Festplattenverschlüsselung

Allgemeines

Bitte beachten Sie die den Unterschied zwischen Kennwort, PIN und erweiterter PIN.

- **Kennwort**: Von Kennwörtern wird gesprochen, wenn es sich um eine Authentifizierung des Users gegenüber dem System **ohne Nutzung von TPM** handelt.
- **PIN/Erweiterter PIN**: Von PIN wird gesprochen, wenn es sich um eine Authentifizierung des Users gegenüber dem System **mit Nutzung von TPM** handelt.
 - Pin: Zahlen von 0-9
 - **Erweiterter Pin:** Verschiedene Zeichen (Groß- und Kleinbuchstaben, Symbole, Zeichen, Leerzeichen)

An der Jade Hochschule wird BitLocker für **Systeme ohne Anbindung an das Active-Directory** angeboten - also vorrangig für mobile Geräte.

Vorbereitungen

- 1. Sichern Ihrer persönlichen Daten bzw. des Systems!
- 2. Wird der Rechner von einer oder mehreren Personen genutzt?
 - Empfehlung bei Einzelnutzung: Entsperrung des Laufwerks durch ein Kennwort (s.u.)
 - Empfehlung bei Nutzung mit mehreren Personen: Entsperrung des Laufwerks mit einem USB-Speicherstick (s.u.)
- 3. Passwort für lokales Windows-Konto vergeben, falls noch nicht geschehen
- 4. Betriebssystem auf den neusten Stand aktualisieren (Windows-Update)
- 5. TPM-Status im BIOS/UEFI überprüfen **Bitte aktivieren!** Die Abbildungen dienen lediglich als Hilfestellung. Je nach Modell kann die Darstellung im BIOS/UEFI abweichen.
 - BIOS/UEFI aufrufen bei Dell: F2

ettings	TPM 2.0 Security	
General		
- System Configuration	TPM On	Clear
Video		
- Security	PPI Bypass for Enable Commands	Attestation Enable
Admin Password		
- System Password	PPI Bypass for Disable Commands	Key Storage Enable
Strong Password		
Password Configuration	PPI Bypass for Clear Command	V SHA-256
Password Bypass		
- Password Change	Disabled	
Non-Admin Setup Changes		
UEFI Capsule Firmware Updates	(Enabled	
TPMI20 Security		
Computrace(R)	This option lets you control whether the Trust	ted Platform Module (TPM) Endorsement Hierarchy is available
CPO XD Support	to the operating system. Disabling this setting	g restricts the ability to use the TPM for signing and signature
Admin Setup Lockeut	operations.	
Master Parquerd Lockout		
	Key Storage Enable :	and Distorm Module (TDM) Storage Managing is sustable to the
Secure Boot	operating system. Disabling this setting restri	icts the ability to use the TPM for storing owner data
Intel® Software Guard Extensions™		
Performance	SHA-256 :	
Power Management	This setting controls the type of hash algorithm	m that is used by the TPM. When this option is checked, the
- POST Behavior	BIOS and the TPM will use the SHA-256 hash	algorithm to extend measurements into the TPM PCRs during
Manageability	setting should be left in the default configurat	tion (checked) under most circumstances.
Virtualization Support		
- Wireless	Disabled/Enabled :	
Maintenance	Disabled - When this option is selected, t	he TPM will be disabled. It will not execute any commands
System Logs	information	sources, nor will it allow any access to stored owner
	Enabled = When this option is selected, th	the TPM will be enabled. This is the normal operating state for
	the TPM when you want to use	e its complete array of capabilities.
		Restore Settings Apply Exit

0

TPM Embedded Security		N
TPM Specification Version	20	M
TPM Device	Available 0	
TPM State		
Clear TPM	On next boot	
TPM Activation Policy	No prompts	
:Fl aufrufen bei Lenov	/o: F1, F2 oder <u>ESC (Modella</u> t	∙hängig)
:Fl aufrufen bei Lenov	/o: F1, F2 oder ESC (Modellab)hängig)
Fl aufrufen bei Lenov	/o: F1, F2 oder ESC (Modellab Security ity Chip	ohängig) Item Specific
Fl aufrufen bei Lenov Secur Secur rity Chip Type rity Chip	/o: F1, F2 oder ESC (Modellab Security ity Chip TPM 2.0 (Enabled)	ohängig) Item Specific Enablel Security chip is
Fl aufrufen bei Lenov Secur rity Chip Type rity Chip	vo: F1, F2 oder ESC (Modellat Security ity Chip TPM 2.0 (Enabled)	ohängig) Item Specific [Enable] Security chip is functional.
Fl aufrufen bei Lenov Secur Trity Chip Type Trity Chip Trity Chip Trity Reporting Opt Trity Reporting Opt	/o: F1, F2 oder ESC (Modellak Security ity Chip TPM 2.0 (Enabled) tions [Enter]	ohängig) Item Specific [Enable] Security chip is functional. [Disabled] Security chip is
Fl aufrufen bei Lenov Secur Trity Chip Type Trity Chip Trity Reporting Opt ar Security Chip el (R) TXT Feature	vo: F1, F2 oder ESC (Modellak Security ity Chip TPM 2.0 [Enabled] Lions [Enter] [Disabled]	Dhängig) Item Specific IEnableJ Security chip is functional. IDisabledJ Security chip is hidden and is not functional.
Fl aufrufen bei Lenov Secur Trity Chip Type Trity Chip Trity Chip Trity Reporting Opt Trity Reporting Opt Trity Reporting Opt Trity Chip Trity Chip Trity Chip Trity Chip Trity Chip Trity Chip	vo: F1, F2 oder ESC (Modellak Security rity Chip TPM 2.0 (Enabled) tions [Enter] [Disabled] Clear [Disabled]	ohängig) Item Specific [Enable] Security chip is functional. [Disabled] Security chip is hidden and is not functional.

6. Lokale Gruppenrichtlinien für BitLocker anpassen (s.u.)

Select Item

Select Menu

7. Kennwort/Pin für BitLocker ausdenken/erstellen

Help

Exit

- 8. USB-Stick für Entschlüsselungs-Key bereithalten (nur sehr geringe Speicherkapazität erforderlich)
 - Für die Authentifikation mittels USB-Stick wird eine weiterer USB-Stick benötigt

F5/F6

Enter

Change Values

Select ► Sub-Menu

Einrichtung

Anpassung der lokalen Gruppenrichtlinien

Vorgehensweise:

Setup Defaults

Save and Exit

F9

F10

1. Öffnen Sie die lokalen Gruppenrichtlinien mit Eingabe von gpedit.msc in der Windows Suchmaske. Expandieren Sie anschließend in den Ordner Computerkonfiguration \rightarrow Administrative Vorlagen \rightarrow Windows-Komponenten \rightarrow BitLocker Laufwerksverschlüsselung. Anschließend klicken Sie auf Betriebssystemlaufwerke.

2. Unter Betriebssystemlaufwerke öffnen Sie mit einem Doppelklick "Zusätzliche Authentifizierung beim Start anfordern".

Editor f ür lokale Gruppenrichtlinien	0	– 🗆 ×
Datei Aktion Ansicht ?		
💠 🏟 🙍 📷 📴 🖬 🐨		
 Windows-Einstellungen Administrative Vorlagen Drucker Metzwerk Server Startmenü und Taskleiste System Systemsteuerung Windows-Komponenten ActiveX-Installerdienst Anwendungskompatibilität App-Datenschutz App-Datenschutz App-Laufzeit Arbeitsordner Audiorecorder Audiorecorder Benutzerschnittstelle für Anmeldeinformationen Bereitstellung von App-Paketen Bil Locker-Laufwerkverschlüsselung Betriebssystemlaufwerke 	Betriebssystemlaufwerke Markieren Sie ein Element, um dessen Beschreibung anzuzeigen.	Einstellung Einstellung Ei Netzwerkentsperrung beim Start zulassen Ei Sicheren Start für Integritätsüberprüfung zulassen Ei Zusätzliche Authentifizierung beim Start anfordern Ei Zusätzliche Authentifizierung beim Start erforderlich (Win Ei PIN- oder Kennwortänderung durch Standardbenutzer nik Ei InstantGo- oder HSTI-kompatible Geräte benötigen keine Ei Verwendung der BitLocker-Authentifizierung mit erforderi Ei Erweiterte PINs für Systemstart zulassen Ei Minimale PIN-Länge für Systemstart konfigurieren Ei Verwendung der hardwarebasierten Verschlüsselung für B Ei Laufwerkverschlüsselungstyp auf Betriebssystemlaufwerk Ei Verwendung von Kennwörtern für Betriebssystemlaufwerk Ei Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerk Ei TPM-Plattformvalidierungsprofil für systemeigene UEFI-F Ei Meldung und URL für die Pre-Boot-Wiederherstellung kon Ei Plattformvalidierungsdaten nach BitLocker-Wiederherstell
Wechseldatenträger		Erweitertes Validierungsprofil für Startkonfigurationsdater
Cloudinneit Patei-Explorer	Foweitert Standard	< >>
19 Einstellung(en)	Commencer (Juditional)	

3. Aktivieren Sie die Option und stellen Sie sicher, dass bei "BitLocker ohne kompatibles TPM zulassen (…)" **kein** Häkchen gesetzt ist. Nun übernehmen Sie die Auswahl und bestätigen mit "OK".

Zusätzliche Authent	ifizierung beim Sta	rt anfordern			-		\times
Zusätzliche Authent	tifizierung beim Sta	rt anfordern		Vorherige Einstellung	Nächste Eins	tellung	
 Nicht konfiguriert Aktiviert Deaktiviert 	Kommentar:						×
	Unterstützt auf:	Mindestens	Windows Ser	ver 2008 R2 oder Windows	; 7		< >
Optionen:			Hilfe:				
BitLocker ohne komp ein Kennwort oder eir Systemstartschlüssel e Einstellungen für Compu TPM-Start konfigurieren TPM-Systemstart-PIN ko Systemstart-PIN bei TPM	atibles TPM zulasse n USB-Flashlaufwer erforderlich) uter mit einem TPM : TPM zulassen onfigurieren: M zulassen	n (hierfür ist k mit	Mit dieser F BitLocker b Authentifiz TPM (Trust Richtliniene angewende Hinweis: Be Authentifiz Richtlinienf	Richtlinieneinstellung könn ei jedem Computerstart ei ierung erfordert und ob Si ed Platform Module) verw einstellung wird bei Aktivie et. eim Start kann nur eine der ierungsoptionen erforderli fehler auftritt.	nen Sie konfigur ine zusätzliche e BitLocker mit o renden. Diese erung von BitLoo r zusätzlichen ich sein, da ande	ieren, ob oder ohne cker ernfalls ein	^
TPM-Systemstart-PIN bei TPM TPM-Systemstartschlüssel bei TPM-Systemstartschlüssel un Systemstartschlüssel un	el konfigurieren: i TPM zulassen el und -PIN konfigu d PIN bei TPM zula	urieren: ssen	Falls Sie Bit möchten, a kompatible entweder e Verwendun Schlüsselin verwendet ein USB-Sti wird der Zu das Laufwe	Locker auf einem Comput ktivieren Sie das Kontrollk is TPM zulassen". In dieser in Kennwort oder ein USB- g eines Systemstartschlüss formationen, die zum Vers werden, auf dem USB-Lau ck entsteht. Wenn der USB griff auf das Laufwerk aut rk zugegriffen werden. We	er ohne TPM ve ästchen "BitLoci n Modus ist für Laufwerk erford sels werden die schlüsseln des La fwerk gespeiche Stick eingestec hentifiziert, und enn der USB-Stic	rwenden ker ohne den Start lerlich. Bei aufwerks ert, wodurc kt wird, es kann au k verloren	¦h ⊿f
				ОК	Abbrechen	Übernehr	nen

Verschlüsselung

Öffnen Sie die BitLocker Verwaltung durch Eingabe von "BitLocker verwalten" in die Windows Suchmaske. Aktivieren Sie BitLocker für das gewünschte Laufwerk in dem Sie auf "**BitLocker aktivieren**" klicken. All Ditt a clean I auf unde sourch Kingshur

itartseite der Systemsteuerung	BitLocker-Laufwerkverschlüsselung
	Das Schützen der Laufwerke mit BitLocker trägt dazu bei, Dateien und Ordner vor nicht autorisiertem Zugrif zu schützen.
	Betriebssystemlaufwerk
	System-Win10E-64 (C:) BitLocker deaktiviert
	SitLocker aktivieren
	Festplattenlaufwerke
	BitLocker (E:) BitLocker deaktiviert
	SitLocker aktivieren
	Wechseldatenträger - BitLocker To Go
Siehe auch	Schließen Sie einen USB-Speicherstick an, um BitLocker To Go zu verwenden.
TPM-Verwaltung	
Datenträgerverwaltung	
Datenschutzbestimmungen	

Laufwerk auswählen [Bildquelle: Lennart Thurow]

Hinweis: Bitte beachten Sie, dass bei einer Verschlüsselung der Systemfestplatte ein vorher festgelegtes Kennwort während des Startvorgang des Rechners abgefragt wird. Falls eine Festplatte oder Partition verschlüsselt wird, die lediglich als Datenspeicher fungiert, so erfolgt hier keine Abfrage eines Kennworts.

Festlegen, wie das Laufwerk beim Start entsperrt werden soll

Wählen Sie hier

- USB-Speicherstick anschließen bei Nutzung mit mehreren Personen
- Pin eingeben bei Einzelnutzung

Pin zum Entsperren des Laufwerks erstellen

Bedingt durch den Versionsstand von Windows 10 können verschiedene Möglichkeiten angeboten werden, das Laufwerk zu entsperren. Seitens des Hochschulrechenzentrums wird lediglich die Nutzung einer Pin bzw eines Sticks angeboten.

Wie soll der Wiederherstellungsschlüssel gesichert werden

- Möglichkeit 1: Auf USB-Speicherstick speichern
 - Verwenden Sie diesen jedoch nur zur Sicherung des Wiederherstellungsschlüssels, nicht für andere Aufgaben
- Möglichkeit 2: In Datei speichern (Empfehlung des HRZ)
 - Speichern Sie die Wiederherstellungsdatei in einem Ort außerhalb Ihres PCs (z.B. Laufwerk Z:\)

Möglichkeit 3: Wiederherstellungsschlüssel drucken
 Ausdruck auf Papier

Der Wiederherstellungsschlüssel darf sich niemals auf dem verschlüsselten Gerät befinden. Je nach Version und Versionsstand von Windows 10 kann es vorkommen, dass angeboten wird den Wiederherstellungsschlüssel auf einem Microsoft-Konto zu speichern - wovon wir abraten. Grundsätzlich ist es empfehlenswert den Schlüssel auf einem Medium zu speichern, welches nicht jederzeit erreichbar ist.

Auswählen, wie viel Speicherplatz des Laufwerks verschlüsselt werden soll

Wählen Sie hier die Option "Gesamtes Laufwerk verschlüsseln"

 \times

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.

- O 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

Zu verwendenden Verschlüsselungsmodus auswählen

Wählen Sie hier die Option "Neuer 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)

O Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)

Waiter Abbrechen	Abbrechen	
weiter Abbrechen	Abbrechen	

Möchten Sie das Laufwerk jetzt verschlüsseln?

Aktivieren Sie die Option "BitLocker-Systemüberprüfung ausführen" und folgen Sie den Anweisungen. Der Computer muss dann zur BitLocker-Laufwerksverschlüsselung neu gestartet werden.

Optionen

Verschlüsselung von externen Datenträgern

1. Bitlocker auf entsprechenden Laufwerk aktivieren

🙀 BitLocker Drive Encryption				- 🗆	\times
$\leftarrow ightarrow \uparrow i i i i i i i i i i i i i i i i i i $	ol Panel > All Control Panel Items > Bit	Locker Drive Encryption 🗸	ڻ		,p
Control Panel Home	BitLocker Drive Encryptio Help protect your files and folder	N s from unauthorised access by protecting your drives with BitLocker.			0
	Operating system drive				
	OS (C:) BitLocker on			\odot	
	1	 Suspend protection Change how drive is unlocked at start-up Back up your recovery key Change PIN Turn off BitLocker 			
	Fixed data drives				
	Removable data drives -	BitLocker To Go			
	F: BitLocker off			\odot	
See also TPM Administration Disk Management	-	Turn BitLocker on			
Privacy statement					

2. Passwort eingeben und auf weiter klicken

3. Recovery-Key drucken und auf einem externen Datenträger speichern. Dieser Datenspeicher sollte ausschließlich zur Verwahrung des Recovery-Keys dienen. Beachten Sie bitte auch die Möglichkeit unserer Verwahrfunktion unter Laufwerk "x" (Siehe Abschnitt: "Wie soll der Wiederherstellungschlüssel gespeichert werden")

←	Rev BitLocker Drive Encryption (F:)	^
	How do you want to back up your recovery key?	
	 Some settings are managed by your system administrator. 	
	If you forget your password or lose your smart card, you can use your recovery key to access your drive.	
	ightarrow Save to your Microsoft account	
	\rightarrow Save to a file	
	\rightarrow Print the recovery key	
	How can I find my recovery key later?	
	Next Cance	I

4. Bitte wählen Sie "gesamtes Laufwerk verschlüsseln" aus.

 \sim

🙀 BitLocker-Laufwerkverschlüsselung (E:)

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)

5. Wählen Sie bitte den kompatiblen Modus aus.

🙀 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 f
ür Laufwerke geeignet, die von diesem Ger
ät entfernt werden k
önnen)

	Weiter Abbrechen
--	------------------

6. Vorgang bestätigen. Abschließend ist Ihr externer Datenträger verschlüsselt

Entschlüsselung von Laufwerken

Um das Laufwerk zu entschlüsseln müssen Sie auf weitere Optionen klicken und anschließend "Wiederherstellungsschlüssel eingeben" wählen.

Info: Falls Sie bereits vorher das Kennwort zum Entsperren des Laufwerks eingegeben haben oder das Laufwerk automatisch entsperrt wird, ist bei einer anschließenden Entschlüsselung die Eingabe des Wiederherstellungsschlüssels nicht notwendig und auch nicht möglich*.

BitLocker kann dementsprechend mit Eingabe des Kennwortes komplett deaktiviert werden, ohne dass eine zusätzliche Kennung/Identifizierung notwendig ist. Deaktivierung ist in diesem Fall mit Entschlüsselung gleich zu setzen.

*bezieht sich auf einen Benutzer mit Administratorrechten. Die Deaktivierung von BitLocker kann durch Beschränkung der Rechte eines Standardbenutzers unterbunden werden.

Entsperrung von Laufwerken

- Sie können die automatische Entsperrung eines Laufwerkes aktivieren oder deaktivieren. Hierfür rufen Sie mit Rechtklick auf das Laufwerk "BitLocker verwalten" auf
- Entsperrung durch Doppelklick auf das Laufwerk und Eingabe des Kennworts (Falls es sich nicht um eine Systempartition handelt)
- Automatische Entsperrung des Laufwerks bei bestimmten Rechnern. Hierfür wird das Häkchen bei "Auf diesem PC automatisch entsperren" gesetzt und durch Eingabe des Passworts bestätigt

BitLocker (F:)

Geben Sie das Kennwort ein, um dieses Laufwerk zu entsperren.

Weniger Optionen

Wiederherstellungsschlüssel eingeben

Auf diesem PC automatisch entsperren



Entsperrung von Laufwerken

Systemstartschlüssel auf mehreren USB-Speichersticks speichern

Öffnen Sie mit Rechtsklick auf einem mit BitLocker geschütztem Laufwerk das Menü "BitLocker verwalten". Hier kann der Systemstartschlüssel dupliziert werden. Alternativ lässt sich die Datei auch kopieren. Diese ist standardmäßig allerdings als Systemdatei markiert und daher ausgeblendet.

Informationen

HRZ-Wiki - https://hrz-wiki.jade-hs.de/

Quellen

From: https://hrz-wiki.jade-hs.de/ - **HRZ-Wiki**

Permanent link: https://hrz-wiki.jade-hs.de/de/tp/pc-t/hdd-encryption

Last update: 2024/03/04 06:20

