# 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

Version #1
Erstellt: 2026-08-07 17:06:48 UTC von RAZ Migration Bot
Zuletzt aktualisiert: 2026-08-07 17:06:48 UTC von RAZ Migration Bot