

Um Daten vor dem Zugriff Dritter zu schützen, ist eine Verschlüsselung der Daten die beste Wahl. Wir zeigen Ihnen, wie Sie Ihre komplette Festplatte verschlüsseln können und so einen Rundumschutz gewährleisten. Dabei kommt die mit Vista eingeführte Bitlocker-Funktion zum Einsatz und für alle, die darauf keinen Zugriff haben, das kostenlose Tool „TrueCrypt“, das nun auch für Vista tauglich ist.

- Die Vorteile der Laufwerksverschlüsselung F 16/2
- Das müssen Sie über Bitlocker wissen F 16/3
- Die erste Maßnahme: Aktivieren Sie die Nutzung eines USB-Sticks F 16/4
- Bereiten Sie die Festplatte für Bitlocker vor F 16/5
- Schon kann es losgehen: Festplattenverschlüsselung mit Bitlocker F 16/6
- Die Verschlüsselung rückgängig machen F 16/8
- Panne: Der USB-Schlüssel funktioniert nicht mehr F 16/9
- Panne: Die Verschlüsselung funktioniert einwandfrei, aber Windows Vista startet nicht mehr F 16/10
- Windows Vista Home und Windows XP verschlüsseln Sie mit TrueCrypt F 16/12
- So nutzen Sie TrueCrypt F 16/13
- Im Pannenfall hilft die TrueCrypt-Notfall-CD F 16/17
- So erzeugen Sie primäre Partitionen F 16/18
- Alternative: Festplatten mit integrierter Verschlüsselung F 16/20

Autor: Sascha Mölck



Wer persönliche Daten auf seinem PC gespeichert hat, beispielsweise die Steuererklärung oder Informationen über die eigenen Finanzen, hat kein Interesse daran, dass irgendjemand Zugang dazu bekommt. Die einzige Möglichkeit, dies sicher zu verhindern, ist die Verschlüsselung der Daten.

Windows Vista enthält eine Verschlüsselungsfunktion

Windows Vista enthält eine Verschlüsselungsfunktion: Bitlocker. Bitlocker verschlüsselt keine einzelnen Dateien, sondern die einzelnen Partitionen der Festplatte. Leider ist Bitlocker nur unter Windows Vista Ultimate und Enterprise nutzbar. Unter den übrigen Vista-Versionen und unter Windows XP können Sie die Festplatte mit dem Freeware-Tool „TrueCrypt“ verschlüsseln.

Sichern Sie vorher Ihre Daten!

Bevor Sie überhaupt beginnen, eine der Anleitungen dieses Artikels anzuwenden, gilt es, Ihre persönlichen Daten zu sichern. Denn bei jeder Operation an der Festplatte kann es zu Datenverlusten kommen. Daher erstellen Sie vorher eine Sicherheitskopie!

Die Vorteile der Laufwerksverschlüsselung

Alle Dateien sind wirksam geschützt!

- Sämtliche Daten eines Laufwerks werden verschlüsselt. Sie müssen nicht jedes Mal daran denken, eine Datei zu verschlüsseln.
- Auf die Daten eines Windows-PCs kann man immer von außen zugreifen – beispielsweise mit einer Windows-Installations-DVD/-CD. Bei einer verschlüsselten Festplatte ist das unmöglich.
- Sollten Sie einmal Ihre Festplatte verkaufen, dann müssten Sie sich keine Sorgen machen, dass der Käufer Ihre Daten auf der Festplatte wiederherstellen könnte.

- Sollten Sie Ihr Notebook irgendwo vergessen, käme niemand an Ihre Daten heran.
- Niemand hat Zugriff auf temporäre Daten, aus denen man ersehen könnte, was Sie am PC gemacht haben.



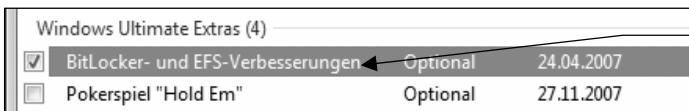
Grundsätzlich sinkt die Arbeitsgeschwindigkeit des PCs durch die Verschlüsselung ein wenig. Bei einer normalen PC-Nutzung werden Sie davon nichts spüren. Nur wenn Sie den PC an seine Leistungsgrenzen führen, dürften Sie etwas merken.

Die Verschlüsselung senkt die Arbeitsgeschwindigkeit

Das müssen Sie über BitLocker wissen

Seit der Veröffentlichung von Windows Vista hat Microsoft BitLocker zweimal erweitert: In Form eines Windows Ultimate Extras wurde ein Assistent hinzugefügt; seit dem Service Pack 1 kann BitLocker auch Nicht-Systempartitionen verschlüsseln. Wir setzen beide Erweiterungen voraus.

Spielen Sie zuerst alle BitLocker-Aktualisierungen ein

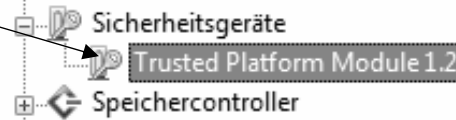


Diese Erweiterung sollten Sie installieren.

Windows Ultimate Extras lassen sich über die Windows Update-Funktion einspielen.

BitLocker kennt zwei Authentifizierungsmöglichkeiten. Erst nach erfolgreicher Authentifizierung startet das verschlüsselte System. Das Hauptaugenmerk legt Microsoft auf ein sogenanntes „Trusted Platform Module“, einen speziellen Chip innerhalb eines PCs. In dem Chip wird ein Schlüssel abgelegt, der erst den Zugriff auf die verschlüsselten Laufwerke erlaubt. Die wenigsten Rechner enthalten einen solchen Chip. Bei Business-Notebooks ist er allerdings geläufig.

Der Chip muss mindestens die TPM-Version 1.2 unterstützen.

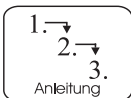


Der Geräte-Manager verrät, ob ein TPM-Chip vorhanden ist.

Wird nur der TPM-Chip genutzt, kann trotzdem noch jeder Nutzer auf den PC zugreifen. Daher kann man den TPM-Schutz noch mit weiteren Schutzmöglichkeiten kombinieren. So kann eine PIN abgefragt werden, ein USB-Schlüssel benutzt werden oder beides zusammen.

BitLocker lässt sich auch mit einem USB-Stick nutzen

Da vermutlich die meisten Nutzer von Windows Vista Ultimate oder Enterprise über keinen PC mit TPM-Chip verfügen, gibt es auch eine Möglichkeit, BitLocker ohne einen TPM-Chip zu nutzen. Dabei wird ein USB-Stick sozusagen als „Zündschlüssel“ verwendet. Ist der Stick nicht eingesteckt, dann startet der PC nicht. Wir zeigen Ihnen, wie Sie BitLocker mit einem USB-Zündschlüssel nutzen.



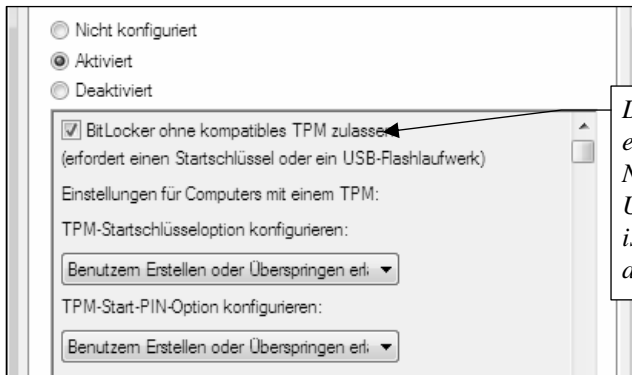
Die erste Maßnahme: Aktivieren Sie die Nutzung eines USB-Sticks

Standardmäßig ist BitLocker darauf eingestellt, einen TPM-Chip zur Authentifizierung zu nutzen. Alle anderen Möglichkeiten müssen manuell aktiviert werden. So gehen Sie vor:

Öffnen Sie den Gruppenrichtlinien-Editor

1. Klicken Sie im Startmenü auf „Alle Programme/Zubehör/Ausführen“. Geben Sie in das Feld „Öffnen“ den Befehl „gpedit.msc“ ein und klicken Sie auf „OK“. Es öffnet sich der lokale Gruppenrichtlinien-Editor.
2. Öffnen Sie in der Spalte am linken Rand den Ast „Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/BitLocker-Laufwerkverschlüsselung“.

3. Doppelklicken Sie dann im rechten Teil des Fensters auf „Systemsteuerungssetup: Erweiterte Startoptionen aktivieren“. Es öffnet sich ein Eigenschaften-Dialog. Setzen Sie innerhalb des Dialogs die Funktion auf „Aktiviert“ und klicken Sie auf „OK“.



Diese Option ermöglicht die Nutzung eines USB-Sticks. Sie ist standardmäßig aktiviert.

So sollte der Dialog bei Ihnen aussehen.

Bereiten Sie die Festplatte für BitLocker vor

Um eine Verschlüsselung zu ermöglichen, benötigt BitLocker zwei sogenannte primäre Partitionen. Bei der Systempartition von Windows handelt es sich immer um eine primäre Partition. Sollte auf Ihrem PC nur eine solche Partition vorhanden sein, können Sie einen kleinen Teil der Systempartition abzwicken und eine neue Partition erstellen. Diese benötigt BitLocker, um die eigentlichen Partitionen zu verschlüsseln.

Microsoft stellt für diese Aufgabe das „BitLocker Laufwerkvorbereitungstool“ bereit. Dieses kommt mit dem auf Seite 3 erwähnten Windows Ultimate Extra auf Ihr System. Der Assistent spaltet einen Teil (ca. 1,5 GB) vom Systemlaufwerk ab und erzeugt auf diesem Teil ein neues Laufwerk mit dem Buchstaben „S:“.

BitLocker benötigt zwei Partitionen

Ein Assistent erledigt die Aufteilung der Festplatte

Hier finden Sie den Assistenten

Der Assistent arbeitet vollautomatisch. Sie müssen keine Einstellungen vornehmen. Er verbirgt sich im Startmenü unter „Alle Programme/Zubehör/Systemprogramme/BitLocker“.

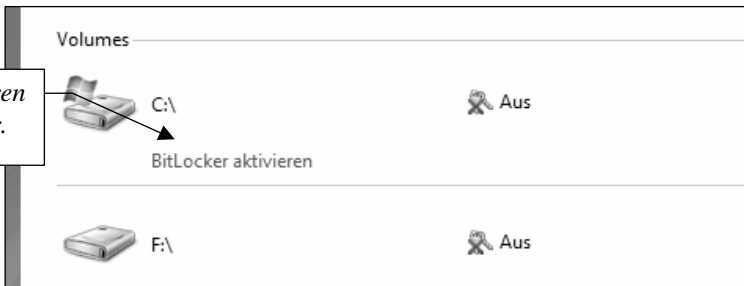
Schon kann es losgehen: Festplattenverschlüsselung mit BitLocker

Haben Sie alle Vorbereitungen abgeschlossen, dann können Sie auch schon mit der Verschlüsselung loslegen:

1. Öffnen Sie die Systemsteuerung und aktivieren Sie die klassische Ansicht. Doppelklicken Sie dann auf das Symbol „BitLocker-Laufwerksverschlüsselung“.
2. Sie sehen nun alle Partitionen, die verschlüsselt werden können. Zuerst muss allerdings die Systempartition verschlüsselt werden. Erst danach lassen sich auch weitere Partitionen verschlüsseln. Klicken Sie auf „BitLocker aktivieren“.

Als Erstes muss die Systempartition verschlüsselt werden

Hier aktivieren Sie BitLocker.



Diese Partitionen kann BitLocker verschlüsseln.

Zuerst wird der „Zündschlüssel“ erstellt ...

3. Als Erstes wird der künftige „Zündschlüssel“ des PCs erstellt. Stöpseln Sie Ihren USB-Stick ein und klicken Sie auf „Systemstart-USB-Schlüssel ist bei jedem Systemstart erforderlich“. Wählen Sie im nächsten Fenster den USB-Stick und klicken Sie auf „Speichern“.

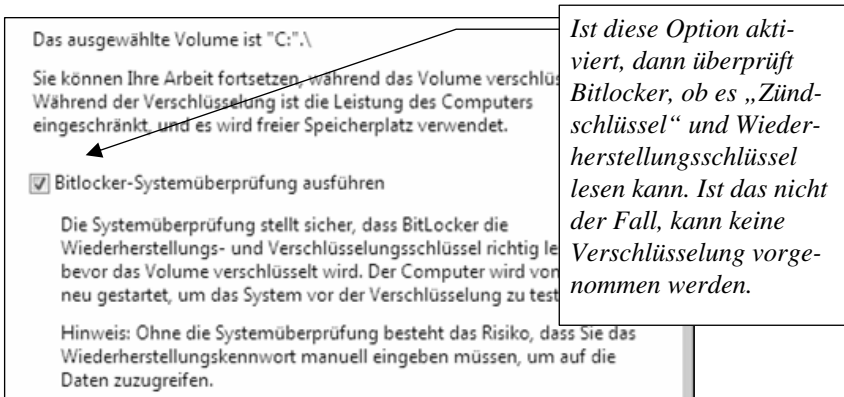
4. Anschließend erzeugt Bitlocker einen Wiederherstellungsschlüssel. Mit diesem können Sie auf die Festplatte zugreifen, falls der USB-Schlüssel (oder – wenn vorhanden – der TPM-Chip) gelöscht wird oder nicht mehr funktioniert.

... und dann ein Wiederherstellungsschlüssel

Bitlocker gibt Ihnen die Möglichkeit, dieses Passwort ebenfalls auf einem USB-Stick zu speichern, es auszudrucken oder es in einer Datei auf einer unverschlüsselten Partition der Festplatte zu speichern. Wählen Sie eine Möglichkeit. Danach klicken Sie wieder auf „Weiter“.

Ein Ausdruck des Wiederherstellungsschlüssels ist vielleicht die beste Wahl, da in den anderen beiden Fällen der Datenträger zerstört werden kann und somit der Wiederherstellungsschlüssel verloren ist. Das gedruckte Wiederherstellungskennwort sollten Sie aber gut wegschließen.

5. Nun befinden Sie sich im Dialog „Volume verschlüsseln“. Aktivieren Sie die Option „Bitlocker-Systemüberprüfung ausführen“ und klicken Sie auf „Weiter“.



Der letzte Schritt vor der Verschlüsselung



**Das BIOS
muss USB-
Geräte erken-
nen können**

6. Bitlocker fordert Sie zu einem Neustart auf. Kommen Sie dem nach und klicken Sie auf „Jetzt neu starten“.

Hinweis: Damit Sie Bitlocker mit einem USB-Stick nutzen können, muss das BIOS Ihres PCs schon beim Start in der Lage sein, USB-Geräte zu erkennen. Sollte Bitlocker nach dem Neustart melden, dass es den Schlüssel nicht lesen kann, könnte hier der Grund liegen. Entweder ist diese Funktion deaktiviert oder Ihr BIOS verfügt nicht über eine solche Funktion. Konsultieren Sie hierzu das Handbuch Ihres BIOS. Oft findet sich eine entsprechende Option unter der Bezeichnung „USB Legacy Support“.

7. War die Überprüfung von Zünd- und Wiederherstellungsschlüssel erfolgreich, startet nach dem Neustart automatisch die Verschlüsselung. Diese läuft im Hintergrund. Sie können währenddessen problemlos das System nutzen.
8. Die Vorgehensweise zur Verschlüsselung weiterer Laufwerke ist identisch. Allerdings muss kein weiterer Zündschlüssel angelegt werden, sondern lediglich ein separater Wiederherstellungsschlüssel für jedes weitere Laufwerk. Anschließend lässt sich die Verschlüsselung direkt starten.

**Weitere Lauf-
werke ver-
schlüsseln
Sie so**

Von nun an müssen Sie immer erst den USB-Zündschlüssel anstöpseln, bevor Sie Ihren PC starten.

Die Verschlüsselung rückgängig machen

**So machen
Sie die Ver-
schlüsselung
rückgängig**

Wer die Verschlüsselung nicht mehr nutzen möchte, kann diese auch wieder rückgängig machen. Rufen Sie dazu einfach den Dialog aus Schritt 2 des vorigen Abschnitts auf und klicken Sie auf „Bitlocker deaktivieren“. Im dann folgenden Fenster klicken Sie auf „Laufwerk entschlüsseln“.

Sollen bestimmte Systemänderungen durchgeführt werden, rät Microsoft, BitLocker vorher zu deaktivieren. Dies wird empfohlen bei der Aktualisierung des BIOS, beim Austausch des Mainboards, beim Einbau der Festplatte in einen anderen PC oder bei der Aktualisierung des Vista-Systemkerns bzw. der Boot-Komponenten. Danach können Sie BitLocker wieder aktivieren. Die Deaktivierung läuft wie die Entschlüsselung. Nur im letzten Dialog klicken Sie auf „BitLocker deaktivieren“ statt auf „Alle Laufwerke deaktivieren“.

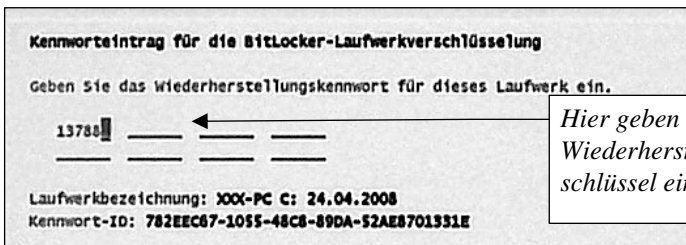
Vor Änderungen am System sollten Sie BitLocker deaktivieren

Panne: Der USB-Schlüssel funktioniert nicht mehr

Für den Fall der Fälle, dass der USB-Zündschlüssel verloren geht, zerstört wird oder durch irgendetwas anderes unlesbar wird, gibt es den Wiederherstellungsschlüssel. Mit diesem lässt sich das System trotzdem starten:

Mit dem Wiederherstellungsschlüssel können Sie auf das System zugreifen

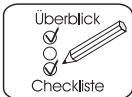
1. Werden Sie nach dem Systemstart aufgefordert, den USB-Schlüssel einzustöpseln, drücken Sie stattdessen die Eingabetaste.
2. Im nächsten Fenster werden Sie aufgefordert, den Wiederherstellungsschlüssel einzugeben. Kommen Sie dem nach. Haben Sie diesen korrekt eingegeben, fährt das System hoch.



Der Wiederherstellungsschlüssel ist eine 48-stellige Zahlenfolge.

Erstellen Sie anschließend einen neuen Zündschlüssel

3. Nach dem Start des Systems können Sie einen neuen Zündschlüssel anlegen. Rufen Sie dazu in der Systemsteuerung den BitLocker-Dialog auf und klicken Sie im Bereich des Systemlaufwerks auf den Link „BitLocker-Schlüssel verwalten“. Im nächsten Fenster klicken Sie dann auf „Systemstartschlüssel kopieren“.



Panne: Die Verschlüsselung funktioniert einwandfrei, aber Windows Vista startet nicht mehr

Sollte der USB-Schlüssel problemlos funktionieren, Windows aber anschließend nicht starten, weil es einen Defekt aufweist, können Sie vielleicht mithilfe der Windows Vista-DVD auf die verschlüsselte Festplatte zugreifen und Ihre Daten retten. Sie können die Daten mithilfe der Eingabeaufforderung auf ein anderes Laufwerk kopieren.

Ein Dateimanager erleichtert den Zugriff auf die Daten

Wer es einfacher haben möchte, kann einen Dateimanager auf einen USB-Stick speichern und diesen Dateimanager dann mithilfe der Eingabeaufforderung aufrufen. Ihre Daten lassen sich so viel einfacher kopieren. Wie empfohlen für diese Aufgabe den kostenlosen Dateimanager „A43“. Verwenden Sie dabei die „Portable“-Version. Nur diese lässt sich von einem USB-Stick starten. Laden Sie den Dateimanager unter folgender Adresse herunter und entpacken Sie ihn auf einen USB-Stick:

<http://www.portablefreeware.com/?q=A43>

Rufen Sie die Reparaturoptionen der Windows Vista-DVD auf

1. Booten Sie Ihren PC mit der Windows Vista-DVD. Nach einiger Zeit öffnet sich das Windows Vista-Installationsprogramm. Klicken Sie im ersten Fenster auf „Weiter“. Innerhalb des zweiten Fensters klicken Sie auf die Schaltfläche „Computerreparaturoptionen“.

2. Standardmäßig erkennt die Vista-DVD eine mit Bitlocker verschlüsselte Partition und fordert Sie an dieser Stelle auf, den Wiederherstellungsschlüssel einzugeben. Dazu öffnet sich ein Assistent. Geben Sie den Wiederherstellungsschlüssel ein. Anschließend wird nach Vista-Versionen auf Ihrer Festplatte gesucht. Klicken Sie dann auf „Weiter“.
3. Im Fenster „Systemwiederherstellungsoptionen“ klicken Sie auf die Verknüpfung „Eingabeaufforderung“. Innerhalb der Eingabeaufforderung geben Sie den Befehl „Diskpart“ ein und drücken dann die Enter-Taste.
4. Zuerst müssen Sie herausfinden, welche Laufwerksbuchstaben der USB-Stick zugewiesen bekommen hat. Geben Sie dazu den Befehl „list volume“ ein und bestätigen Sie mit der Enter-Taste. Haben Sie die gesuchten Informationen bekommen, beenden Sie das Programm „Diskpart“ mit dem Befehl „exit“.

Die Vista-DVD kann auf verschlüsselte Partitionen zugreifen

Öffnen Sie die Eingabeaufforderung

Diskpart verrät Ihnen die nötigen Laufwerksbuchstaben

```
DISKPART> list volume
```

Volume ###	Bst	Bezeichnung	DS	Typ	Größe
Volume 0	H	IOMEGA_HDD	NTFS	Partition	298 GB
Volume 1	C		RAW	Partition	18 GB
Volume 2	D		NTFS	Partition	1500 MB
Volume 3	E	Volume	NTFS	Partition	5887 MB
Volume 4	G	VOLUME	FAT32	Wechselmed	3906 MB
Volume 5	F	VistaLite	CDFS	CD	3026 MB

Der USB-Stick trägt den Laufwerksbuchstaben „G:“ – erkennbar an der Bezeichnung „Wechselmedium“ in der Spalte „Typ“. Wir haben zusätzlich noch eine externe Festplatte angeschlossen (Laufwerk „H:“), auf die die Daten kopiert werden.

5. Wechseln Sie auf den USB-Stick. Geben Sie dazu dessen Laufwerksbuchstaben ein und drücken Sie auf „Enter“.

So starten Sie den Dateimanager innerhalb der Eingabeaufforderung

6. Anschließend wechseln Sie in den Entpackordner des A43-Dateimanagers – in unserem Beispiel ist dies der Ordner „a43“. Geben Sie den Befehl „cd a43“ ein und drücken Sie auf „Enter“.
7. Nun rufen Sie das Tool auf, indem Sie „a43.exe“ eingeben und erneut die Enter-Taste betätigen.

Das Bitlocker Repair Tool gibt es nur für Unternehmenskunden

Falls Sie sich einmal näher mit Bitlocker beschäftigen, werden Sie über kurz oder lang auf das „Bitlocker Repair Tool“ stoßen. Mit diesem Tool lassen sich die Daten einer defekten verschlüsselten Partition auf eine andere Festplatte kopieren, falls der Zugang zum System weder mit dem USB-Zündschlüssel noch mit dem Wiederherstellungsschlüssel möglich ist. Wir hätten Ihnen dieses nützliche Tool gerne näher vorgestellt, doch leider ist es nur für Unternehmenskunden erhältlich. Privatkunden steht es nicht zur Verfügung.

Windows Vista Home und Windows XP verschlüsseln Sie mit TrueCrypt

TrueCrypt gibt's kostenlos

„TrueCrypt“ ist ein kostenloses Verschlüsselungs-Tool. Bisher war TrueCrypt darauf spezialisiert, verschlüsselte Containerdateien zu erstellen, die sich sozusagen als verschlüsselte Laufwerke ins System einbinden lassen.

Auch Systempartitionen können verschlüsselt werden

Seit der Version 5 kann TrueCrypt auch die Systempartition von Windows verschlüsseln – so wie Bitlocker. Im Gegensatz zu Bitlocker lässt TrueCrypt den Zugang zum System aber nur mit einem Passwort zu. Sie finden TrueCrypt hier:

<http://www.truecrypt.org/>

Soll nur die Systempartition verschlüsselt werden, können Sie sofort loslegen. Möchten Sie aber noch eine weitere Partition verschlüsseln, gilt es, die Festplatte darauf vorzubereiten. TrueCrypt kann nur primäre Partitionen verschlüsseln. Andere Partitionen müssten Sie erst umwandeln. Unter Windows Vista müssen Sie sich darüber keine Sorgen machen. Vista-Partitionen kann TrueCrypt generell verschlüsseln. Unter Windows XP könnte eine Umwandlung nötig sein. Wie dies funktioniert, zeigen wir Ihnen unter der Überschrift „So erzeugen Sie primäre Partitionen“ ab Seite F 16/18.

Die Festplatte vorbereiten

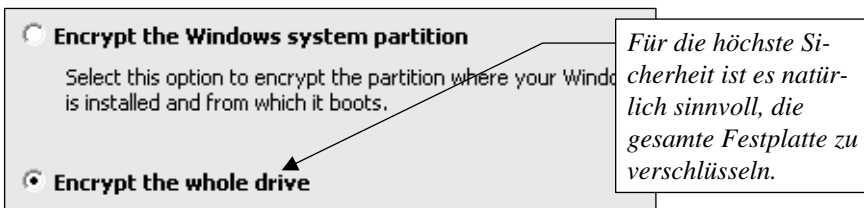
So nutzen Sie TrueCrypt

Wir zeigen Ihnen die Nutzung von TrueCrypt an folgendem Beispiel: Auf Ihrer Festplatte sind zwei primäre Partitionen eingerichtet. Auf der einen Partition ist Windows installiert, auf der anderen Partition befinden sich Ihre Daten. Beide Partitionen werden verschlüsselt:



Das ist unser Szenario

1. Starten Sie TrueCrypt und klicken Sie im Menü „System“ auf den Eintrag „Encrypt System Partition/Drive...“.
2. Sie werden als Erstes gefragt, ob die Systempartition von Windows („Encrypt the Windows system partition“) oder die gesamte Festplatte („Encrypt the whole drive“) verschlüsselt werden soll. Wählen Sie die Option „Encrypt the whole drive“ und klicken Sie auf „Next“.



Welche Partitionen sollen verschlüsselt werden?

Nutzen Sie mehrere Betriebssysteme?

3. Sind auf Ihrem PC mehrere Betriebssysteme installiert, wählen Sie im nächsten Fenster die Option „Multi-boot“, ansonsten die Option „Single-boot“. In unserem Beispiel wählen wir „Single-boot“. Klicken Sie dann auf „Weiter“.

Das will TrueCrypt wissen, falls Sie „Multi-boot“ gewählt haben

Sollten Sie die Option „Multi-boot“ gewählt haben, müssen Sie nun noch drei Zwischenschritte absolvieren: Sie werden gefragt, ob das aktuell laufende Betriebssystem auf dem Boot-Laufwerk installiert ist. Anschließend möchte TrueCrypt wissen, auf wie vielen Festplatten Ihres PCs ein Betriebssystem installiert ist. Danach werden Sie gefragt, ob auf Ihrem System ein Nicht-Windows-Bootloader installiert ist. Das kommt vor, wenn Sie beispielsweise neben Windows Linux auf Ihrem PC installiert haben.

4. Wählen Sie den Verschlüsselungsalgorithmus aus. Ändern Sie dabei an den Vorgaben nichts. Klicken Sie dann auf „Next“.

Als Verschlüsselungsalgorithmus („Encryption Algorithm“) wird „AES“ benutzt.

Der „Hash Algorithm“ ist eine Art Zufallsgenerator. Dieser erzeugt die Zeichenfolge aus Schritt 6.

Encryption Options

Encryption Algorithm

AES Test

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

[More information on AES](#) Benchmark

Hash Algorithm

RIPEND-160 [Information on hash algorithms](#)

Welcher Verschlüsselungsalgorithmus soll es sein?

5. Nun kommen Sie zum wichtigsten Punkt: der Wahl des Passworts. Geben Sie das Passwort zweimal ein und klicken Sie dann auf „Next“.

1. →
2. →
3.
Anleitung

Password

Password: *****

Confirm: *****

Use keyfile

Wählen Sie möglichst ein Passwort, das aus Buchstaben, Zahlen und Sonderzeichen besteht. Nur solche Passwörter sind sicher.

Ihr Passwort sollte aus mindestens 20 Zeichen bestehen.

6. Bewegen Sie jetzt innerhalb des Fensters „Collecting Random Data“ den Mauszeiger für einige Augenblicke in zufälligen Bahnen. Dabei generiert TrueCrypt eine zufällige Zeichenfolge, die für die Verschlüsselung wichtig ist. Klicken Sie danach auf „Next“. Im nächsten Fenster sehen Sie das Ergebnis. Klicken Sie erneut auf „Next“.
7. Auch die Entwickler von TrueCrypt haben an den Notfall gedacht: Es wird nun auf Ihrer Festplatte ein Abbild einer Rettungs-CD angelegt. Mit dieser können Sie auf die verschlüsselten Daten zugreifen, falls das Boot-Programm der Festplatte defekt ist. Wählen Sie einen Speicherort für das Abbild und klicken Sie auf „Next“.
8. Nun müssen Sie das Abbild auf eine CD brennen. Das muss genau an dieser Stelle geschehen, da TrueCrypt vorher nicht weiterarbeitet. Lassen Sie die CD anschließend im Laufwerk liegen und klicken Sie auf „Next“. Hat TrueCrypt die CD erkannt, klicken Sie erneut auf „Next“.
9. Nun können Sie wählen, ob Sie einen „Wipe Mode“ nutzen möchten. Dieser verhindert die Wiederherstellung gelöschter Daten. Während der Verschlüsselung verschiebt

Lassen Sie die Maus tanzen

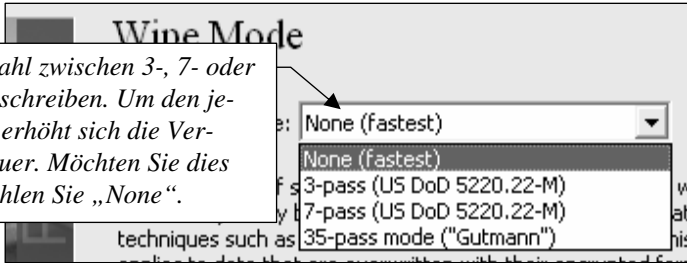
Für den Pannefall gibt's eine Notfall-CD

Brennen Sie sofort die Notfall-CD

1. →
2. →
3.
Anleitung

TrueCrypt Daten auf der Festplatte. Die ursprüngliche Speicherstelle wird dann mehrmals überschrieben. Klicken Sie anschließend auf „Next“.

Sie haben die Wahl zwischen 3-, 7- oder 35-fachem Überschreiben. Um den jeweiligen Faktor erhöht sich die Verschlüsselungsdauer. Möchten Sie dies nicht nutzen, wählen Sie „None“.



Möchten Sie den „Wipe Mode“ nutzen?

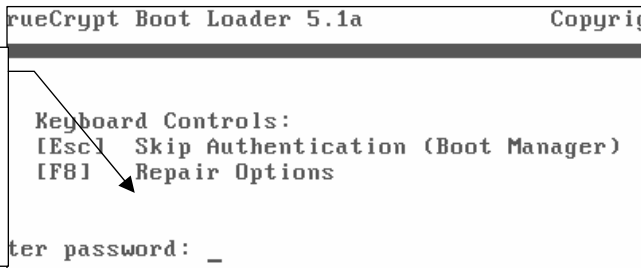
TrueCrypt überprüft, ob die Verschlüsselung möglich ist

10. Klicken Sie auf die Schaltfläche „Test“ und TrueCrypt überprüft, ob sich Ihre Festplatte problemlos verschlüsseln lässt. Dazu ist ein Neustart nötig. Vorher öffnet sich ein Hinweis-Fenster. Schließen Sie dieses mit „OK“. Erlauben Sie nun den Neustart durch einen Klick auf „Ja“.

Geben Sie das Passwort ein, um den PC zu starten

11. Nach dem Start des PCs sehen Sie das Fenster des TrueCrypt-Bootloaders. Geben Sie das Passwort ein und bestätigen Sie mit der Enter-Taste.

Hinter den „Repair Options“ verbirgt sich die Möglichkeit, die Verschlüsselung rückgängig zu machen.



Nach der erfolgreichen Verschlüsselung der Partition(en) sehen Sie diesen Bildschirm in Zukunft immer nach dem Einschalten des PCs.

12. Nach dem Windows-Start zeigt TrueCrypt an, ob der Test erfolgreich verlief. Ein Klick auf die Schaltfläche „Encrypt“ löst dann die Verschlüsselung aus. Vorher erscheint ein weiterer Hinweis. Schließen Sie diesen mit einem Klick auf „OK“ und die Verschlüsselung beginnt.

Ist der Vorgang abgeschlossen, bestätigen Sie mit „OK“. Anschließend klicken Sie auf „Finish“, um das Programmfenster von TrueCrypt zu schließen.

Vergessen Sie niemals Ihr Passwort! Ohne das Passwort kommen Sie nicht mehr an Ihre Daten heran – auch nicht mithilfe der Notfall-CD!

Nun lässt sich die Festplatte endgültig verschlüsseln

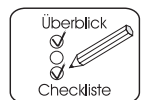


Möchten Sie Ihre Festplatte wieder entschlüsseln, klicken Sie im Programmfenster von TrueCrypt im Menü „System“ auf „Permanently Decrypt System Partition/Drive...“ und bestätigen Sie zweimal mit „Ja“.

So machen Sie die Verschlüsselung rückgängig

Im Pannenfall hilft die TrueCrypt-Notfall-CD

Die Notfall-CD sollten Sie gut aufbewahren, denn sollte es zu Defekten kommen, können Sie diese mit der CD reparieren.



Booten Sie Ihren PC mit der CD und klicken Sie auf die Taste „F8“, um die Reparaturoptionen aufzurufen.

- Taste „1“: Mit dieser Funktion können Sie die Verschlüsselung rückgängig machen.
- Taste „2“: Ein defekter Boot-Loader wird repariert. Diese Option benötigen Sie, falls der TrueCrypt-Bootloader aus irgendeinem Grund gelöscht wurde.

Diese Reparaturen ermöglicht die CD

- Taste „3“: Sollte der Boot-Loader melden, dass Sie ein falsches Passwort eingegeben haben, obwohl Sie es mehrmals korrekt eingegeben haben, weist dies auf einen Defekt des für die Verschlüsselung verwendeten Schlüssels (das ist nicht das Passwort) hin. Mit der Option „Restore key data“ sollte sich dies reparieren lassen.

Nach Nutzung dieser Option ist eine neue Notfall-CD nötig

Sollten Sie jemals diese Option nutzen, müssten Sie anschließend eine neue Notfall-CD anlegen. Denn diese Option lässt sich nur einmal verwenden. Um eine neue Notfall-CD anzulegen, klicken Sie im Programmfenster von TrueCrypt im Menü „System“ auf den Eintrag „Create Rescue Disk“.

- Taste „4“: Schreibt den originalen Boot-Loader wieder auf Ihre Festplatte. Dies könnte nötig sein, wenn Sie die Verschlüsselung rückgängig gemacht haben und Windows anschließend nicht startet. Diese Option dürfen Sie nur bei nicht verschlüsselten Laufwerken nutzen.

```

TrueCrypt Boot Loader 5.1a                                Copyright
-----
Available Repair Options:
[1]   Permanently decrypt system partition/drive
[2]   Restore TrueCrypt Boot Loader
[3]   Restore key data (volume header)
[4]   Restore original system loader
[Esc] Cancel
To select, press 1-9: _

```

Diese vier Reparaturoptionen bietet die TrueCrypt-CD.



So erzeugen Sie primäre Partitionen

Wie erwähnt kann TrueCrypt nur primäre Partitionen verschlüsseln. Andere Partitionen müssten vor der Verschlüsselung umgewandelt werden.

Zuerst müssen Sie dazu herausfinden, welche Partitionen sich auf Ihrer Festplatte befinden. Dazu gehen Sie so vor:

1. Doppelklicken Sie innerhalb der Systemsteuerung auf das Symbol „Verwaltung“. Im nächsten Fenster doppelklicken Sie auf „Computerverwaltung“.
2. Im Fenster „Computerverwaltung“ klicken Sie in der Spalte am linken Rand auf „Datenträgerverwaltung“.

Überprüfen Sie die Partitionierung in der Datenträgerverwaltung



Die Festplatte besitzt eine Kapazität von 5 GB. Es ist eine primäre Partition („C:“) eingerichtet und ein logisches Laufwerk („E:“) innerhalb einer erweiterten Partition.

Eine Umwandlung einer Partition in eine primäre Partition ist nicht ohne Weiteres möglich. Sie müssten eine solche Partition erst löschen und dann eine neue Partition anlegen. So gehen Sie vor:

Eine primäre Partition wird so eingerichtet

Auch hier noch einmal der Hinweis: Sichern Sie vorher Ihre Daten. Es wird hier eine Partition gelöscht. Alle Daten dieser Partition sind verloren, wenn Sie diese nicht sichern.



1. Klicken Sie mit der rechten Maustaste auf das logische Laufwerk der erweiterten Partition. Wählen Sie aus dem Kontextmenü den Eintrag „Logisches Laufwerk löschen“. Die Sicherheitsabfrage beantworten Sie mit „Ja“. Sollten innerhalb einer erweiterten Partition mehrere logische Laufwerke eingerichtet sein, müssen Sie alle löschen.

Löschen Sie das logische Laufwerk ...

... und dann die erweiterte Partition

2. Nun klicken Sie auf den freien Speicherplatz der erweiterten Partition und wählen im Kontextmenü den Eintrag „Partition löschen“. Auch das bestätigen Sie mit „Ja“.
3. Nun klicken Sie mit der rechten Maustaste auf den nicht zugeordneten Speicherplatz. Diesmal klicken Sie im Kontextmenü auf den Eintrag „Neue Partition“ und es öffnet sich ein Assistent zum Erstellen einer Partition.

Ein Assistent hilft Ihnen

4. Im ersten Fenster des Assistenten klicken Sie auf „Weiter“. Im zweiten Fenster wählen Sie die Option „Primäre Partition“. Sie können jetzt alle Fenster bis zum Ende des Assistenten durchklicken, da Sie keine weiteren Einstellungen vornehmen müssen. Im letzten Fenster klicken Sie auf „Fertig stellen“ und die primäre Partition wird erstellt.



Alternative: Festplatten mit integrierter Verschlüsselung

Wer nicht auf eine Software-Verschlüsselung setzen will, findet immer mehr Festplatten auf dem Markt, die eine integrierte Verschlüsselung besitzen.

Seagate und Fujitsu-Siemens haben bereits entsprechende Modelle im Angebot

So veröffentlicht Maxtor im ersten Halbjahr 2008 unter der Bezeichnung „BlackArmor“ externe USB-Festplatten mit integrierter Verschlüsselung.

Seagate und Fujitsu-Siemens haben entsprechende 2,5-Zoll-Notebook-Festplatten im Angebot. Seagate hält verschlüsselte Festplatten mit Kapazitäten von 80 bis 160 GB in der Serie „Momentus 5400 FDE.2“ bereit. Bei Fujitsu-Siemens trägt die Festplattenserie die Bezeichnung „MHZ2 CJ“ und kommt mit Speicherkapazitäten von 80 bis 320 Gigabyte daher.