

Sicherheit in der IT

- Einen USB-Stick mit Bit-Locker verschlüsseln
- Verschlüsseln von Dateien und Ordnern

Einen USB-Stick mit BitLocker verschlüsseln

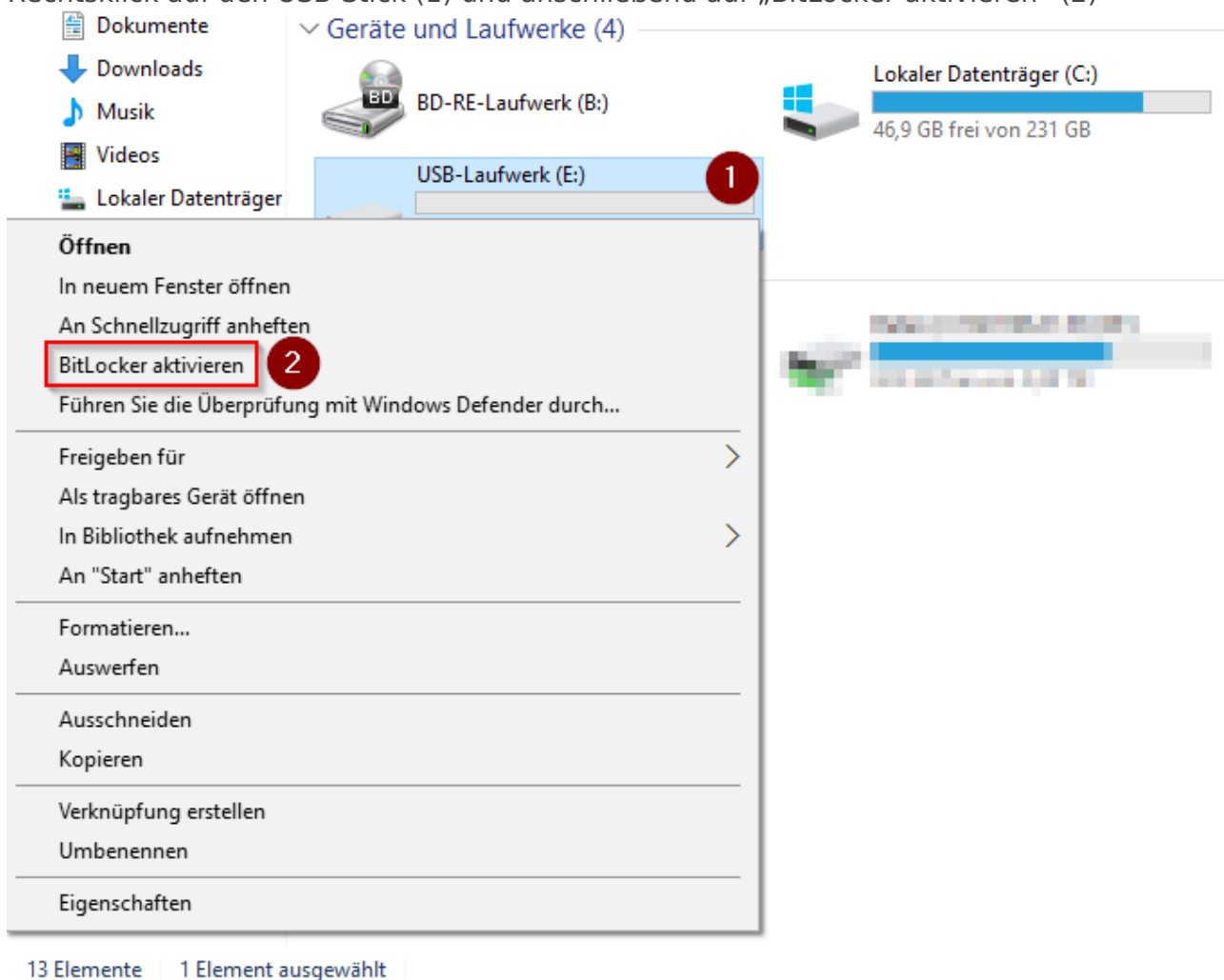
Kennen Sie das Problem?!? USB-Stick am Rechner vergessen bzw. irgendwo liegen gelassen? Dann die Angst: „Oh mein Gott! MEINE DATEN! Die Aufgaben! Die Lösungen! Oh Nein!“

Hier die Lösung für das Problem: Den USB-Stick mit BitLocker verschlüsseln! Okay das hilft nicht gegen das Vergessen, aber nicht jeder kann die Daten sofort lesen.

WICHTIG: Sichern Sie Ihre Daten vom USB-Stick vorab!


Und so geht's:

1. USB-Stick mit dem Computer verbinden
2. „Diesen PC“ mit Windows Explorer öffnen
3. Rechtsklick auf den USB-Stick (1) und anschließend auf „BitLocker aktivieren“ (2)



4. Als nächsten müssen Sie ein Passwort vergeben. Diese wird dann immer beim Verbinden abgefragt -> Also nicht vergessen!



←  BitLocker-Laufwerkverschlüsselung (E:)

Methode zum Entsperren des Laufwerks auswählen



Kennwort zum Entsperren des Laufwerks verwenden

Kennwörter sollten Groß- und Kleinbuchstaben, Zahlen, Leerzeichen und Symbole enthalten.

Kennwort eingeben

Kennwort erneut eingeben



Smartcard zum Entsperren des Laufwerks verwenden

Sie müssen Ihre Smartcard einstecken. Die Smartcard-PIN ist erforderlich, wenn Sie das Laufwerk entsperren.


Weiter

Abbrechen


! Bitte wählen Sie ein sicheres Passwort !

5. Zur Sicherheit werden nun aufgefordert den Wiederherstellungsschlüssel zu speichern. Legen Sie den Schlüssel an einem sicheren Ort ab! Ihr privates Home-Laufwerk der Schule wäre dafür zum Beispiel geeignet.



←  BitLocker-Laufwerkverschlüsselung (E:)

Wie soll der Wiederherstellungsschlüssel gesichert werden?

 Der Wiederherstellungsschlüssel wurde gespeichert.

Wenn Sie das Kennwort vergessen oder die Smartcard verlieren, können Sie mithilfe eines Wiederherstellungsschlüssels auf das Laufwerk zugreifen.

→ [In Microsoft-Konto speichern](#)

→ [In Datei speichern](#)

→ [Wiederherstellungsschlüssel drucken](#)

[Was ist ein Wiederherstellungsschlüssel?](#)

Weiter

Abbrechen

6. Wählen Sie hier die „Erstverschlüsselung“. Generel empfehlen wir das gesamte Laufwerk zu verschlüsseln.



Auswählen, wie viel Speicherplatz des Laufwerks verschlüsselt werden soll

Bei der Einrichtung von BitLocker auf einem neuen Laufwerk oder PC muss nur der derzeit verwendete Teil des Laufwerks verschlüsselt werden. Beim Hinzufügen neuer Daten werden diese von BitLocker automatisch verschlüsselt.

Falls Sie BitLocker auf einem bereits verwendeten PC oder Laufwerk aktivieren, sollten Sie das gesamte Laufwerk verschlüsseln. Durch die Verschlüsselung des gesamten Laufwerks wird der Schutz aller Daten sichergestellt. Dazu gehören auch gelöschte Daten, die möglicherweise immer noch abrufbare Informationen enthalten.


- ☐ Nur verwendeten Speicherplatz verschlüsseln (schneller, optimal für neue Computer und Laufwerke)
- ☒ Gesamtes Laufwerk verschlüsseln (langsamer, aber optimal für PCs und Laufwerke, die bereits verwendet werden)

Weiter

Abbrechen

7. Nun der Verschlüsselungsmodus!



←  BitLocker-Laufwerkverschlüsselung (E:)

Zu verwendenden Verschlüsselungsmodus auswählen

Mit Windows 10 (Version 1511) wird ein neuer Datenträger-Verschlüsselungsmodus (XTS-AES) eingeführt. Dieser Modus unterstützt zusätzliche Integrität, ist mit älteren Windows-Versionen aber nicht kompatibel.

Bei einem Wechseldatenträger, den Sie mit einer älteren Windows-Version verwenden möchten, sollten Sie den kompatiblen Modus wählen.

Bei einem Festplattenlaufwerk oder einem Laufwerk, das nur mit Geräten eingesetzt wird, auf denen Windows 10 (Version 1511) oder höher ausgeführt wird, sollten Sie den neuen Verschlüsselungsmodus wählen.


- ☒ Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeignet)
- ☐ Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)

Weiter

Abbrechen

8. Und ab geht's...



←  BitLocker-Laufwerkverschlüsselung (E:)

Möchten Sie das Laufwerk jetzt verschlüsseln?

Das Laufwerk kann mithilfe eines Kennworts entspert werden.

Die Verschlüsselung kann abhängig von der Größe des Laufwerks einige Zeit in Anspruch nehmen.

Bis zum Abschluss der Verschlüsselung werden die Dateien nicht geschützt.

Verschlüsselung starten

Abbrechen

9. Warten Warten Kaffee trinken ... Warten ... Warten ...

BitLocker-Laufwerksverschlüsselung



Verschlüsselung...

Laufwerk "E:": 99.8 % abgeschlossen



Anhalten



Halten Sie die Verschlüsselung an, bevor Sie das Laufwerk entfernen, da andernfalls die Dateien auf dem Laufwerk beschädigt werden können.

[BitLocker verwalten](#)

10. Und das war es auch schon. Ihre Daten werden ab sofort verschlüsselt gespeichert.

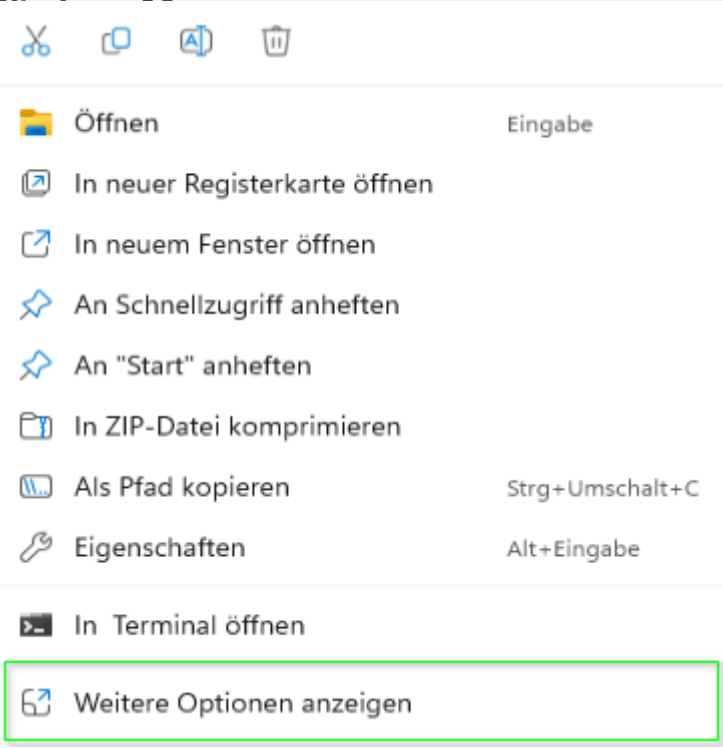
Verschlüsseln von Dateien und Ordnern

Das BSI [Bundesamt für Sicherheit in der Informationstechnik] empfiehlt eine Verschlüsselung von Dateien, Ordner sowie Datenträger nach dem Stand der Technik. Dazu existieren eine Reihe von Open-Source-Apps. Für eine Verschlüsselung stellen wir euch auf den Rechnern der Schule das Programm 7-Zip zur Verfügung. Mit diesem könnt Ihr Dateien auf sicherem Weg versenden (z.B. per E-Mail). Wichtig ist hierbei das ein sicheres Passwort zur Verschlüsselung gewählt wird und dieses auf einen zweiten unabhängigen Kommunikationsweg übermittelt wird (z.B. per Telefon). Versenden Sie niemals das Passwort und die Datei in einer E-Mail zusammen.

Wie funktioniert das nun?

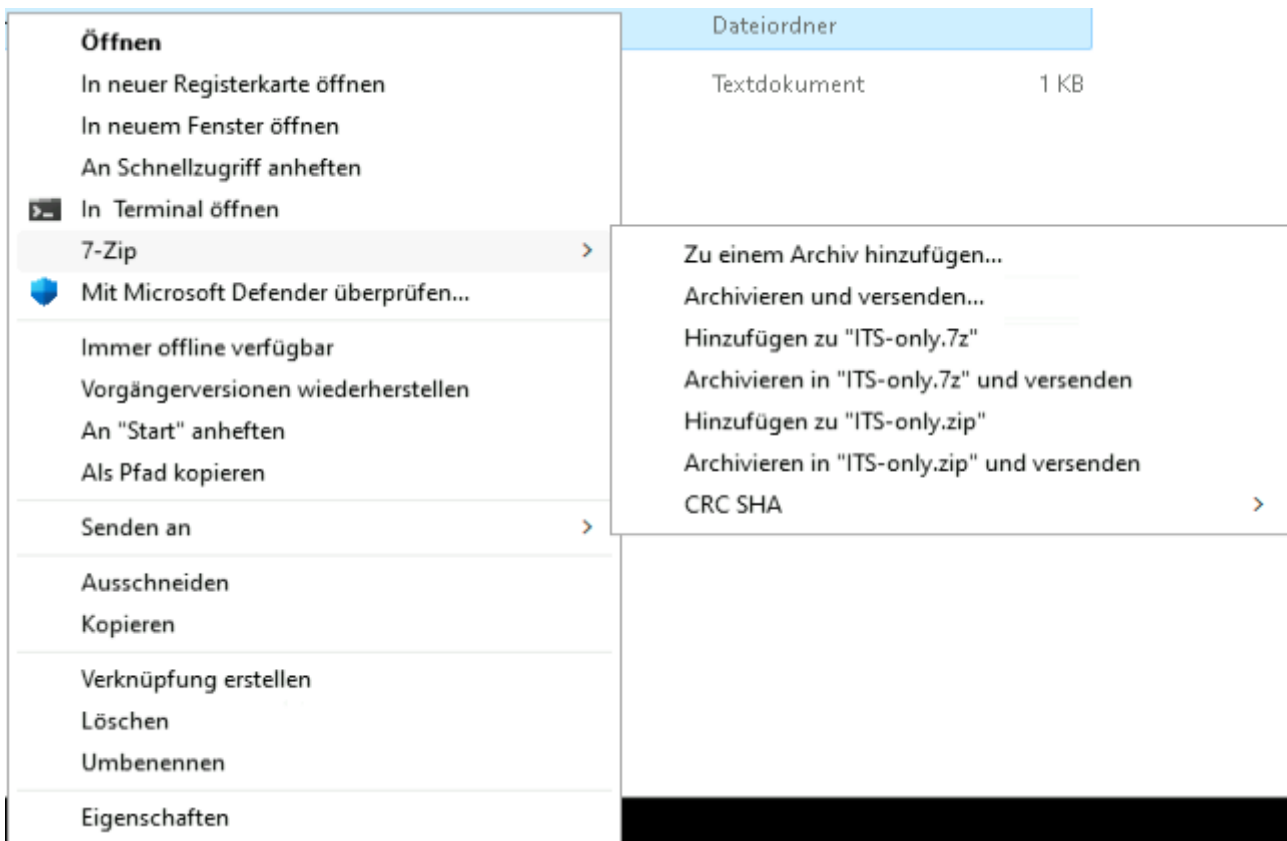
Sammelt die zu versenden Daten soweit noch nicht geschehen in einem Ordner. Auf diesem Ordner klickt Ihr nun mit der rechten Maustaste und ein Kontextmenü öffnet sich.

Besonderheit bei Windows 11



Bei Windows 11 muss man zuerst auf den Ordner klicken und dann das neue Kontextmenü öffnen. Erst dann kommt das gewohnte Menü.

Klick und dann öffnen. Erst dann kommt das gewohnte Menü.



Wählt im Kontextmenü die Punkt "7-Zip" und anschließend der Unterpunkt "Zu einem Archiv hinzufügen ..." aus.

Zu Archiv hinzufügen

Archiv: T:\ ITS-only.7z

Archivformat: 1 7z

Kompressionsstärke: 5 - Normal

Kompressionsverfahren: * LZMA2

Wörterbuchgröße: * 16 MB

Wortgröße: * 32

Größe solider Blöcke: * 4 GB

Anzahl CPU-Threads: * 4 / 4

Speicherbedarf beim Komprimieren: 656 MB / 3248 MB / 4060 MB * 80%

Speicherbedarf beim Entpacken: 18 MB

In Teildateien aufsplitten (Bytes):

Parameter:

Optionen

Art der Aktualisierung: Hinzufügen und Ersetzen

Verzeichnisstruktur: Relative Pfadangaben

Optionen

- ☐ Selbstentpackendes Archiv (SFX) erstellen
- ☐ Zum Schreiben geöffnete Dateien einbeziehen
- ☐ Dateien nach Komprimierung löschen

Verschlüsselung 2

Passwort eingeben: *****

Passwort bestätigen: *****

☐ Passwort anzeigen

Verfahren: AES-256

☐ Dateinamen verschlüsseln

OK Abbrechen Hilfe

Unter Punkt 1 sollte als Archivformat "7z" ausgewählt sein. Nicht jedes Archivformat unterstützt die Verschlüsselung.

Vergebt nun unter Punkt 2 einen sicheres Kennwort.

Anschließend könnt ihr das Archiv verschlüsselt erstellen lassen. Klick dazu einfach auf "OK".

Die neu erstelle Datei kann man nun über einen beliebigen Kommunikationsweg austauschen.

Und das war es auch schon.