

Anleitung



Bitlocker



Schützen Sie Ihre Daten durch Verschlüsselung

Verschlüsselung von Wechseldatenträgern mit Bitlocker

Wechseldatenträger, vor allem USB-sticks, gehen recht häufig verloren, was auch die Gefahr eines unberechtigten Zugriffs durch Dritte mit sich bringt. Auch wenn der Laptop, mit dem der USB-stick verwendet wird, durch Kennwort und sonstige Maßnahmen geschützt ist, gilt dieser Schutz nicht für den Wechseldatenträger. Alle auf ihm befindlichen Daten können ohne weiteres gelesen werden. Das ist eine gravierende Sicherheitslücke, die unbedingt geschlossen werden muß.

Den USB-stick vor unberechtigtem Zugriff zu schützen, ist ganz einfach und erfordert nur einige wenige Handgriffe. Der Schutz besteht darin, die Daten zu verschlüsseln. Im Windows-Betriebssystem ist ein gutes Verschlüsselungsprogramm enthalten: Bitlocker.

1. Arbeitsschritt: Bitlocker starten

Bitlocker kann auf verschiedenen Wegen aufgerufen werden, z.B. über die Systemsteuerung; um die Beschreibung nicht unnötig aufzublähen, wurde auf eine Aufzählung der alternativen Wege verzichtet.

a) Das Windowssymbol links unten in der Startleiste mit der rechten Maustaste anklicken und dort ...b) ... den Punkt "Suchen" auswählen.

c) Im Feld "Suchbegriff hier eingeben" "Bitlocker" eintragen.





d) Den link "Bitlocker verwalten" in der rechten Hälfte des Fensters starten.

Alle	Apps	Dokumente	Einstellungen	Fotos	s Mehr 🗸		Feedback	
Höchste	Übereins	timmung						
🤏 🛿	B itLocker Systemsteu	verwalten Ierung		\rightarrow				
						BitLocker verwalten Systemsteuerung		
					🗂 Öffnen			
,∕⊂ bitle	ocker ver	walten						

2. Bitlocker einrichten

a) Wenn Bitlocker das erste Mal gestartet wird, ist noch kein Laufwerk verschlüsselt und Bitlocker überall deaktiviert. Wählen Sie die Option "Wechseldatenträger – Bitlocker To Go".

Nystemsteuerung\System und Sicl	erheit\BitLocker-Laufwerkverschlüsselung			- C]	×
← → · ↑ ♣ > Systemsteu	rung > System und Sicherheit > BitLocker-Laufwerkverschlüsselung	ٽ ~	Systemsteueru	ng durchsu	chen	P
Startseite der Systemsteuerung	BitLocker-Laufwerkverschlüsselung					2
	Das Schützen der Laufwerke mit BitLocker trägt dazu bei, Dateien und Ordner vor nicht autorisiertem Zugriff zu schützen.					
	Betriebssystemlaufwerk					
	System (C:) BitLocker deaktiviert			\bigcirc		
	BitLocker aktivieren					
	Festplattenlaufwerke					
	Daten (D:) BitLocker deaktiviert			\odot		
	Wechseldatenträger - BitLocker To Go					
	F: BitLocker deaktiviert			\odot		
Siehe auch						
💎 TPM-Verwaltung						
Datenträgerverwaltung						
Datenschutzbestimmungen						

b) Wenn Sie die Maus über den Text "F: Bitlocker deaktiviert" ziehen, färbt sich das gesamte Feld hellblau.



Hinweis: F: steht hier für das Laufwerk des USB-sticks. Bei anderen Computerkonfigurationen kann sich ein davon abweichender Laufwerksbuchstabe ergeben (G: oder E:).



c) Nach einem Mausklick erscheint die Option "Bitlocker aktivieren".



d) Durch Anklicken der Option "Bitlocker aktivieren" wird das Laufwerk initialisiert.

Hinweis: dieses Fenster erscheint nur bei USB-sticks, nicht aber beim Verschlüsseln interner Festplatten.

÷	New BitLocker-Laufwerkverschlüsselung (F:)
	BitLocker wird gestartet
	Warten Sie, während das Laufwerk von BitLocker initialisiert wird.
	A Das Laufwerk darf beim BitLocker Setup nicht entfernt werden.
	Wie lauten die Systemanforderungen für BitLocker?
	Abbrechen

e) Kennworteingabe

Hinweis: Bitte beachten Sie, daß der Schutz Ihrer Daten einzig und allein am Kennwort hängt. Während der Zugriff auf in der Hochschulinfrastruktur gespeicherte Daten zusätzlich noch durch die Benutzerkennung abgesichert wird, steht zwischen Ihren Daten und dem Auge des Kriminellen nur das Kennwort.

→ Legen Sie also bitte besonders großen Wert auf ein komplexes, nicht herausfindbares Kennwort!

~	RitLocker-Laufwerkverschlüsselung (F:)	×
	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.	



f) Wiederherstellungssschlüssel generieren

Wenn man das Kennwort für die Anmeldung an der Hochschuldomäne vergessen hat, kann man es sich durch den Benutzerservice zurücksetzen lassen. Ein solches Verfahren ist, wie dies auch bei Bitlocker der Fall ist, nicht für individuell verwaltete Datenbestände möglich. Wenn das Bitlocker-Kennwort vergessen wird, können die verschlüsselten Daten nicht mehr entschlüsselt werden und wären unrettbar verloren. Dieser Gefahr begegnet Bitlocker durch die Generierung eines Wiederherstellungsschlüssels, also einer Art Ersatzkennwort. Falls man das eigentliche Bitlockpaßwort vergessen hat, kann man durch Eingabe des Wiederherstellungsschlüssels wieder auf die Daten auf dem USBstick zugreifen.

→ Wählen Sie die Option "In Datei speichern"

÷	RitLocker-Laufwerkverschlüsselung (F:)
	Wie soll der Wiederherstellungsschlüssel gesichert werden?
	1 Einige Einstellungen werden vom Systemadministrator verwaltet.
	Wenn Sie das Kennwort vergessen oder die Smartcard verlieren, können Sie mithilfe eines Wiederherstellungsschlüssels auf das Laufwerk zugreifen.
	\rightarrow In Datei speichern
	→ Wiederherstellungsschlüssel drucken
	Wie finde ich später meinen Wiederherstellungsschlüssel? Weiter Abbrechen

g) Wiederherstellungssschlüssel abspeichern

Speichern Sie die Textdatei, die den Wiederherstellungsschlüssel enthält, in einem geeigneten Ordner.

→ Y T → Dieser PC → XXXXX! (\\lbmpf	s03\home) (Z:) >		✓ [™] "msf441 (\\	bmpfs03\home) (🔎
anisieren 🔻 Neuer Ordner				≣= - (
Dieser PC ^ Name	Änderungsdatum	Тур	Größe	
3D-Objekte	17.07.2020 08:18	Dateiordner		
Bilder D	17.07.2020 11:00	Dateiordner		
Deskton	14.07.2020 09:48	Dateiordner		
Pi Pi	17.07.2020 08:22	Dateiordner		
Dokumente sc	17.07.2020 12:56	Dateiordner		
Downloads	16.07.2020 15:51	Dateiordner		
Musik 🔤 🗸	16.07.2020 15:51	Dateiordner		
Videos 🖹 N	14.07.2020 15:41	Textdokument	1 KB	
System (C:)				
Daten (D:)				
USB-Laufwerk (F				
Universal (U:)				
msf441 (\\lbmpf y				
		105 TVT		
Dateiname: BitLocker-Wiedemeistellungssch	USSEI DDC99E/B-183F-4926-A43D-9D79924EB	(85.171		
Dateityp: Textdateien (*.txt)				



h) Verschlüsselungsmethode wählen

Man muß sich zwischen zwei Methoden entscheiden, je nachdem ob der Datenträger bereits Daten enthält oder noch nicht. Bei einem ganz neuen Datenträger geht die Bitlockereinrichtung sehr schnell, da erst wirklich verschlüsselt wird, wenn Dateien auf dem Datenträger abgelegt werden. Befinden sich bereits Daten auf dem Datenträger, muß dieser komplett, byte für byte, verschlüsselt werden, was ziemlich lange dauert. Zur groben Orientierung: die Verschlüsselung eines 4 GB sticks hat ca. 15 Minuten gebraucht.

Falls ein USB-stick erst wenige Dateien enthält, empfiehlt es sich daher, diese auf einen anderen Speicherort zu verschieben und nach der Bitlockeinrichtung wieder zurückzuschieben, damit das schnellere Verfahren bei leeren Datenträgern genutzt werden kann.

>	<
← 🏘 BitLocker-Laufwerkverschlüsselung (F:)	
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)	
<u>Gesamtes Laufwerk verschlüsseln (langsamer, aber optimal für PCs und Laufwerke, die bereits</u> verwendet werden)	
<u>W</u> eiter Abbrechen	

Im darauffolgenden Fenster beläßt man die Voreinstellung, da diese für Wechseldatenträger am besten geeignet ist.

		~
🕂 🥀 BitLock	ker-Laufwerkverschlüsselung (F:)	
Zu verw	vendenden Verschlüsselungsmodus auswählen	
Mit Windo Dieser Mo	ows 10 (Version 1511) wird ein neuer Datenträger-Verschlüsselungsmodus (XTS-AES) e odus unterstützt zusätzliche Integrität, ist mit älteren Windows-Versionen aber nicht kr	eingeführt. ompatibel.
Bei einem den komp	ı Wechseldatenträger, den Sie mit einer älteren Windows-Version verwenden möchter patiblen Modus wählen.	n, sollten Sie
Bei einem Windows wählen.	n Festplattenlaufwerk oder einem Laufwerk, das nur mit Geräten eingesetzt wird, auf d 10 (Version 1511) oder höher ausgeführt wird, sollten Sie den neuen Verschlüsselungs	enen modus
() <u>N</u> euer \	Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeign	et)
● <u>K</u> ompa	itibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werd	en können)
	Weiter A	Abbrechen



i) Fertigstellen

÷	RitLocker-Laufwerkverschlüsselung (F:)
	Möchten Sie das Laufwerk jetzt verschlüsseln?
	Das Laufwerk kann mithilfe eines Kennworts entsperrt 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
	<u>V</u> erschlüsselung starten Abbrechen

Die Betätigung des Schalters "Verschlüsselung starten" schließt die Bitlockinstallation ab.

3. Sonstige Tätigkeiten und Hinweise

a) Zugriff auf ein verschlüsseltes Laufwerk

Wenn man ein mit Bitlocker verschlüsseltes Laufwerk anklickt, öffnet sich automatisch das Kennworteingabefenster. Nach Eingabe des Kennworts kann das verschlüsselte Laufwerk wie ein ganz normales Laufwerk genutzt werden. Die Entschlüsselung erfolgt während des Dateizugriffs. Die Arbeit mit der Datei wird durch die Entschlüsselung nicht merklich verzögert.

BitLocker (F:)
Geben Sie das Kennwort ein, um dieses Laufwerk zu entsperren.
Weitere Optionen
Entsperren

b) Wiederherstellungsschlüssel ablegen

Je seltener USB-sticks mit schutzwürdigen Daten verwendet werden, desto höher ist die Gefahr des Kennwortvergessens. Darum ist der Wiederherstellungsschlüssel außerordentlich wichtig und darum muß er auch sicher verwahrt werden. Sicher heißt: er sollte nicht von unberechtigten Dritten eingesehen werden können und er sollte zuverlässig zur Verfügung stehen. Das MIT empfiehlt, die Wiederherstellungsschlüssel-Textdatei an die eigene Mailadresse zu schicken und danach die ursprüngliche Schlüsseldatei zu löschen.

c) Wiederherstellungsschlüssel verwenden

In der Wiederherstellungsschlüsseldatei interessiert nur folgender Passus in der Mitte: Wiederherstellungsschlüssel:

344661-015147-581853-611545-651408-671418-452378-569921 (die genannten Zahlen sind fiktiv)



Die den sogenannten Bezeichner betreffenden Angaben beziehen sich auf in der PH Ludwigsburg nicht praktizierte Ablagevarianten, bei denen Schlüssel sehr vieler Anwender gemeinsam aufbewahrt werden.

• Sie klicken auf das USB-Laufwerk, wodurch sich das unter 3.a) beschriebene Kennworteingabefenster öffnet.

BitLocker (F:)
Geben Sie das Kennwort ein, um dieses Laufwerk zu entsperren.
Weniger Optionen
Wiederherstellungsschlüssel eingeben
Auf diesem PC automatisch entsperren
Entsperren

- Sie klicken auf "Weitere Optionen" und danach auf "Wiederherstellungsschlüssel eingeben".
- Der Eingabebildschirm für den Wiederherstellungsschlüssel öffnet sich. Man gibt nacheinander die 48 Ziffern ein; die Unterteilung in durch Bindestrich getrennte Sechserblöcke nimmt das System selbständig vor.

EitLocker (F:)	
Geben Sie den 48-stelligen Wiederherstellungsschlüssel Laufwerk zu entsperren. (Schlüssel-ID: 2D06FBE2)	ein, um dieses
	Entsperren

• Die Eingabe wird mit dem Schalter "Entsperren" bestätigt.

c) Keine Verfügbarkeitsgarantie

Hinweis: Bitlocker kann wie jedes andere Verschlüsselungsverfahren Ihre Daten nur vor unberechtigtem Zugriff (Lesen und Verändern) schützen, nicht jedoch die Daten selbst. Die Daten können also durch kriminelles Handeln oder unsachgemäße Handhabung gelöscht oder sonstwie unbrauchbar gemacht werden. Insbesondere kann der Datenträger formatiert werden, ohne daß Bitlocker ein Veto einlegt. Sie sollten daher wichtige Daten niemals ausschließlich auf einem mobilen Datenträger speichern, sondern immer auf den Netzlaufwerken. Der externe Datenträger sollte nur verwendet werden, um Daten mit anderen Personen auszutauschen oder um unabhängig vom Hochschulnetz arbeiten zu können.