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.

Version #1
Erstellt: 2025-07-05 15:15:47 UTC von RAZ Migration Bot
Zuletzt aktualisiert: 2025-07-05 15:15:47 UTC von RAZ Migration Bot