

Verschlüsselung externer Datenträger

EDV-Betreuung Abt. Psychologie (psyadmin@uni-bielefeld.de)

23. Februar 2024

1 Verschlüsselung: Wie und wofür?

Im Arbeitsalltag der Abt. Psychologie kommt es regelmäßig vor, dass mit Daten mit hohem oder sehr hohem Schutzbedarf (wie bspw. Gesundheitsdaten) gearbeitet wird. Diese Daten müssen auch gelegentlich auf externen Datenträgern wie z.B. USB-Sticks und externen Festplatten gespeichert und weitergegeben werden. Damit sensible Daten im Falle von Verlust oder Diebstahl des Datenträgers nicht in unbefugte Hände geraten, muss dieser verschlüsselt werden. Es ist daher notwendig, alle externen Datenträger, die dienstlich genutzt werden, zu verschlüsseln.

Hierfür stehen derzeit zwei verschiedene Methoden zur Verfügung, die Komfort in der Nutzung mit einem sehr hohen Sicherheitsstandard verbinden: **Bitlocker** und **Veracrypt**. Beide Methoden entsprechen dem Stand der Technik, was die Sicherheit angeht, und können daher für Daten aller Schutzbedarfsklassen verwendet werden. Wenn Sie sich bzgl. des Schutzbedarfs Ihrer Daten unsicher sein sollten, berät die DISK der Abt. Psychologie Sie gerne.

Von den verfügbaren Lösungen bietet Bitlocker den etwas größeren Nutzungskomfort, sodass wir empfehlen, in reinen Windows-Umgebungen auf diese Lösung zu setzen. Sollten hingegen in Ihrer AE Macintosh-Rechner eingesetzt werden, so empfehlen wir an dieser Stelle den Einsatz von Veracrypt, da Bitlocker auf dem Mac auf kostenpflichtige Zusatzsoftware angewiesen ist. Das Team der EDV-Betreuung berät Sie gerne bei der Auswahl der passenden Lösung für Ihre AE oder Ihr Projekt.

2 Bitlocker

Im folgenden wird Schritt für Schritt erklärt, wie man einen externen Datenträger mit Bitlocker verschlüsselt. Hierfür sind keine Adminrechte notwendig.



Abbildung 1: Option "Bitlocker aktiveren" im Kontextmenü (Rechtsklick) des Windows-Explorers

🎕 Billocker-Laufweiserschlämitung (D)	
Methode zum Entsperren des Laufwerks auswählen	
Einige Einstellungen werden vom Systemadministrator verwaltet.	
C Bernwort zum Entsperen des Laufwerks verwenden	
Kennwörter sollten Groß- und Kleinbuchstaben, Zahlen, Leerzeichen und Symbole enthalten.	
Kenneort eingeben	
Kenneort eingeben	
Smertcard zum Entsperren des Laufwerks verwenden	
Sie müssen ihre Smartcard einstecken. Die Smartcard-PIN ist erfonderlich, wenn Sie das Laufwerk entsperren.	

Abbildung 2: An dieser Stelle legen Sie ein mindestens achtstelliges Passwort für den Datenträger fest.

-	Ritocke Lasheriverschizselung (D)			
	Wie soll der Wiederherstellungsschlüssel gesichert werden?			
	One Wiederheitelkungsschlüssel konste nicht an diesem Speicherort gespeichert werden. Wählen Sie einen anderen Speicherort.			
	Worn Sie das Kennwort vergessen oder die Smartcard verlieren, können Sie mithöfe eines Wiederherstellungsschlissels auf das Laufwerk zugreifen.			
	→ In Datei speichern			
	→ Wiederherstellungsschlüssel drucken			
	We finds ich später meinen Wederberstelungsschlissef!			
	Witter Akknecke			

Abbildung 3: Bitte speichern Sie den Wiederherstellungsschlüssel oder drucken Sie ihn aus und verwahren Sie ihn an einem sicheren Ort. Ohne Schlüssel oder Passwort kann auch die EDV-Betreuung den Datenträger nicht entschlüsseln!

	×		
H	🔨 Billocker-Laufwerkverschlässlung (D)		
	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 werschlisselt werden. Beim Hinzufligen neuer Daten werden diese von Bitlocker automatisch verschlisselt.		
	Falls Sie Bittocker auf einem benehts werwendeten PC oder Laufwerk aktivieren, sollten Sie das gesonnte Laufwerk verschlösseln. Durch die Verschlösselnung das gesannten Laufwerks wiel der Schutz aller Daten sicherspröfelt. Dezu gehören auch gelöschle Deten, die rectglicherweise immer noch absorbare Informationen enthalten.		
	Nar verwendeten Speicherpletz verschlassen (schneller, optimal far neue Computer und Laufwerke)		
	 Gesentes Laufwerk verschlüsseln (langsamer, aber optimol für PCs und Laufwerke, die bereits verwendet werden) 		
	Weiter Abbrechen		

Abbildung 4: Hier sollte für neue und bereits genutzte Datenträger die jeweils empfohlene Option ausgewählt werden.

3 Veracrypt

Die Verschlüsselung mit Veracrypt ist etwas komplizierter einzurichten als Bitlocker. Es ist außerdem erforderlich, dass die Software "Veracrypt" auf Ihrem System installiert ist.

	×
÷	💘 Bittocker-Lasfweriverschlässelung (D)
	Zu verwendenden Verschlüsselungsmodus auswählen
	Mit Windows 10 (Version 1511) wird ein neuer Datentstiger Verschlisserkungsmocks (XTS-AES) eingeführt. Dieser Modus unterstützt zusätzliche Integrität, ist mit älleren Windows-Versionen aber nicht kompatibel.
	Bei einem Wechseldstentsiger, den Sie mit einer äbren Windows-Version verwenden müchten, sollten Sie des kompetiblen Modus wählen.
	Bei einem Peutpleitenlaufwerk oder einem Laufwerk, dan nar mit Gestilten eingesetzt wird, auf denen Windows 10 (Nersion 1511) oder höher ausgeführt wird, sollten Sie den neuen Verschlässelungsmodus wihlen.
	Neuer Verschlüsselungsmodus (am besten für Festplattenlaufverke auf desem Gesit geeignet)
	(Kompatible: Modux (am besten für Laufwerke geeignet, sie von diesem Gerät entfernt werden können)
	Weiter Abbrechen

Abbildung 5: Hier bitte den neuen Verschlüsselungsmodus wählen.



Abbildung 6: Verschlüsselung starten.

\$8.cdd	e-Laufwerksverschlösselung	
	Verschlüsselung	
	Lashwerk "D.": 42.6 % abgeschlossen	
		Ashabes
A H	alten Sie die Verschlüsselung an, bewor Sie das uhweik entformer, die andernfalls die Dateien if dem Laufwerk beschlidigt werden können.	
5	Locker verwalten	

Abbildung 7: Die Verschlüsselung kann, gerade bei bereits belegten Datenträgern, einige Zeit in Anspruch nehmen.