speichern kannst (und damit auch einfach z. B. auf den Desktop). {.is-info}

Wähle im Assistenten `Wiederherstellungsschlüssel drucken`.

2-wiederherstellungsschlüssel-drucken.png

4. Wähle den (virtuellen) Drucker `in Datei speichern` und wähle einen Ordner deiner Wahl aus, in dem der Wiederherstellungsschlüssel gespeichert werden soll.

3-wiederherstellungsschlüsse-in-datei-drucken.png

So sieht übrigens dein Wiederherstellungsschlüssel aus

ansicht-wiederherstellungsschlüssel.png

Er besteht aus zwei Teilen:

- **Bezeichner**: Er identifiziert deine Festplatte eindeutig und ist hilfreich, wenn du mehrere Wiederherstellungsschlüssel/Laptops sicherst. Die Nummer wird dir angezeigt, wenn du deinen Wiederherstellungsschlüssel eingeben musst.
- **Wiederherstellungsschlüssel**: Das ist das Passwort, mit dem du die Festplatte entschlüsseln kannst. Du solltest ihn geheim halten und an einem sicheren Ort speichern.

5. Wähle als nächstes `Gesamtes Laufwerk verschlüsseln`.

4-gesamtes-laufwerk-verschlüsseln.png

6. Wähle den `neuen Verschlüsselungsmodus`.

5-neue-verschlüsselungsmethode-nutzen.png

7. Aktiviere die `BitLocker-Systemüberprüfung`.

6-systemüberprüfung-aktivieren.png

8. Als nächstes wird dir angezeigt, dass ein `Neustart erforderlich` ist. Die Verschlüsselung beginnt nach dem Neustart automatisch. Starte deinen Laptop neu (vergiss nicht, dir diese Anleitung zu speichern).

7-verschlüsselung-beginnt-nach-neustart.png

9. Nach dem Neustart beginnt die Verschlüsselung automatisch im Hintergrund. Du findest im Systemtray rechts unten (der Pfeil nach oben) ein Symbol für die Verschlüsselung. Wenn du dort drauf klickst, siehst du den Fortschritt der Verschlüsselung.

8-verschlüsselung-läuft.png

9-bitlocker-verschlüsselung-beginnt.png

Es kann etwas dauern bis die Verschlüsselung erfolgreich abgeschlossen ist.

10-bitlocker-verschlüsselung-abgeschlossen.png

10. In den BitLocker-Einstellungen kannst du überprüfen: `C: BitLocker aktiv`. Damit ist deine Festplatte verschlüsselt.

11-bitlocker-ist-aktiviert.png

> Falls du hier im Fenster zwei Partitionen (z. B. C: und D:) hast, achte darauf dass Bitlocker für alle Partitionen aktiv ist. Wenn du diese Anleitung befolgst ist C:

> (das System) verschlüsselt, aber D: (Datenpartition) nicht (falls du eine hast). {.is-danger}

Als nächstes solltest du unbedingt Pre-Boot Authentication aktivieren. Das ist ein wichtiger zusätzlicher Schutz. Was das genau ist wird hier beschrieben. Die Anleitung zum Aktivieren findest du hier.

Pre-Boot Authentication in BitLocker aktivieren

Wie kann ich Pre-Boot Authentication unter BitLocker aktivieren?

> Für dieses Feature braucht du BitLocker (nur vergübar unter Windows Pro/Enterprise). Mit der "Geräteverschlüsselung" (Windows Home) kannst du das Feature nicht nutzen. Mehr Informationen zur Festplattenverschlüsselung unter Windows findest du hier. {.is-info}

> Falls du mit dieser Anleitung nicht zurecht kommst: Es gibt auch alternative Anleitungen zu diesem Thema (Anleitung auf Deutsch, Anleitung auf Englisch, Video auf Englisch). {.is-info}

1. Öffne zunächst den `Gruppenrichtlinien-Editor`. Suche dazu im Startmenü nach `Gruppenrichtlinie bearbeiten` und gehe rechts auf `Öffnen`.

1-gruppenrichtlinien-editor.png

2. Dann musst du dich durch die Ordnerstruktur auf der linken Seite durchklicken:

2-bitlocker-einstellungen-ändern.png

`Administrative Vorlagen -> Windows-Komponenten -> BitLocker-Laufwerksverschlüsselung -> Betriebssystemlaufwerke`

> Auf der rechten Seite siehst du (in der Spalte "Status"), dass bislang keine Einstellungen vorgenommen wurden (nicht konfiguriert). {.is-info}

4. Mache einen Doppelklick (linker Mauszeiger) auf `Zusätzliche Authentifizierung beim Start anfordern`

3-tpm-pin-beim-start-zulassen.png

In diesem Fenster änderst du zwei Dinge:

- links oben: von `Nicht konfiguriert` auf `Aktiviert` wechseln
- links unten: `TPM-Systemstart-PIN konfigurieren`: dort wählst du `Systemstart-PIN bei TPM zulassen`

Drücke auf "OK", um zu speichern und das Fenster zu schließen.

> Jetzt siehst du in der Spalte "Status", dass die Einstellung aktiviert wurde. {.is-info}

Damit du nicht nur numerische PINs, sondern auch Passwörter mit Buchstaben nutzen kannst, braucht es noch eine Einstellung.

6. Mache dazu einen Doppelklick (linker Mauszeiger) auf `Erweiterte PINs für Systemstart zulassen`.

4-erweiterte-pin-erlauben.png

7. Wie eben auch wählst du links oben anstatt `Nicht konfiguriert`, `Aktiviert` aus. Mehr braucht es hier nicht. Mit "OK" kannst du speichern und das Fenster schließt sich.

45-erweiterte-pins-erlauben.png

8. Die eben geänderten Einstellungen müssen noch übernommen werden. Dazu hast du zwei Optionen: **UPDATE:** Du kannst Schritt 8 wahrscheinlich ignorieren. Mach ruhig erst mal mit Schritt 9 weiter.

   - A) Du startest den Laptop neu.
   - B) Du öffnest die `Eingabeaufforderung` als Administrator*in (im Startmenü nach `Eingabeaufforderung` suchen) und gibst dort `gpupdate /force` ein.

5-gruppenrichtlinien-aktualisieren.png

9. Wenn du nun wieder in die BitLocker-Einstellungen gehst (im Startmenü nach `BitLocker` suchen), findest du dort eine neue Option: `Ändern, wie das Laufwerk beim Start entsperrt wird.` Klicke den Text an (einfacher Linksklick genügt).

6-bitlocker-einstellungen.png

10. Wähle hier `PIN eingeben` aus.

7-pin-eingeben.png

11. Im nächsten Schritt (leider kein Screenshot) kannst du eine PIN (Passwort) setzen. Dieses Passwort muss auch nicht super lang und komplex sein, da der TPM/Sicherheitschip verhindert, dass es gebruteforct werden kann.

    > Damit ist hast du Pre-Boot Authentication erfolgreich aktiviert. {.is-success}

    > Falls du deine PIN/Passwort mal ändern möchtest: In den BitLocker-Einstellungen gibt es eine Option, um die PIN zu ändern. {.is-info}

Ab sofort wirst du bei jedem Start des Laptops aufgefordert, dein eben gesetztes Passwort einzugeben. Erst dadurch wird die Festplatte entschlüsselt. Wenn du damit mal Probleme hast, kannst Escape/ESC drücken und mit dem Wiederherstellungsschlüssel die Festplatte entschlüsseln.

pre-boot-authentication.jpeg

Wie kann ich meinen BitLocker Wiederherstellungsschlüssel (Recovery Key) sichern?

Wie kann ich meinen BitLocker Wiederherstellungsschlüssel (Recovery Key) sichern?

> Grundlegende Informationen zur Festplattenverschlüsselung unter Windows findest du hier. {.is-info}

> Um zu schauen, ob dein Laptop bereits verschlüsselt ist, kannst du diese Anleitung nutzen. {.is-info}

> Wenn du Windows Home nutzt, ist `BitLocker` bei dir nicht verfügbar. Stattdessen gibt es bei dir die `Geräteverschlüsselung`. Bei der

> "Geräteverschlüsselung" gibt es in der Oberfläche allerdings keine Möglichkeit, den Wiederherstellungsschlüssel anzuzeigen/zu sichern. Du kannst dir den Wiederherstellungsschlüssel über die Kommandozeile anzeigen lassen:
>
> 1. Suche im Startmenü nach `Eingabeaufforderung`
> 2. Öffne die `Eingabeaufforderung` als `Administrator*in`
> 3. Gebe folgenden Befehl ein und bestätige mit Enter: `manage-bde -protectors -get C:`
> 4. Folgende Ausgabe erscheint: `Numerisches Kennwort:` `ID: {GUID}` `Kennwort:` `123456-123456-123456-123456-123456-123456-123456-123456` Das `numerische Kennwort` ist der Wiederherstellungsschlüssel. {.is-info}

1. Suche im Startmenü nach `BitLocker` und gehe rechts auf `Öffnen`.

1-startmenü-bitlocker.png

2. Wenn dein Laptop bereits verschlüsselt ist, findest du dort `Wiederherstellungsschlüssel sichern`.

1-bitlocker-ist-aktiviert.png

3. Als nächstes gehst du auf `Wiederherstellungsschlüssel drucken` und wählst bei den Druckern den virtuellen `in Datei speichern`-Drucker aus.

> Warum nicht `in Datei speichern`? Weil dir Windows nicht erlaubt, den Wiederherstellungsschlüssel auf deinen Laptop zu speichern (aus Sicherheitsgründen - du brauchst ihn ja wenn dein Laptop nicht mehr geht). {.is-info}

2-wiederherstellungsschlüssel-drucken.png

4. Wähle einen Ordner deiner Wahl und speichere den Wiederherstellungsschlüssel in eine Datei.

3-wiederherstellungsschlüsse-in-datei-drucken.png

So sieht übrigens dein Wiederherstellungsschlüssel aus

ansicht-wiederherstellungsschlüssel.png

Er besteht aus zwei Teilen:

- **Bezeichner**: Er identifiziert deine Festplatte eindeutig und ist hilfreich, wenn du mehrere Wiederherstellungsschlüssel/Laptops sicherst. Die Nummer wird dir angezeigt, wenn du deinen Wiederherstellungsschlüssel eingeben musst.
- **Wiederherstellungsschlüssel**: Das ist das Passwort, mit dem du die Festplatte entschlüsseln kannst. Du solltest ihn geheim halten und an einem sicheren Ort speichern.

> Am Besten speicherst du den Wiederherstellungsschlüssel in deinem Passwort-Manager und löscht die Datei wieder von der Festplatte. {.is-info}

> Wenn du in Zukunft mal deinen Wiederherstellungsschlüssel brauchst, dann wird dein Laptop in der Situation nicht funktionieren. Daher musst du sicherstellen, dass du auch ohne deinen Laptop auf deinen Wiederherstellungsschlüssel/Passwort-Manager zugreifen kannst. {.is-warning}

Grundlegende Informationen zur Windows Festplattenverschlüsselung

Grundlegende Informationen zur Windows Festplattenverschlüsselung

Zuletzt aktualisiert: 06/2026

Anleitungen

Wenn du gleich loslegen willst, findest du hier die Anleitungen.

- Welche Windows Version nutze ich?
- Ist mein Laptop bereits verschlüsselt?
- Windows-Laptop mit BitLocker verschlüsseln
- Pre-Boot Authentication in BitLocker aktivieren
- BitLocker Wiederherstellungsschlüssel (Recovery Key) sichern

Das ist aber viel Text und klingt alles sehr kompliziert! Was ist denn jetzt sicher? Und was soll ich tun?

Zusammenfassung (mehr Details unten):

- **Du hast Windows Pro/Enterprise?** Aktiviere BitLocker, aktiviere Pre-Boot Authentication und sichere deinen Wiederherstellungsschlüssel in deinem Passwort-Manager. Dann bist du sicher! Und die Einrichtung ist okayish einfach.
- **Du hast Windows Home?** Du könntest auf Windows Pro upgraden. Ansonsten die "Geräteverschlüsselung" aktivieren. Der Unterschied: Du kannst deinen Wiederherstellungsschlüssel nicht auslesen und er ist im Microsoft-Konto gespeichert. Außerdem kannst du keine Pre-Boot Authentication aktivieren. Die Einrichtung ist dafür sehr einfach. Allerdings hast du wirklich nur einen Basis-Schutz und die Polizei wird das Gerät wahrscheinlich entschlüsseln können, wenn sie wirklich motiviert ist.
- **Ich traue Microsoft nicht** (könnte ja eine Backdoor haben): Dann nutze Veracrypt. Die Einrichtung ist allerdings nicht ganz so einfach. Oder installiere dir Linux.

Welche Möglichkeiten gibt es, um meinen Windows-Laptop zu verschlüsseln?

Du kannst die Verschlüsselung von Windows nutzen oder Veracrypt als eigenes Tool installieren (Anleitung). Der Code von Veracrypt ist öffentlich und kann als sicher eingestuft werden. Eine System-mit-Veracrypt-installieren-Anleitung findest du hier (ist jedoch etwas veraltet).

Was spricht gegen Veracrypt?

Die Installation mit Veracrypt ist komplizierter als die Verschlüsselung mit den von Windows mitgebrachten Tools. Veracrypt integriert sich tief ins System, was manchmal nach Windows-Updates zu Problemem führen kann. Du solltet auf jeden Fall vorher (und danach regelmäßig) ein Backup machen, bevor du deinen Windows Laptop mit Veracrypt verschlüsselst.

Wieso ist die Windows Version wichtig?

Die Verschlüsselungs-Optionen unter Windows hängen von der Windows Version ab. Wenn du Windows Home nutzt, bietet dir Windows die "Geräteverschlüsselung". Nutzt du Windows Pro oder Windows Enterprise, kannst du BitLocker nutzen. Hier findest du die Anleitung "Welche Windows Version nutze ich?".

Worin unterscheiden sich "Geräteverschlüsselung" und BitLocker?

Die Geräteverschlüsselung unter Windows 11 speichert den Wiederherstellungsschlüssel automatisch in deinem Microsoft Konto. Das heißt die Polizei könnte ihn bei Microsoft anfragen und so deine Festplatte entschlüsseln. Außerdem kannst ohne BitLocker keine Pre-Boot Authentication aktivieren. Dieses Feature ist sehr wichtig und wird weiter unten erlärt. Unter der Haube funktioniert die Verschlüsselung von Geräteverschlüsselung/BitLocker sehr ähnlich.

Was soll ich machen, wenn ich Windows Home habe?

Wenn du wirklich sicher sein willst solltest du dein System mit Veracrypt verschlüsseln. Alternativ kannst du auf Windows Pro upgraden, um die BitLocker-Features nutzen zu können. Für das Upgrade auf Windows Pro kannst du den offiziellen Weg gehen und Geld bezahlen. Alternativ gibt es im Internet auch Skripte, mit denen das geht. **Die "Geräteverschüsselung" auf Windows Home (ist wie BitLocker nur ohne Pre-Boot Authentication) sollte nicht als sicher angesehen werden.**

Ich nutze noch Windows 10, ist das ein Problem?

Die Anleitungen hier im Wiki basieren auf Windows 11. Die Anleitungen sollten aber auf Windows 10 genauso funktionieren. Solltest du noch das ältere Windows 10 haben, solltest du aber unbedingt upgraden. In Zukunft bekommt Windows 10 keine Updates mehr. In der Vergangenheit wurden verschiedene Sicherheitsprobleme in Bezug auf die Windows-Verschlüsselung durch Windows-Updates behoben.

Wie funktioniert die Windows-Verschlüsselung?

Moderne Laptops besitzen einen Sicherheitschip (TPM 2.0), der deine Festplatte beim Starten des Laptops automatisch entschlüsselt. Du musst heutzutage unter Windows kein Passwort eingeben, damit das Gerät entschlüsselt wird. Die PIN/Passwort, die du dann beim Anmelden eingibst, ist nicht das Passwort zum Entschlüsseln der Festplatte, sondern nur dein Benutzer*innen-Passwort (es kann ja mehrere Accounts auf dem Laptop geben). Dass du beim Starten kein Festplatten-Passwort eingeben musst ist bequem, aber nicht besonders sicher.

Was ist der Wiederherstellungsschlüssel?

Stell dir vor du kippst Wassser auf deinen Laptop und er geht nicht mehr an. Dann funktioniert die Festplatte meist noch, aber der Laptop startet halt nicht mehr. Du kannst deine Festplatte ausbauen und an einen anderen Laptop anschließen. Allerdings ist die Festplatte ja verschlüsselt. Und für die Entschlüsselung brauchst du den Sicherheitschip, der sich aber im (kaputten) Laptop befindet.

Deshalb gibt es Wiederherstellungsschlüssel (auch Recovery Key genannt). Das ist im Grunde ein automatisch generiertes langes Passwort, mit dem du deine Festplatte manuell entschlüsseln kannst.

Du solltest auf jeden Fall darauf achten, deinen Wiederherstellungsschlüssel zu sichern (Anleitung). Wenn die Polizei den Wiederherstellungsschlüssel in deine Hände bekommt, kann sie so deine Festplatte entschlüsseln. Daher solltest du den Wiederherstellungsschlüssel nicht im Microsoft-Konto speichern.

Was ist Pre-Boot Authentication?

Wenn die Pre-Boot Authentication aktiviert ist musst du beim Start des Laptops noch ein zusätzliches Passwort eingeben. Das Passwort wird an den Sicherheitschip geschickt. Wenn du das richtige Passwort eingegeben hast, rückt der Sicherheitschip den Schlüssel/Key heraus (mit dem die Festplatte verschlüsselt ist) und die Festplatte wird entschlüsselt. Da der Sicherheitschip auch einen Warte-Mechanichmus enthält (bei zu oft falsch eingegebenen Passwort musst du warten), kann das Passwort auch nicht gebrutefocrt werden. Das Passwort muss also nicht super kompliziert sein.

Warum ist Pre-Boot Authentication wichtig?

In den letzten Jahren sind immer wieder Schwachstellen bekannt geworden, durch die die Windows-Verschlüsselung einfach umgangen werden konnte. Beispiele:

- TPM-Sniffing-Angriff (2024, Demo auf YouTube)
- die Bitpixie-Schwachstelle (2024, wurde sehr lange nicht behoben)
- auf dem 39C3 (Kongress vom Chaos Computer Club) wurden mehrere Schwachstellen gezeigt, wie man durch das Ausnutzen von einfachen Logik-Fehlern die Windows-Verschlüsselung umgehen konnte (2025)
- die YellowKey-Schwachstelle, Verschlüsselung konnte sehr einfach umgangen werden (2026)

Wichtig: Bei all diesen Schwachstellen war das Problem, dass die Festplatte beim Start automatisch entschlüsselt wurde. **Systeme mit einem zusätzlichen Passwort (Pre-Boot Authentication) waren bei allen Problemen der letzten Jahre nicht betroffen.** Bendenke auch, dass dein Laptop über viele Monate bzw. Jahre bei der Polizei liegt und da da keine Sicherheitsupdates mehr bekommt.

Ist mein Laptop schon verschlüsselt?

Hier findest du die passende Anleitung dazu. Falls BitLocker bereits aktiviert wurde, aktiviere am besten noch zusätzlich Pre-Boot Authentication (Anleitung). Du benötigst dazu Windows Pro/Enterprise (Welche Windows Version nutze ich?).

Wie kann ich BitLocker aktivieren?

Das schöne an BitLocker ist, dass es relativ einfach zu aktivieren ist. Du musst vorher kein Backup machen. Eine Anleitung findest du hier. Nutzt du die "Geräteverschlüsselung" unter Windows Home, kannst du die Anleitung auch nutzen. Du musst nur "Geräteverschlüsselung" anstatt "BitLocker" im Startmenü suchen.

Wie kann ich Pre-Boot Authentication aktivieren?

Wenn du dir nicht sicher bist, ob du Pre-Boot Authentication schon aktiviert hast, kannst du mal in diese Anleitung schauen. Die Anleitung zur Aktivierung findest du hier. Du benötigst dazu Windows Pro/Enterprise (Welche Windows Version nutze ich?).

Wie kann ich meinen Wiederherstellungsschlüssel sichern?

Hier findest du die Anleitung dazu. Am besten speicherst du ihn in deinem Passwort-Manager.

Wie kann ich den Wiederherstellungsschlüssel aus dem Microsoft-Konto entfernen?

Dazu haben wir selbst keine Anleitung. Es gibt aber

- hier ein Video-Tutorial (auf Englisch) auf YoutTube.
- Hier findest du einen Blog-Post dazu (auf Englisch).
- Oder direkt zu Microsoft: https://account.microsoft.com/devices/recoverykey