Festplattenverschlüsselung mit MS-BitLocker

Der Microsoft Bitlocker ermöglicht die Verschlüsselung von Festplatten und erschwert/verhindert das Auslesen von Daten, z.B. bei Verlust/Diebstahl, eines Rechners.

Voraussetzung: aktueller Windows-Rechner & ein externes Speichermedium (z.B. USB-Stick)

So verschlüsseln und entschlüsseln Sie ihre Festplatte:

- 1. Gehen Sie auf "Dieser PC" und klicken Sie mit Rechtsklick auf das Laufwerk "C:"
- 2. Klicken Sie auf "BitLocker aktivieren"
- 3. Wählen Sie "In Datei speichern"

✓ Geräte und L	aufwerke (2)		 RitLocker-Laufwerkverschlüsselung (C:)
Lokale	r Datenträger (C:)	Video 1 (D:)	Wie soll der Wiederherstellungsschlüssel gesichert werden?
			 Einige Einstellungen werden vom Systemadministrator verwaltet.
151 GE	ifre O ED		Ein Wiederherstellungsschlüssel kann für den Zugriff auf Dateien und Ordner verwendet werden, falls Sie Ihren PC nicht entsperen können. Es wird empföhlen, mehrere Wiederherstellungsschlüssel getrennt vom PC aufzubewahren.
daten	(\\a 🚬 Öffnen	Eingabe	→ In Microsoft-Konto speichern
39,7 G	^{B fri} 🕜 In neuem Fenster öffner	Ifnen	→ Wiederherstellungsschlüssel druc <u>k</u> en
	BitLocker aktivieren	<hr/> 2.	Wie finde ich später meinen Wiederherstellungsschlüssel?
	🕹 Formatieren	4	Weiter Abbrechen

- 4. Wählen Sie einen Speicherort aus (z.B. einen USB-Stick oder Server-Laufwerk) und gehen Sie auf Speichern.
- 5. Wählen Sie eine der möglichen Optionen

Reit ocker-Wiedehenstellungsschlüssel speichem unter								
$\leftarrow \rightarrow \checkmark \uparrow$ Disser PC	✓ C Dieser PC durchsuchen ₽	 ReitLocker-Laufwerkverschlüsselung (C:) 						
Organisieren • > OndDrive > OndDrive • Ondbrive • Ondbrive <	B: Videos	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 altivieren, sollten Sie das gesamte Laufwerk verschlüsselt. Durch die Verschlüsseltung 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 Cor • Gesamtes Laufwerk verschlüsseln (langsamer, aber optimal für PCs und Laufw verwendet werden)						
Dateiname: BitLocker-Wiederherstellungsschlüssel 2F2CD36C-24C3-4697-8A8E-7270B1CCC7B9	~							
Dateityp: Textdateien (*.txt)	~							
∧ Ordner ausblenden	Speichern Abbrechen	Weiter Abbrechen						

- 6. Wählen Sie "Neuer Verschlüsselungsmodus" und gehen auf "Weiter"
- 7. Aktivieren Sie die BitLocker-Systemprüfung und gehen auf "weiter"

	×			×
¢	🛛 🎭 BitLocker-Laufwerkverschlüsselung (C:)		← 🏘 BitLocker-Laufwerkverschlüsselung (C:)	
	Zu verwendenden Verschlüsselungsmodus auswählen		Möchten Sie das Laufwerk jetzt verschlüsseln?	
	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.		Je nach Größe des Laufwerks dauert der Verschlüsselungsvorgang unter Umständen eine Weile.	
	Bei einem Wechseldatenträger, den Sie mit einer älteren Windows-Version verwenden möchten, sollten Sie den kompatiblen Modus wählen.		Sie können Ihre Arbeit fortsetzen, während das Laufwerk verschlüsselt wird. Die Leistung des Comp kann jedoch eingeschränkt sein.	uters
	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.		BitLocker-Systemüberprüfung ausführen Die Systemüberprüfung stellt sicher, dass BitLocker die Wiederherstellungs- und Verschlüsselungsschlüssel richtig lesen kann, bevor das Laufwerk verschlüsselt wird.	
	• Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät <u>deeidnet)</u>		Der Computer wird von BitLocker vor der Verschlüsselung neu gestartet.	1
	\odot Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfern 6 .		Hinweis: Diese Prüfung kann einige Zeit dauern, wird jedoch empfohlen, um ausgewählte Methode zum Entsperren ohne Wiederherstellungsschlüssel fur 7 .	s die
	Weiter Abbrechen		Weiter Abb	echen

Die Verschlüsselung, wird nach dem Neustart durchgeführt. Geschützte Laufwerke (Speichermedien) sind an dem eingeblendeten Schloss zu erkennen.



BitLocker-Schutz anhalten/deaktivieren

- 1. Gehen Sie auf "Dieser PC" und klicken Sie mit Rechtsklick auf das Laufwerk "C:"
- 2. Gehen Sie auf "Weitere Optionen anzeigen" und auf "BitLocker verwalten"
- 3. Gehen Sie auf "BitLocker deaktivieren"

BitLocker-Laufwerkverschlüsselung						
\leftarrow \rightarrow \checkmark \uparrow \square > Syst	emsteuerung > System und Sicherheit >	BitLocker-Laufwerkverschlüsselung v C	م			
Startseite der Systemsteuerung	BitLocker-Laufwerkverschlüsse	lung	•			
	Das Schützen der Laufwerke mit BitLocke zu schützen.	er trägt dazu bei, Dateien und Ordner vor nicht autorisiertem Zugriff				
	1 Zu Ihrer Sicherheit werden einige Einstellungen vom Systemadministrator verwaltet.					
	Betriebssystemlaufwerk					
	C: BitLocker aktiviert		^			
	1	 Schutz anhalten Wiederherstellungsschlüssel sichern BitLocker deaktivieren 	3.			
	Festplattenlaufwerke	L				
	Video 1 (D:) BitLocker deaktiv	iert	~			
	Wechseldatenträger - BitLocker To Go					
Siehe auch	Schließen Sie einen USB-Speicherstick	: an, um BitLocker To Go zu verwenden.				
TPM-Verwaltung Datenträgerverwaltung						
Datenschutzbestimmungen						

4. Die Laufwerksverschlüsselung wird aufgehoben

