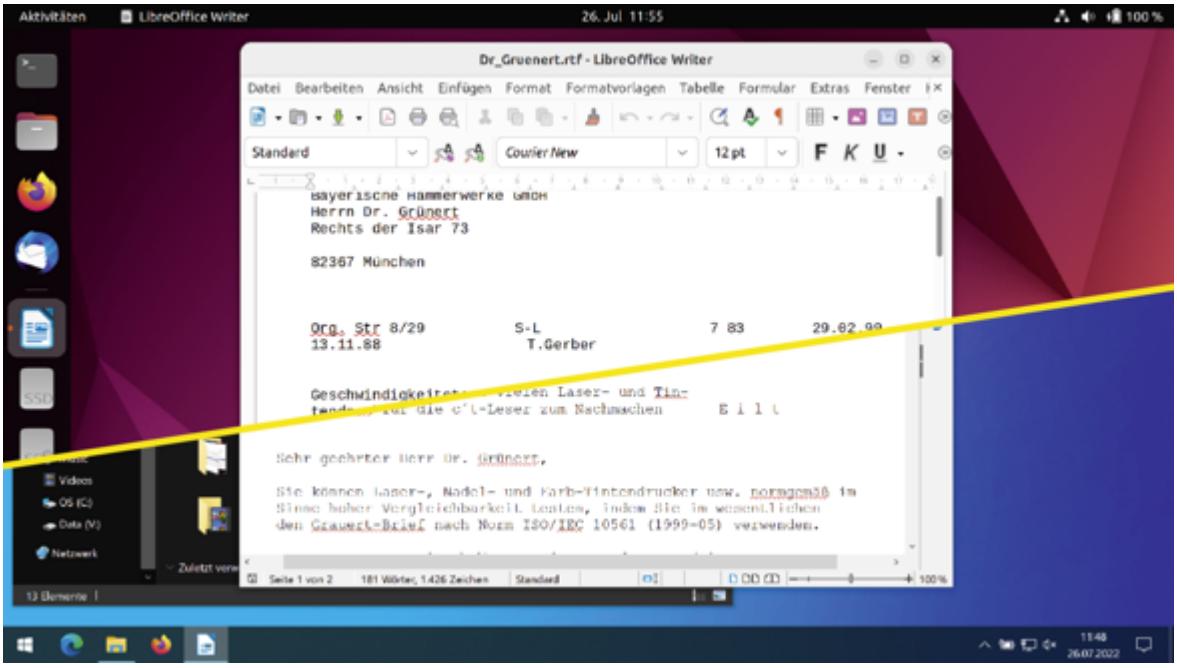
Windows und Linux zusammen

Und los!

Die Anleitungen in dieser Ausgabe helfen Ihnen durch die Einrichtung beider Betriebssysteme. Los geht es auf Seite 16, wo wir beschreiben, wie Sie Windows so schrumpfen, dass Linux sich zusätzlich installieren lässt. Der Beitrag ab Seite 22 beschreibt, wie Sie Linux verschlüsselt auf dem gleichen Datenträger installieren.

Abschließend geht es um das Entscheidende: Ihre Daten. Die lagern Sie, sofern das nicht eh schon der Fall ist, künftig getrennt vom Betriebssystem. Würden Sie die Daten auf dem Windows-Laufwerk belassen, müssten Sie später von Linux aus darauf zugreifen. Das ist eine genauso schlechte Idee wie Windows auf Linux zugreifen zu lassen. Es bestünde in beiden Fällen die Gefahr, dass ein System das andere demoliert, was Folgen bis hin zum Datenverlust haben könnte. Die Trennung vermeidet das. Zudem ist sie die Voraussetzung dafür, dass Ihre Daten ebenfalls verschlüsselt, aber für beide Betriebssysteme erreichbar sind.

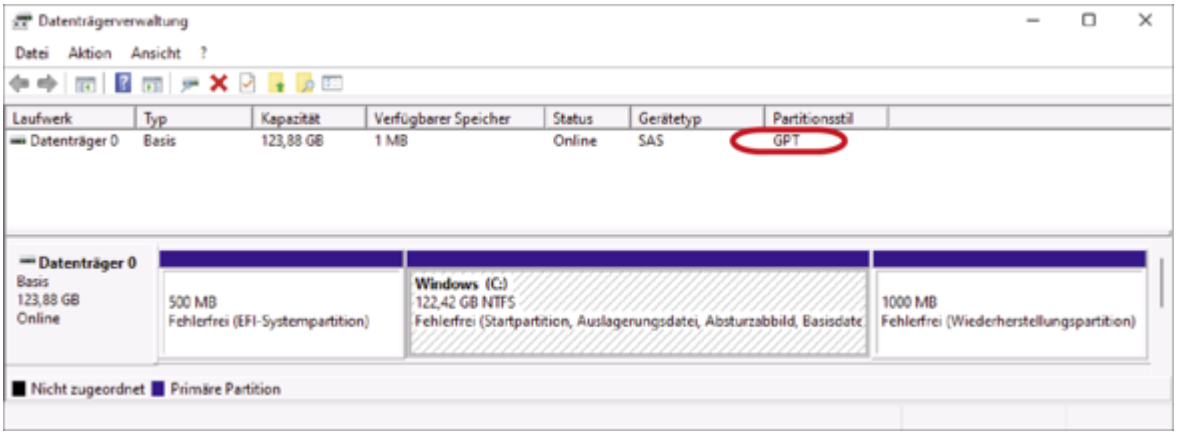
Haben Sie erst mal alle Anleitungen durchgespielt, reduziert sich die seit Jahrzehnten andauernde Diskussion um das bessere Betriebssystem für Sie auf die simple Frage, welches Betriebssystem Sie beim Einschalten des Computers starten. Und die völlig undogmatische Antwort lautet: jenes, das in diesem Moment das geeignetere ist. (*axv@ct.de*)



Windows und Linux laufen auf demselben PC und mit beiden Systemen können Sie Ihre verschlüsselten Dateien bearbeiten, ohne erst etwas hin und her zu kopieren.

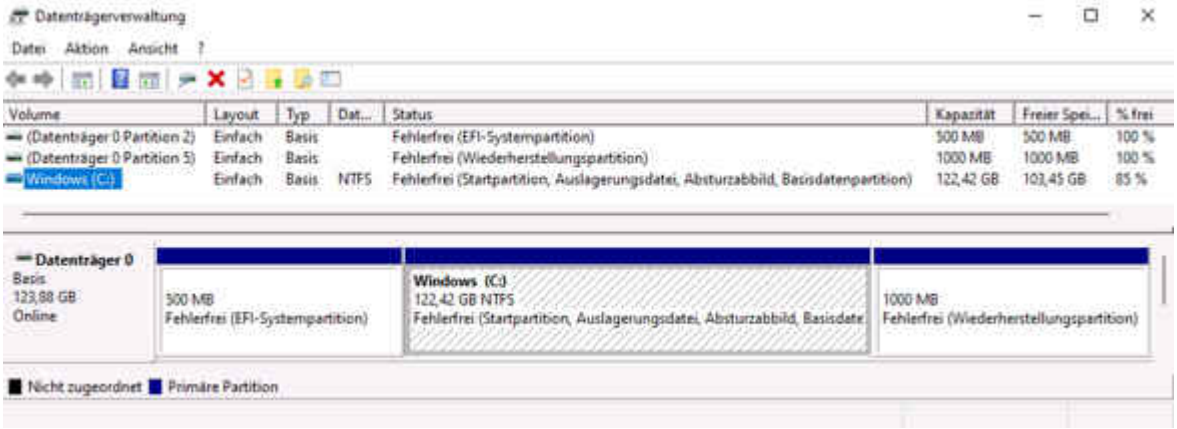
Vorbereiten

Der erste Handgriff ist derselbe wie vor vielen anderen Operationen am offenen Windows: Fertigen Sie ein Backup an. Unser Sicherungsskript c’t-WIMage [1] erstellt auf einem USB-Laufwerk eine Kopie Ihrer kompletten Windows-Installation, die Sie auf quasi jeder Windows-kompatiblen Hardware wiederherstellen können. Wichtig wie bei jedem anderen Backup auch: Testen Sie nach dem Sichern, ob es wirklich geklappt hat. Alle nötigen Anleitungen und das Skript selbst finden Sie via ct.de/wimage.



Wenn Sie in der Datenträgerverwaltung unter Ansicht die

„Anzeige oben“ auf „Datenträgerliste“ umstellen, steht in der Spalte Partitionsstil bei heutigen Computern meist „GPT“. Falls das bei Ihnen anders ist, kommt zusätzliche Arbeit auf Sie zu.



So sieht die Aufteilung eines internen Datenträgers bei einer Windows-Standardinstallation aus: Vorn die EFI-Partition mit dem Bootloader, in der Mitte die eigentliche Windows-Installation und am Ende das Rettungssystem „Windows RE“.
Der zweite Handgriff ist optional: Schaffen Sie Platz auf C:, denn je mehr Platz dort frei ist, umso mehr können Sie von C: abknapsen. Am einfachsten gelingt das mit der Windows-eigenen Datenträgerbereinigung. Die löscht temporäre Dateien, Update-Überreste und vieles mehr. Starten können Sie sie beispielsweise, indem Sie im Eigenschaften-Dialog von C: die Schaltfläche „Bereinigen“ anklicken. Klicken Sie anschließend auf „Systemdateien bereinigen“. Dann wählen Sie kurzerhand alle Kästchen aus und lassen das Werkzeug seine Arbeit verrichten.

Noch nicht genug Platz frei? Öffnen Sie im Explorer Laufwerk C: und tippen Sie oben rechts in das Suchfeld Größe:>50M ein. Daraufhin sucht Windows alle Dateien auf C:, die größer sind als 50 MByte. Den Wert können Sie nach Belieben anpassen. Achtung: Löschen Sie von den gefundenen Dateien auf gar(!) keinen(!) Fall(!) solche, von denen Sie keine Ahnung haben, wozu sie gut sind. Denn sonst kann es passieren, dass Windows oder einzelne Anwendungen nicht mehr korrekt laufen. Entsorgen Sie also stattdessen ausschließlich, was Ihnen bekannt ist, etwa heruntergeladene Installationspakete, nicht mehr benötigte ISO-Abbilder, bereits gesehene Filme und so weiter.

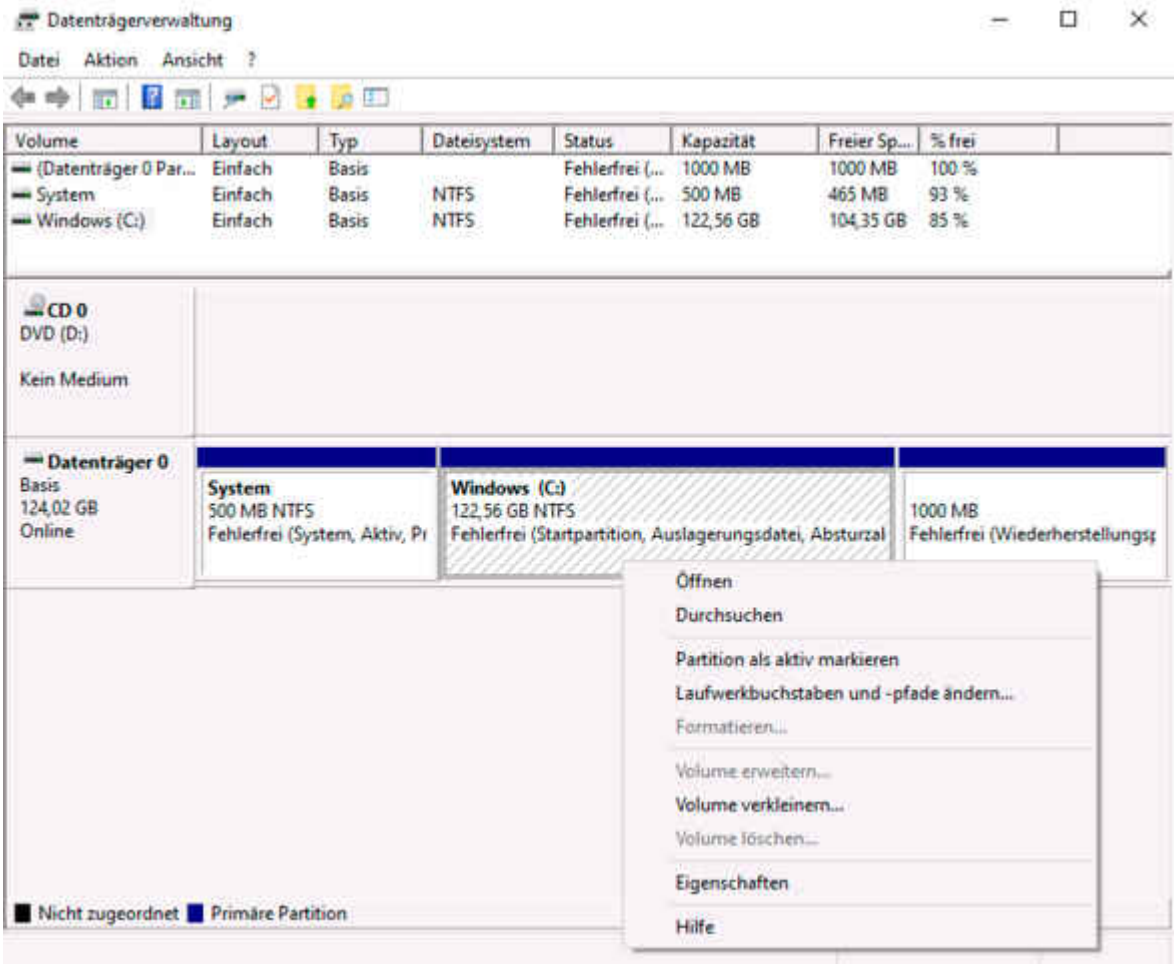
Falls der Platz immer noch nicht ausreicht: Das Titelthema von c’t 8/2018 bietet gleich fünf Artikel mit vielen weiteren Tipps [2].

Noch ein letzter Handgriff, bevor es wirklich losgeht: Ziehen Sie alle externen Datenträger wie USB-Platten ab, um nachfolgend die Übersichtlichkeit möglichst hoch zu halten und Verwechslungen zu vermeiden. CDs und DVDs werfen sie aus. Das gilt auch für virtuell eingebundene Festplattendateien im VHD- und VHDX-Format.

Sofern C: mit BitLocker verschlüsselt ist [3], macht das nichts. Alle nachfolgend genannten Handgriffe funktionieren auch dann. Sie brauchen dafür an BitLocker also nicht herumzukonfigurieren.

Wie siehts hier denn aus?

Verschaffen Sie sich zuerst einen Überblick über die Partitionierung. Das gelingt am schnellsten mit der Windows-eigenen Datenträgerverwaltung, die unter Windows 10 und 11 gleichermaßen funktioniert (eine ausführliche Einführung haben wir in [4] veröffentlicht). Zum Starten drücken Sie die Tastenkombination Windows+X und wählen Sie den Eintrag „Datenträgerverwaltung“.



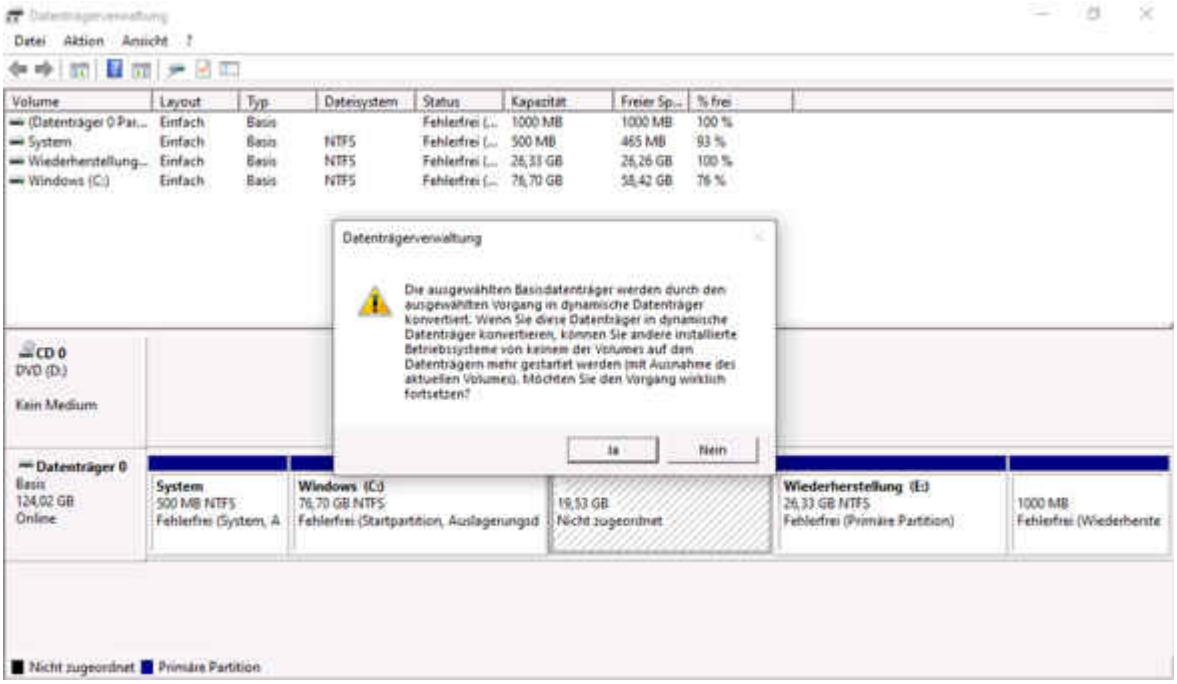
Die Datenträgerverwaltung bringt einen Assistenten zum Verkleinern der Windows-Partition mit. Der Haken ist die RE-Partition, die hier am Ende des Datenträgers liegt.
Das Programm präsentiert oben eine detaillierte Liste mit den vorhandenen Partitionen inklusive Füllstand, Art des Dateisystems, Status, ob es BitLocker-verschlüsselt ist und so weiter. Klicken Sie in der Menüleiste unter „Ansicht/Anzeige oben“ auf „Datenträgerliste.“ In der Spalte „Partitionsstil“ steht entweder „GPT“ oder „MBR“. Die Abkürzungen stehen für die zwei Partitionsschemata, mit denen sich die Partitionen auf einem Laufwerk verwalten lassen.

GPT ist das modernere Schema und gilt seit Jahren als Standard. Die Wahrscheinlichkeit ist daher hoch, dass Ihr Datenträger GPT-partitioniert ist, und wenn dem so ist, steht dem Platzfreischaufeln nichts im Wege. Sie können dann im Abschnitt „Schrumpfkur“ weiterlesen.

Das MBR-Problem

Bei Ihnen steht „MBR“? Das ist unschön, denn MBR (veröffentlicht 1983) leidet an altersbedingten Einschränkungen. Die hier wichtigste: Es verzeichnet die Partitionen in einer Partitionstabelle, die für maximal vier Einträge Platz bietet (die „Primärpartitionen“). Weitere primäre Partitionen können Sie mit MBR nicht anlegen. Um Ihnen eigene zeitraubende Versuche zu ersparen, zuerst zu dem, was hier nicht hilft.

Das MBR-Partitionsschema kennt als Krücke die „erweiterte Partition“. Mit deren Hilfe lassen sich weitere Partitionstabellen mit der ersten verketten, die jeweils Platz für maximal vier weitere logische Partitionen bieten. Das ist aber nicht empfehlenswert, allein schon, weil die erweiterte Partition einen der vier Plätze in der Tabelle benötigt. Sind derzeit alle belegt, müssten Sie also zuerst eine der vorhandenen Partitionen löschen und dazu vorab die Daten von dieser Partition wegsichern. Zudem können Sie nicht frei wählen, welche primäre Partition Sie durch eine erweiterte ersetzen wollen. Denn beispielsweise der Bootloader muss zwingend in einer primären liegen. Kurzum: Lassen Sie das. (Für die Hartgesottenen unter Ihnen, die dennoch wissen wollen, wie sie eine erweitere Partition anlegen: Das geht unter Windows nur mit Diskpart per Create Partition Extended.)



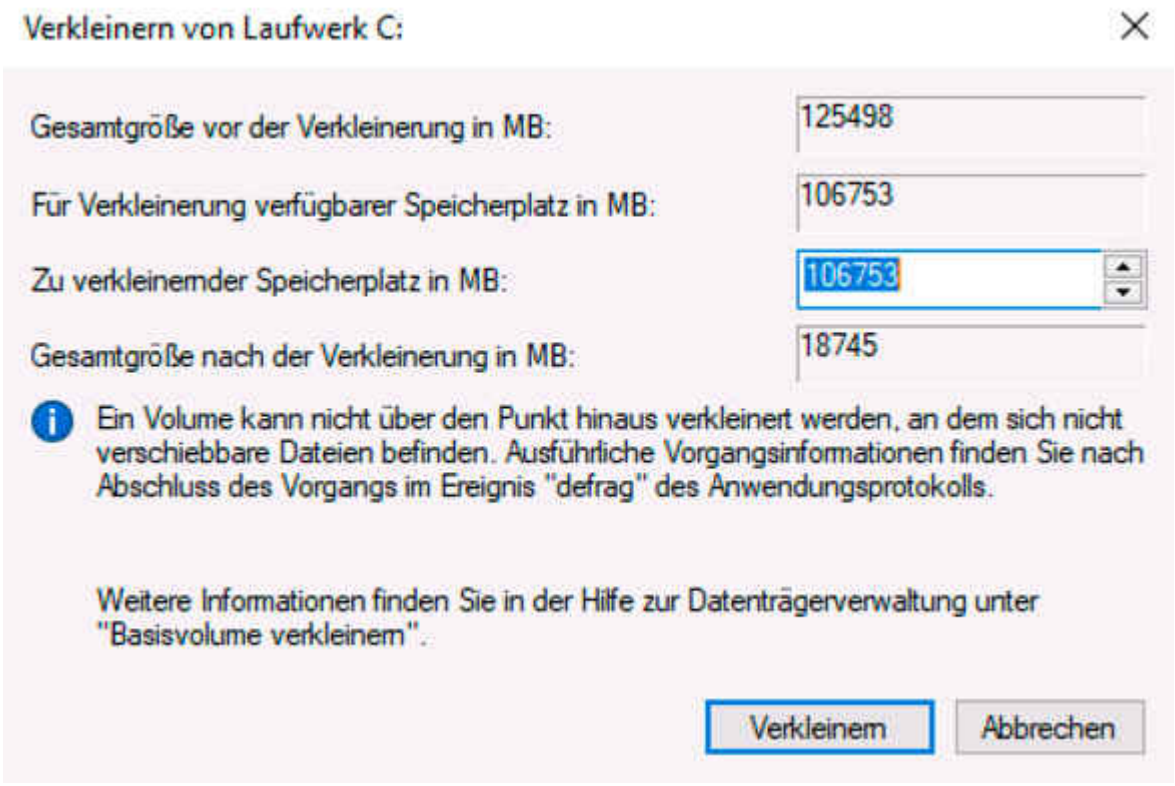
Wenn auf dem Datenträger das alte Partitionsschema MBR verwendet wird, kann das Erstellen einer weiteren Partition scheitern. Die Datenträgerverwaltung hilft dann nicht weiter.
Die Datenträgerverwaltung möchte Ihnen eine andere Krücke andrehen. Wenn Sie probieren, auf einem MBR-Datenträger eine fünfte primäre Partition zu erstellen, will sie den Datenträger in einen „dynamischen“ umwandeln. Dahinter steckt im Wesentlichen eine Microsoft-eigene RAID-Lösung. Hilft nur nichts: Selbst wenn Sie auf „Ja“ klicken, wird der Datenträger trotzdem nicht umgewandelt. Stattdessen beschwert sich Windows mit einer Fehlermeldung über Platzmangel. Es fehlt ja unverändert Platz für einen weiteren Eintrag in der Partitionstabelle.

Zum Glück gibt es eine Lösung, die wirklich funktioniert: Ersetzen Sie das MBR-Partitionsschema durch GPT, denn damit sind mindestens 128 Partitionen verwaltbar. Der Haken: Mit dem Umstellen von MBR auf GPT allein ist es nicht getan. Der PC muss anschließend auch UEFI- statt Legacy-BIOS-Mechanismen zum Hochfahren nutzen, sonst bootet Windows nicht mehr. Zwei Methoden zum Umstellen haben wir in c’t bereits vorgestellt, was aber jeweils einen ganzen Artikel füllte. Die erste: Windows hat das Kommandozeilenwerkzeug „MBR2GPT.exe“ an Bord, mit dem das Vorhaben gelingt – jedenfalls dann, wenn diverse

Voraussetzungen erfüllt sind und Sie einige Bugs umschiffen [5]. Die zweite: Verwenden Sie unser bereits erwähntes Sicherungsskript c't-WIMage. Dann springt im Rahmen der Umstellung auch gleich noch eine Sicherungskopie Ihrer Windows-Installation für Sie heraus. Wie die Umstellung mit c't-WIMage gelingt, steht ausführlich in [6].

Schrumpfkur

Nun zum Verkleinern der Windows-Partition. Das erledigen Sie in der Datenträgerverwaltung. Wählen Sie in der unteren Fensterhälfte „Volume Verkleinern …" aus dem Kontextmenü der Windows-Partition. Falls Sie sich wundern, warum Windows scheinbar identische Bereiche des physischen Datenträgers mal als „Partition" und mal als „Volume" bezeichnet: Eine Partition belegt einen ganzen oder nur einen Teil eines physischen Datenträgers, kann sich aber nicht über mehrere erstrecken. Eine Partition enthält wiederum ein Volume, wobei es sich um das eigentliche logische Laufwerk handelt. In den meisten Fällen füllt ein Volume eine komplette Partition. Doch es kann sich auch über mehrere Partitionen erstrecken, die sogar wie bei einem RAID oder Storage Space auf unterschiedlichen Datenträgern liegen dürfen.



Der Assistent zum Verkleinern will nicht die Zielgröße wissen, sondern um wie viele MBytes die Partition verkleinert werden soll.
Nach dem Anklicken von „Volume verkleinern“ startet ein Assistent, der mehrere Werte anzeigt, von denen Sie einen verändern können: „Zu verkleinernder Speicherplatz in MB“. Sie wählen also nicht die Zielgröße des Laufwerks, sondern die Anzahl an MByte, die am hinteren Ende abgeschnitten werden. Der Assistent bietet den Maximalwert an, der vom Füllstand abhängt (die zu Windows-7-Zeiten geltende Beschränkung auf maximal die Hälfte spielt heute keine Rolle mehr).

Wie weit Sie das Windows-Volume verkleinern, hängt von zweierlei ab: Erstens muss Windows hinterher noch drauf passen. Wie viel Platz die Installation belegt, können Sie im Explorer in den Eigenschaften von C: ablesen. Doch dieser Platz allein reicht nicht: Windows braucht zusätzlich im laufenden Betrieb freien Platz beispielsweise für temporäre Dateien und Updates, und das gilt auch für viele Anwendungen. Als Minimum dafür gelten 20 GByte, ziehen Sie also im Assistenten vom vorgegebenen Maximalwert mindestens 20.000 MByte ab. Wenn möglich ist, reduzieren Sie den Wert weiter.

Mehr als 100 GByte freier Platz auf der Windows-Partition ist aber unnötig. Grübeln Sie über den Wert lieber eine Minute länger als zu kurz, denn nachträgliche Änderungen sind zwar machbar, aber nur mit viel Aufwand.

Sie haben einen zufriedenstellenden Wert eingetragen? Ein Klick auf „Verkleinern“ lässt den Assistenten die Schrumpfkur erledigen. In der Datenträgerverwaltung erscheint nun hinter der verkleinerten Windows-Partition ein Bereich „Nicht zugeordnet“ mit einem schwarzen Balken darüber .

Das RE-Problem

An sich können Sie den gerade freigeschaufelten Platz seiner neuen Bestimmung zuführen. Doch lesen Sie stattdessen besser erst noch diesen Abschnitt. Denn außer der Windows-Partition gibt es noch eine weitere, die Ihrer Aufmerksamkeit bedarf. Sie enthält die Wiederherstellungsumgebung „Windows RE“ (Recovery Environment, [7]), von der Sie üblicherweise nur dann etwas bemerken, wenn Windows Probleme beim Booten hat. Bei RE handelt es sich um ein eigenständiges kleines Betriebssystem, welches der Bootloader bei Problemen automatisch startet. Es liegt in einer separaten Partition, die hier nachfolgend RE-Partition heißt.

Wie Windows selbst entwickelt Microsoft auch Windows RE immer weiter, und wie Windows wird auch RE immer größer. Als Folge wächst auch die separate RE-Partition – wenn nicht jetzt, dann irgendwann in der Zukunft, und zwar jeweils im Rahmen eines Versions-Upgrades. Die finden derzeit ungefähr jährlich statt. Wenn es so weit ist, passt Windows die Partitionierung im laufenden Betrieb an. Was dabei herauskommt, hängt von diversen Faktoren ab, die zu erläutern hier zu weit führt (Details in [8]). Scheitert Windows beim Anpassen, startet RE schlimmstenfalls nach einem Versionssprung gar nicht mehr oder nur dann, wenn C: nicht mit BitLocker verschlüsselt ist. Auch Defekte des Bootmenüs des Bootloaders sind denkbar, vor allem bei der Installation eines weiteren Betriebssystems, dessen

Entwickler RE und seine Besonderheiten nicht berücksichtigen. Es können zudem zusätzliche Partitionen entstehen, die Platz verschwenden.

Damit Windows beim Vergrößern der RE-Partition nicht scheitert, muss die RE-Partition direkt hinter der Windows-Partition liegen. Dann kann Windows bei Bedarf die RE-Partition löschen, die Windows-Partition etwas verkleinern und in dem so entstandenen freien Platz hinter der Windows-Partition eine neue, nun eben etwas größere RE-Partition anlegen. Die liegt dann wieder direkt hinter der Windows-Partition.

RE verschieben

Zuerst in Kurzform, was zu tun ist, um Probleme mit der RE-Partition zu vermeiden: Deaktivieren Sie RE, woraufhin das komplette Mini-Betriebssystem vorübergehend von der RE- auf die Windows-Partition verschoben wird (es besteht ohnehin nur aus einer einzigen Datei, die beim Start von RE vorübergehend ins RAM entpackt wird). Erstellen Sie hinter der bereits geschrumpften Windows- eine neue RE-Partition und löschen Sie die alte. Zum Abschluss reaktivieren Sie RE, woraufhin es funktionstüchtig an seinem neuen Speicherplatz landet.

Nun zur Langform. Das Prozedere erfordert nicht nur Mausklicks, sondern auch einzutippende Kommandozeilenbefehle. Über ct.de/yxb1 finden Sie eine kleine Textdatei, aus der Sie alle Befehle herauskopieren können. Das Nachfolgende geht davon aus, dass Sie die Windows-Partition bereits wie oben beschrieben geschrumpft haben. Falls nicht, holen Sie das zuerst nach.

Los geht es in der Datenträgerverwaltung: Sehen Sie nach, auf welchem Datenträger die Windows-Partition liegt. Das erkennen Sie ganz links an der Bezeichnung „Datenträger X“, wobei X für eine Zahl steht, beginnend bei 0. Merken Sie sich die Zahl, die hinter „Datenträger“ steht.

Drücken Sie Windows+X. Wählen Sie aus dem Systemmenü je nachdem, was da ist: „Eingabeaufforderung (Administrator)“, „PowerShell (Administrator)“ oder „Terminal (Administrator)“. Tippen Sie darin den Befehl ein:

```
Reagentc /disable
```

Der Befehl deaktiviert RE. Sollte es dabei zu Fehlermeldungen kommen, liegt das üblicherweise nicht an der RE-Partition, sondern an Windows RE selbst. Hilfe und viele Tipps zum Beheben solcher Probleme finden Sie dann in [9].

Starten Sie den Kommandozeilenpartitionierer Diskpart (Einführung in [10]):

```
Diskpart
```

Wählen Sie den Datenträger mit der Windows-Partition, die Zahl ersetzen Sie durch die, die Sie in der Datenträgerverwaltung abgelesen haben:

```
Select Disk 0
```

Die nächsten beiden Befehle erzeugen eine rund 1 GByte große Partition mit dem Dateisystem NTFS und der eindeutigen Bezeichnung „ctRecovery“:

```
Create Partition Primary Size=1000
Format Quick FS=NTFS Label="ctRecovery"
```

Die Bezeichnung können Sie frei wählen, wichtig ist nur, dass sie eindeutig ist. Das hilft später beim Identifizieren und Löschen der alten RE-Partition.

Damit Windows die neue Partition als RE-Partition erkennt, passen die folgenden zwei Befehle den Partitionstyp an (hier für GPT):

```
Set ID=de94bba4-06d1-4d40-a16a-bfd50179d6ac
GPT Attributes=0x8000000000000001
```

Sollte der Datenträger entgegen unserer Empfehlung noch MBR-

partitioniert sein, reicht stattdessen ein einzelner Befehl: Set ID=27.

Alte RE-Partition löschen

Nun können Sie die alte RE-Partition löschen. Dazu benötigen Sie ebenfalls Diskpart. Verschaffen Sie sich zuerst einen Überblick über die vorhandenen Partitionen:

```
List Partition
```

Suchen Sie in der Liste nach Partitionen mit Namen wie „Wiederherstellung“ oder „Recovery“. Bei einer solchen kann es sich um die alte RE-Partition handeln, muss aber nicht. Auf PCs mit vom Hersteller vorkonfigurierten Windows sind oft weitere Partitionen mit ähnlichen oder gar identischen Namen vorhanden. Die enthalten beispielsweise herstellereigene Wiederherstellungswerkzeuge, die vom Windows-eigenen RE unabhängig funktionieren, oder Installationspakete der mitgelieferten Anwendungen und Treiber für den Fall, dass der Kunde selbst Windows neu installieren will. Images zum Wiederherstellen des Auslieferungszustands legten PC-Hersteller früher ebenfalls gern in separaten Partitionen ab, gesehen haben wir sowas aber schon länger nicht mehr.

Die alte RE-Partition erkennen Sie am Namen, am Dateisystem NTFS und an der Größe von rund 1 bis 2 GByte oder kleiner – Wiederherstellungspartitionen der PC-Hersteller sind um ein Vielfaches größer.

Der Befehl List Partition listet für jede Partition eine Nummer auf (ab 1 hochzählend). Suchen Sie die für die alte RE-Partition. Folgende Befehle wählen sie aus und zeigen deren Details an (X an die Partitionsnummer anpassen):

```
Select Partition X
Detail Partition
```

Steht nach dem Abschicken des zweiten Befehls in der Ausgabe eine Zeile namens Typ: de94bba4-06d1-4d40-a16a-bfd50179d6ac

und weiter unten eine andere (!) Bezeichnung als die oben von Ihnen vergebene „ctRecovery“, haben Sie die richtige Partition erwischt. Diese kryptische Typ-ID ist auf GPT-Datenträgern RE-Partitionen vorbehalten (bei MBR-Datenträgern steht hier stattdessen Typ: 27).

Sie löschen die alte RE-Partition mit diesem Befehl (X an die Partitionsnummer anpassen):

Delete Partition Override

Lag die alte Partition bislang vor Windows, entsteht dort freier, aber nicht nutzbarer Platz, woran sich mit Windows-Bordmitteln leider nichts ändern lässt. Nun beenden Sie Diskpart durch Eingabe von Exit und reaktivieren Windows RE durch Eingabe von Reagentc /enable. Ob das geklappt hat, offenbart Reagentc /info, bei Problemen sei erneut auf [8] verwiesen.

(Fast) fertig

Das Wesentliche ist geschafft: Die Windows-Partition ist geschrumpft und die RE-Partition liegt trotzdem wieder direkt dahinter. Die nächsten Handgriffe hängen von Ihrem Vorhaben ab.

Soll der freie Platz lediglich zur Aufnahme einer separaten Datenpartition dienen, öffnen Sie ein weiteres Mal die Datenträgerverwaltung. In der unteren Fensterhälfte finden Sie im Kontextmenü des leeren, mit einem schwarzen Balken markierten Rechtecks den Eintrag „Neues einfaches Volume …“. Ein Klick darauf startet einen weiteren Assistenten, in dem Sie nacheinander die Größe, den künftigen Laufwerksbuchstaben und die „Volumebezeichnung“ festlegen können. Alles andere wie das Dateisystem (NTFS) ist sinnvoll vorbelegt, für Änderungen sollten Sie einen guten Grund kennen (Neugier ist keiner). Wenn der Assistent fertig ist, ist das neue logische Laufwerk bereit.

Anders sieht es aus, wenn Sie zusätzlich Linux installieren und Ihre Daten zudem verschlüsseln wollen. Dann geht es nun weiter für Sie mit den nachfolgenden Artikeln. *(axv@ct.de)*

1. Literatur
2. Axel Vahldiek, Ersatzrad, c’t-WIMage erstellt Windows-Backups, c’t 10/2021, S. 18
3. Axel Vahldiek, Windows entschlacken, Titelthema von c’t 8/2018, S. 66
4. Jan Schüßler, FAQ: BitLocker, c’t 17/2018, S. 173, auch kostenlos online lesbar unter ct.de/-4122147
5. Axel Vahldiek, Plattenteiler, Partitionieren mit Windows-Bordmitteln – Teil 1: Datenträgerverwaltung, c’t 2/2018, S. 154
6. Axel Vahldiek, Anders hochfahren, Windows 10 von klassischem Start auf UEFI-Boot umstellen, c’t 14/2019, S. 162
7. Axel Vahldiek, Starker Helfer, PC-Umzug mit c’t-WIMage, c’t 6/2019, S. 22
8. Axel Vahldiek, Aufstehhelfer, Wie Windows Startprobleme selber löst, c’t 5/2018, S. 74
9. Axel Vahldiek, Wo ist sie, und wenn ja, wie oft?, Windows RE und die Recovery-Partition, c’t 18/2021, S. 162
10. Axel Vahldiek, Hilfe für den Helfer, Windows RE prüfen und reparieren, c’t 5/2018, S. 80
11. Axel Vahldiek, Tipp-Schnippler, Partitionieren mit Windows-Bordmitteln – Teil 2: Diskpart, c’t 3/2018, S. 144

Befehle.txt: ct.de/yxb1

Mitbewohner

Debian und Ubuntu verschlüsselt neben Windows installieren

Ein voll verschlüsseltes Dateisystem schützt Ihre sensiblen Daten auf Notebook und Desktop selbst bei einem Diebstahl des Computers. Bei der Linux-Installation gelingt das aber nur, wenn sich Linux auf der ganzen Festplatte breitmachen darf. Wir verraten Ihnen die nötigen Kniffe, mit denen sich Debian und Ubuntu harmonisch neben Windows einfügen und trotzdem ihre Dateisysteme verschlüsseln.

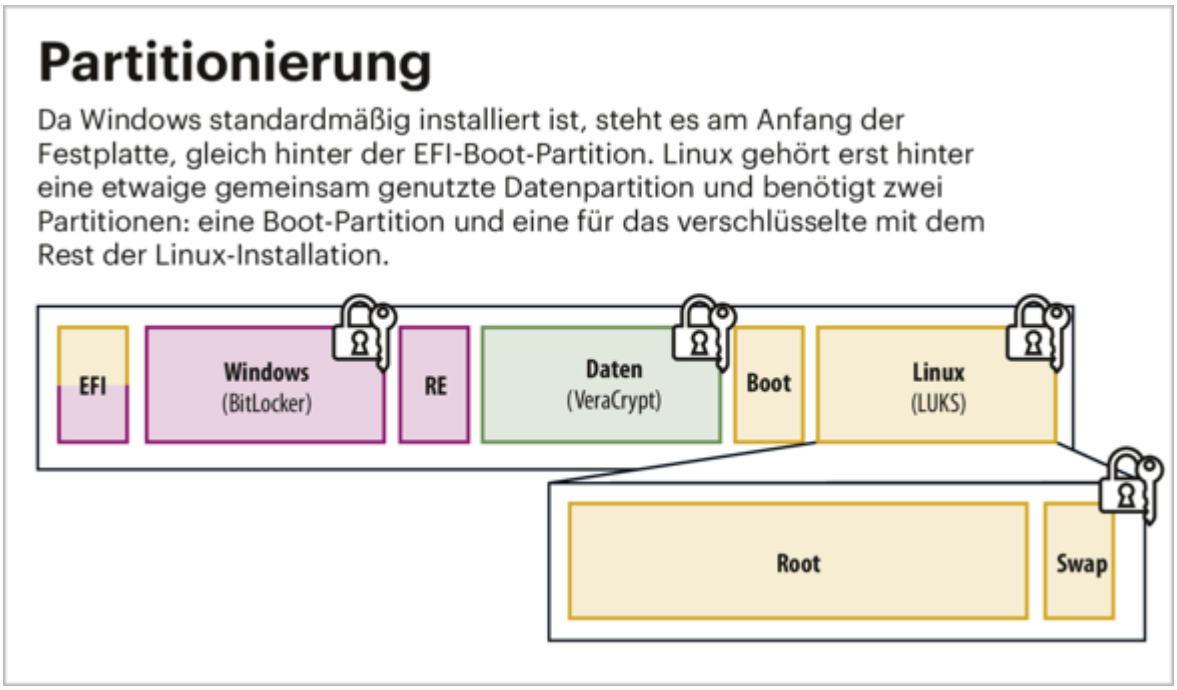
Von Mirko Dölle

Verschlüsselte Betriebssysteminstallationen gehören heute zum guten Ton, so gelangen selbst bei Diebstahl des Computers keine Daten in die falschen Hände. Viele Linux-Distributionen bieten seit Langem voll verschlüsselte Installationen an, jedoch nur dann, wenn sie die gesamte Festplatte für sich beanspruchen dürfen – so auch bei den Installationsprogrammen von Debian 11 und Ubuntu 22.04. Haben Sie Windows parallel installiert, müssen Sie entweder auf die Verschlüsselung verzichten oder sich der nachfolgend beschriebenen Tricks bedienen.

Während es beim eher spartanischen Debian genügt, sich im Installer ein paar Mal im Kreis zu drehen, müssen Sie sich beim ansonsten komfortableren Ubuntu auf der Kommandozeile abmühen, damit sich Linux geschmeidig neben Windows einfügt und trotzdem die Partitionen als LUKS (Linux Unified Key Setup) verschlüsselt. Da Windows auf praktisch allen Rechnern vorinstalliert ist, beginnen Sie damit, Ihre Windows-Installation zu verkleinern und so Platz für Linux zu schaffen. Dazu sollten Sie unbedingt die auf Seite 16 beschriebene Methode mit Windows-Bordmitteln verwenden und

nicht etwa das Partitionierungsprogramm Gparted unter Linux – denn bei Letzterem würden Sie einen Keil zwischen Windows und das Recovery-System treiben.

Damit ergibt sich die rechts oben gezeigte Aufteilung der Festplatte respektive SSD: Am Anfang steht die EFI-Boot-Partition, die Windows und Linux gemeinsam nutzen, dahinter Windows und RE. Wollen Sie später auf Ihre Daten sowohl von Linux und Windows aus zugreifen, wie dies auf Seite 28 beschrieben ist, folgt hinter den beiden Windows-Partitionen die Datenpartition. Dahinter schaffen Sie dann freien, nicht zugeordneten Platz für Linux. Wie viel Platz Sie für Linux benötigen, hängt sehr von der späteren Nutzung ab. Weniger als 50 GByte sollten es nicht sein, auch dann nicht, wenn Sie wie auf Seite 28 beschrieben eine gemeinsame Datenpartition für den Großteil Ihrer Dateien benutzen. Wollen Sie später Spiele installieren, müssen Sie das in jedem Fall einkalkulieren – manche benötigen 100 GByte und mehr für die Installation.



Der Knackpunkt bei der Partitionierung besteht darin, dass Debian und Ubuntu eine verschlüsselte LVM-Gruppe (Logical Volume Management) benutzen, um alle für den Betrieb benötigten (logischen) Laufwerke anzulegen. Dazu gehören mindestens das Root-Dateisystem und Swap, der

Auslagerungsbereich für das RAM. So muss beim Start nur eine Partition entschlüsselt werden, die mit der LVM-Gruppe. Das wiederum erfordert, dass Bootloader Grub, Kernel und die Initial Ramdisk (initrd) auf einer unverschlüsselten Boot-Partition gespeichert sind. Ohne Unterstützung durch die Installationsprogramme müssen Sie die korrekte Partitionierung Schritt für Schritt selbst anlegen. Dies ist absurderweise beim wenig ausgefeilten Debian-Installer einfacher als unter Ubuntu.

Startschuss für Debian

Bei der Debian-Installation folgen Sie einfach dem vorgezeichneten Weg so weit, bis Sie gefragt werden, wo Debian installiert werden soll. Da der Installer die Installation mit einem verschlüsselten LVM nur für den Fall anbietet, wenn Sie die ganze Festplatte für Debian benutzen, wählen Sie hier „Manuell“ aus und finden sich in der Übersicht der Partitionen wieder.

Die nächsten Schritte führen Sie immer wieder zurück zu dieser Übersicht. Manchmal gibt es mehrere Optionen mit scheinbar der gleichen Funktion, folgen Sie dann bitte unserer Anleitung – sonst müssen Sie die Installation schlimmstenfalls wiederholen.

Der erste Schritt ist, eine Boot-Partition im freien Speicherbereich hinter Windows anzulegen. Diese sollte 1 GByte groß sein, damit Platz für mehrere Kernel-Versionen ist. Als Dateisystem verwenden Sie ext4, der Einbindepunkt ist /boot und als Namen sollten Sie den Hostnamen Ihres Rechners gefolgt von „-boot“ verwenden. Also zum Beispiel „debian-boot“, falls Sie den Standard-Hostnamen übernommen haben. Indem Sie möglichst alle Partitionen benennen, behalten Sie leichter den Überblick.

Zurück in der Übersicht der Partitionen wählen Sie den Menüpunkt „Verschlüsselte Datenträger konfigurieren“, um die

Partition für die LVM-Gruppe zu erstellen. Dort wählen Sie den freien Bereich hinter der gerade erstellten Boot-Partition aus, die sie leicht am Dateisystem ext4 in der Liste erkennen. Als Namen empfehlen wir den Hostnamen plus „-crypt“. Erst wenn Sie die Änderungen auf die Festplatte schreiben lassen und „Fertigstellen“ ausgewählt haben, fragt der Installer das Passwort ab und verschlüsselt die Partition. Und wieder landen Sie in der Übersicht der Partitionen, wo die gerade angelegte Partition mit dem Typ „crypto“ aufgeführt ist.

Vor und zurück, vor und zurück: Bis Sie alle für ein verschlüsseltes Debian-System benötigten Partitionen und Laufwerke angelegt haben, landen Sie immer wieder in der Übersicht der Partitionen.

Verschlüsselt, logisch?

Nun können Sie den „Logical Volume Manager konfigurieren“. Auch die „Übersicht der aktuellen LVM-Konfiguration“ werden Sie ebenfalls mehrfach betreten müssen; der erste Schritt besteht darin, eine „Volume-Gruppe“ zu erstellen. Darin

sollten Sie wiederum den Hostnamen Ihres Rechners verwenden – denn das tut auch der Debian-Installer, wenn Sie die ganze Festplatte verschlüsseln lassen. Als physisches Laufwerk für das LVM wählen Sie die gerade erstellte Crypto-Partition aus, die Sie an dem Namenszusatz „-crypt“ erkennen – sie steht normalerweise am Anfang der Liste.

Damit landen Sie erneut in der LVM-Übersicht, wo Sie nun den Eintrag „Logisches Volume erstellen“ vorfinden. Das erste logische Laufwerk, das Sie anlegen, ist für das Root-Dateisystem. Dazu wählen Sie die gerade erstellte Volume Group aus und geben dem logischen Laufwerk den Namen „root“. Bei der Größe sollten Sie mindestens 8192 MByte (8 GByte) für Swap abziehen.

Und wieder landen Sie in der Übersicht der LVM-Konfiguration, wo Sie den noch freien Platz in ein weiteres logisches Laufwerk stecken, diesmal mit dem Namen „swap_1“. Das Laufwerk könnte auch anders heißen, „swap_1“ ist jedoch der Name, den der Debian-Installer standardmäßig für den ersten Auslagerungsbereich bei einer verschlüsselten Installation verwendet.

Die Einrichtung des verschlüsselten LVM ist damit komplett, weshalb Sie sie über „Fertigstellen“ verlassen und schon wieder zur Übersicht der Partitionen zurückkehren. Allerdings weiß der Debian-Installer noch nicht, was er mit den logischen Laufwerken anfangen soll. Deshalb wählen Sie zunächst aus der Liste das logische Laufwerk für Swap aus, klicken auf „Weiter“ und stellen bei „Benutzen als“ „Auslagerungsspeicher (Swap)“ ein.

Jetzt fehlt nur noch das Root-Dateisystem: Zurück in der Übersicht wählen Sie das logische Laufwerk „root“ und klicken wiederum auf „Weiter“, um es als „Ext4“ zu verwenden. Als „Einbindungspunkt“ suchen Sie „/“ aus der Liste heraus und geben der neuen Partition den Hostnamen gefolgt von „-root“, analog zur Boot-Partition.

Damit ist der schwierige Teil der Installation abgeschlossen. Klicken Sie auf „Partitionierung beenden und Änderungen übernehmen“ und dann auf „Weiter“, um den Installer den Rest der Arbeit erledigen zu lassen. Den Abschluss der Debian-Installation bildet ein Neustart, woraufhin Sie dann die Wahl zwischen Debian und Windows haben.

Handarbeit bei Ubuntu

Die Ursache für den Mehraufwand bei der Ubuntu-Installation liegt darin, dass der Ubuntu-Installer bei der manuellen Partitionierung kein LVM unterstützt. Diesen Teil der Arbeit müssen Sie deshalb von Hand im Terminal erledigen. Außerdem bekommt der Installer nicht mit, dass Sie ein verschlüsseltes System einrichten, weshalb Sie auch konfigurieren müssen, dass das Root-Dateisystem beim Booten erst entschlüsselt wird.

Doch der Reihe nach: Wenn Sie Ubuntu vom USB-Stick starten, wählen Sie unbedingt „Ubuntu ausprobieren“ – nur so können Sie in den Installationsprozess eingreifen und zu gegebener Zeit das LVM über das Terminal von Hand konfigurieren. Am Desktop angekommen starten Sie die Installation und folgen dem vorgezeichneten Weg, bis Sie auswählen sollen, wo Ubuntu installiert werden soll.

Komfort gibt es nur, wenn Sie Ubuntu unverschlüsselt oder auf der ganzen Festplatte installieren lassen. Deshalb wählen Sie „Etwas Anderes“ und kümmern sich anschließend selbst um die Partitionierung. Die EFI-Boot-Partition hat Windows bereits angelegt, damit müssen Sie sich nicht weiter befassen. Allerdings benötigt Ubuntu eine eigene Boot-Partition, wir empfehlen dafür mindestens 1 GByte. Lassen Sie sie mit dem Dateisystem ext4 formatieren und unter /boot einbinden.

Im nächsten Schritt legen Sie die Partition für das verschlüsselte Linux-System an. Dabei ist entscheidend, dass Sie unter „Benutzen als“ „physikalisches Volume für Verschlüsselung“ auswählen. Daraufhin erweitert sich der

Dialog um die Passphrase-Abfrage. Sobald Sie den Dialog mit „OK“ bestätigen, verschlüsselt der Installer die Partition unmittelbar, bindet sie unterhalb von /dev/mapper ein und schickt Sie zurück zur Übersicht der Partitonen.

Auf Befehl

Es dauert bis zu einer halben Minute, bis die Partitionstabelle aktualisiert ist und das verschlüsselte Dateisystem als erster Eintrag in der Liste auftaucht. Nun ist es an der Zeit, das Terminal-Programm zu öffnen und das LVM einzurichten. Beginnen Sie damit, die Volume Group vgubuntu anzulegen:

```
sudo vgcreate vgubuntu \
  /dev/mapper/*_crypt
```

Wie viel Platz Sie im LVM haben, verrät Ihnen der Befehl pvdisplay --units m in ganzen Megabytes. Ziehen Sie davon mindestens 8192 MByte für Swap ab, den Rest können Sie mit dem Logical Volume für das Root-Dateisystem belegen:

```
sudo lvcreate -n root \
  -L 200000m vgubuntu
```

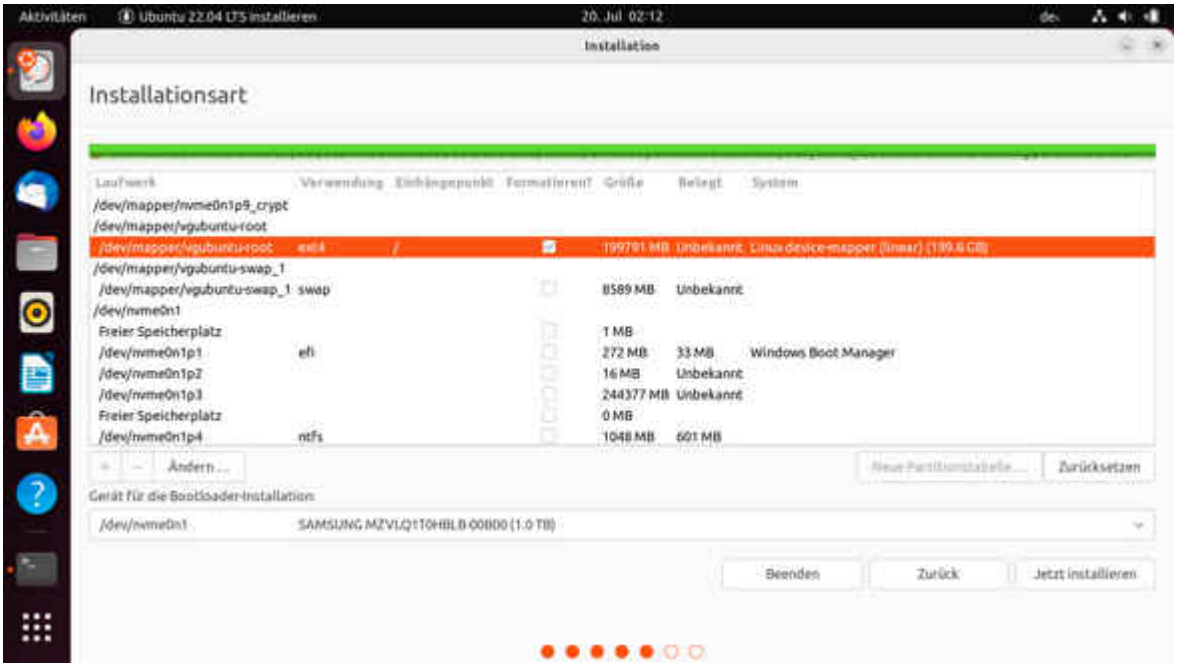
Was noch frei ist, stecken Sie in das Volume „swap_1“:

```
sudo lvcreate -n swap_1 \
  -l 100%free vgubuntu
```

Damit die Einstellungen wirksam werden, übernehmen Sie sie mit dem Befehl sudo vgchange -ay und kehren zum Installer zurück.

In der Partitionsübersicht des Installers klicken Sie nun auf „Zurück“, womit Sie wieder bei der Frage landen, wo Sie Ubuntu installieren wollen. Wählen Sie dort erneut „Etwas Anderes“ und klicken Sie auf „Weiter“ – so erzwingen Sie, dass der Installer die Partitionierung aktualisiert und auch das LVM erkennt. Nun tauchen am Anfang der Liste auch die gerade angelegten logischen Volumes auf. Indem Sie auf den Eintrag

„vgubuntu-root“ respektive „vgubuntu-swap_1“ und dann auf „Ändern“ klicken, lassen Sie das Root-Dateisystem als „Ext4-Journaling-Dateisystem“ formatieren und unter „/“ einbinden; bei Swap müssen Sie lediglich „Auslagerungsspeicher (Swap)“ wählen.



Der Ubuntu-Installer erlaubt es nicht, ein LVM von Hand einzurichten – weshalb Sie diese Schritte im Terminal erledigen müssen. Gibt es ein solches LVM, erkennt es der Installer und erlaubt Ihnen auch, es einzubinden.

Nachgeholfen

Vergessen Sie nicht, die Boot-Partition noch einmal als „Ext4-Journaling-Dateisystem“ zu formatieren und unter „/boot“ einbinden zu lassen: Weil Sie den Partitionierungsdialog verlassen hatten, hat der Installer Ihre früheren Angaben verworfen. Da sich der Installer auch nicht gemerkt hat, dass Sie mit einem verschlüsselten System arbeiten, trägt er die LUKS-Partition auch nicht in der Datei /etc/crypttab auf dem neuen System ein. Als Folge ignoriert das neu installierte System beim Booten die verschlüsselte Partition, findet kein Root-Dateisystem und kann deshalb nicht starten.

Dieses Problem müssen Sie ebenfalls im Terminal lösen, und zwar während der Installer das neu installierte System noch

bearbeitet. Klicken Sie auf „Jetzt installieren“ und bestätigen Sie die Änderungen noch einmal. Während der Installer nun im Hintergrund Dateien kopiert und Pakete installiert, fragt er bereits die Zeitzone ab. Warten Sie einige Minuten, bis die Aktivitäten auf der Festplatte abnehmen. Dann wechseln Sie noch einmal ins Terminal, wo Sie in der crypttab die UUID der verschlüsselten Partition eintragen.

Die UUID besorgen Sie sich zum Beispiel mit dem Befehl

sudo blkid /dev/sda3

falls Sie /dev/sda3 als „physikalisches Volume für Verschlüsselung“ ausgewählt hatten.

Das Root-Dateisystem des neuen Ubuntu ist während der Installation unterhalb des Verzeichnisses /target eingebunden. Mit dem Befehl sudo pico /target/etc/crypttab legt der Editor Pico die Datei neu an und Sie tragen dort folgende Zeile ein:

sda3_crypt UUID=21e8...cf15 none luks,discard

Ist /dev/sda3 nicht Ihre verschlüsselte Partition, müssen Sie den Namen „sda3_crypt“ anpassen – er beginnt stets mit dem Partitionsnamen und endet mit „_crypt“. Die UUID haben wir nur verkürzt abgedruckt, da Ihre ohnehin eine andere ist. Den Rest der Zeile übernehmen Sie 1:1.

Speichern Sie die Datei mit Strg+O, raus aus dem Editor geht es mit Strg+X. Anschließend müssen Sie im Terminal mit folgenden Befehlen die „Initial Ramdisk“ neu bauen lassen:

```
for d in dev sys proc; do
  sudo mount --bind /${d} /target/${d}
done
sudo chroot /target \
  update-initramfs -k all -c
for d in dev sys proc; do
  sudo umount /target/${d}
done
```

Etwaige Meldungen über fehlende Firmware-Dateien können Sie ignorieren. Danach können Sie das Terminal schließen. Zurück im Installer folgen Sie den Dialogen, bis die Installation abgeschlossen ist. Haben Sie den Rechner neu gestartet, empfängt Sie Ihr nun schlüsselfertiges Ubuntu mit der Frage nach dem Passwort Ihres Systems.

Zeitreise

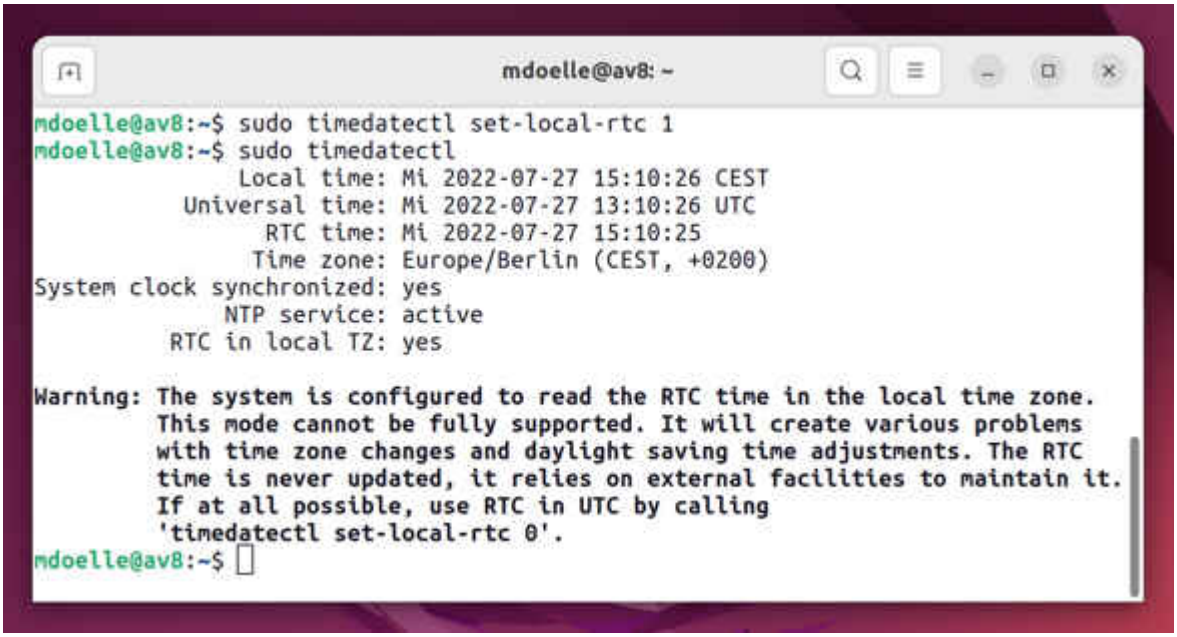
Ein ständiges Ärgernis bei Parallelinstallationen ist, dass Windows und Linux ständig die interne Uhr des Rechners verstellen: Windows speichert standardmäßig die Lokalzeit in der Hardware-Uhr, auch RTC (Real Time Clock) genannt, während Linux standardmäßig die Uhrzeit der Zeitzone UTC speichert. Letzteres lässt sich aber leicht mit dem Programm timedatectl ändern. Dazu öffnen Sie ein Terminal und geben folgenden Befehl ein:

```
sudo timedatectl set-local-rtc 1
```

Anschließend sollten Sie noch die Systemzeit, die in der Standardinstallation mit Zeitservern im Internet abgeglichen wird, in die Hardware-Uhr übertragen:

```
sudo hwclock -w
```

Ob Ihre Hardware-Uhr tatsächlich auf Lokalzeit umgestellt wurde, können Sie anschließend mit dem Befehl sudo timedatectl überprüfen. So vermeiden Sie, dass Windows und Linux ständig mit der falschen Uhrzeit starten und dies erst im laufenden Betrieb korrigieren. Die Warnung, dass es mit der Lokalzeit Probleme etwa bei der Sommer- und Winterzeitumstellung geben könnte, spielt auf Desktop-Rechnern keine Rolle: Das käme allenfalls zum Tragen, wenn Sie während der Zeitumstellung neu booten – und auch dann nur für wenige Minuten, bis die Systemzeit online abgeglichen und damit korrigiert wird.



Während Windows standardmäßig die Lokalzeit im Rechner speichert, benutzt Linux UTC. Dies lässt sich aber leicht ändern, sodass beide Betriebssysteme stets mit der richtigen Uhrzeit booten und nicht ständig an der Uhr drehen.

Fazit

Die Installer von Debian, Ubuntu und anderen Distributionen haben klar ein Defizit, Linux verschlüsselt neben Windows installieren zu können. Indem man sie an die Hand nimmt und die schwierigen Passagen Schritt für Schritt mit ihnen durchläuft, gelingt es aber trotzdem – bei Debian sogar ohne Eingriffe im Terminal, sofern Sie unserer Anleitung penibel folgen. Vielleicht animiert dieser Artikel die Entwickler ja dazu, ihre Installer um die wenigen fehlenden Pirouetten zu ergänzen, damit sich Linux künftig ohne großen Zinnober neben Windows einfügt. (*mid@ct.de*)

Das Beste beider Welten

Praxis: Gemeinsame

verschlüsselte Datenpartition optimal nutzen

Videobearbeitung unter Windows, Server-Administration unter Linux, Surfen und E-Mails überall: Mit einer gemeinsamen Datenpartition können Sie für jede Aufgabe die am besten geeignete Anwendung nutzen. Mit unserem VeraCrypt-Setup werden Ihre Daten zudem automatisch ver- und entschlüsselt, ohne dass Sie sich ein Passwort merken müssen.

Von Mirko Dölle

Obwohl Windows und Linux unterschiedliche Dateisysteme benötigen und verschiedene Verschlüsselungstechniken einsetzen, bedeutet die Parallelinstallation nicht zwangsläufig doppelte Datenhaltung. Mit VeraCrypt und NTFS gibt es einen gemeinsamen Nenner für eine verschlüsselte Datenpartition, mit der beide Betriebssysteme zurechtkommen. So vermissen Sie nie wieder Hörbücher, die Sie unter Windows heruntergeladen hatten, wenn Sie unter Linux programmieren oder Server warten.

Dieser Artikel beschreibt, wie Sie die gemeinsame Datenhalde durch angepasste Standardpfade und symbolische Links so in die Desktop-Umgebungen beider Betriebssysteme einbinden, dass Ihre Bilder, Dokumente, Downloads, Musik und Videos standardmäßig auf der gemeinsam genutzten Partition landen und diese beim Systemstart auch ohne zusätzliche Eingabe eines Passworts eingebunden wird. So verhält sich die Datenpartition transparent, Sie bekommen kaum mit, dass es sie überhaupt gibt, und können unter beiden Betriebssystemen wie gewohnt arbeiten.

Wir haben uns für VeraCrypt entschieden, weil sich das Programm unter Linux und für Windows bewährt hat. Mit der Einrichtung einer VeraCrypt-verschlüsselten Datenpartition

beginnen Sie idealerweise, nachdem Sie wie auf Seite 16 beschrieben Windows verkleinert haben: Öffnen Sie erneut die Datenträgerverwaltung von Windows, klicken Sie mit der rechten Maustaste auf den zuvor freigegebenen Speicherbereich und wählen Sie aus dem Kontextmenü „Neues einfaches Volume…“ aus. Bedenken Sie bei der Größe der künftigen Datenhalde, dass Sie ja noch Platz für die Linux-Installation benötigen – 50 GByte sollten das mindestens sein, mit vielen Anwendungen besser 100 GByte. Falls Sie viele native Linux-Anwendungen oder Spiele installieren wollen, brauchen Sie vielleicht noch mehr. Was Sie nicht für Linux benötigen, geben Sie der neuen Partition und wählen „Keinen Laufwerksbuchstaben oder -pfad zuweisen“ sowie „Dieses Volume nicht formatieren“, damit Windows die Partition in Ruhe lässt und nicht etwa zusätzlich mit BitLocker verschlüsselt.

Als Nächstes laden Sie die Windows-Version der kostenlosen Verschlüsselungssoftware VeraCrypt von veracrypt.fr herunter und installieren diese mit den Standardeinstellungen. Den Abschluss bildet ein Neustart von Windows, danach starten Sie VeraCrypt zum ersten Mal.

Fast unsichtbar

Damit VeraCrypt später nahezu unsichtbar arbeitet und die Datenpartition automatisch einbindet, verwenden Sie anstatt eines Passworts einen Schlüssel zum Entschlüsseln; der ist auf der mit BitLocker oder ebenfalls mit VeraCrypt verschlüsselten Windows-Systempartition und später auf der LUKS-verschlüsselten Linux-Partition sicher aufgehoben. Diesen Schlüssel erzeugen Sie über das Menü „Tools/Keyfile Generator“ und speichern ihn etwa unter dem Namen „winlin-key“ im persönlichen Ordner des Administrators. Anschließend kopieren Sie den Schlüssel mit dem Explorer auf einen USB-Stick, um ihn später unter Linux einlesen zu können.

Über „Tools/ Volume Creation Wizard“ verschlüsseln Sie die zuvor angelegte Datenpartition, indem Sie dort „Encrypt a non-

system partition/drive“ auswählen und ein „Standard VeraCrypt volume“ anlegen lassen. Als „Volume Location“ wählen Sie die Partition aus und klicken anschließend auf „Create encrypted volume and format it“. Wenn VeraCrypt nach dem „Volume Password“ fragt, lassen Sie das leer und aktivieren stattdessen „Use keyfiles“ und wählen unter „Keyfiles…“ die zuvor erzeugte Schlüsseldatei winlin-key aus. Bei der Frage nach „Large Files“ sollten Sie „Yes“ auswählen und bei „Volume Format“ als „Filesystem“ „NTFS“, außerdem „Quick Format“, damit VeraCrypt den Speicherbereich nicht überschreibt. Sofern sich dort zuvor Ihre mit BitLocker verschlüsselte Windows-Partition befunden hat, ist die Schnellformatierung kein Problem – dort lagerten dann keine Klartext-Daten.

Haben Sie die Partition mit VeraCrypt verschlüsselt und formatiert, wählen Sie dafür einen Laufwerksbuchstaben aus – zum Beispiel V:. Keinesfalls sollten Sie D: oder einen anderen vom Anfang des Alphabets nehmen, der zukünftig einem USB-Stick oder Kartenleser zugeordnet werden könnte, denn dann laufen später die neuen Standardpfade ins Leere. Als „Volume“ wählen Sie über „Select Device…“ die gerade vorbereitete Partition aus und klicken dann auf „Auto-Mount Devices“, damit die Partition künftig bei jedem Start von Windows wieder entschlüsselt und eingebunden wird. Wählen Sie bei der Passwortabfrage wiederum „Use keyfiles“ und unter „Key“ winlin-key als Schlüsseldatei aus.

Um die Datenpartition künftig automatisch bei jedem Systemstart einbinden zu lassen, klicken Sie mit der rechten Maustaste in der Liste der Laufwerksbuchstaben auf V: und wählen „Add to Favourites…“ aus dem Kontextmenü. Aktivieren Sie in der Liste der Optionen „Mount selected volume upon logon“ sowie „Mount selected volume when its host device gets connected“.

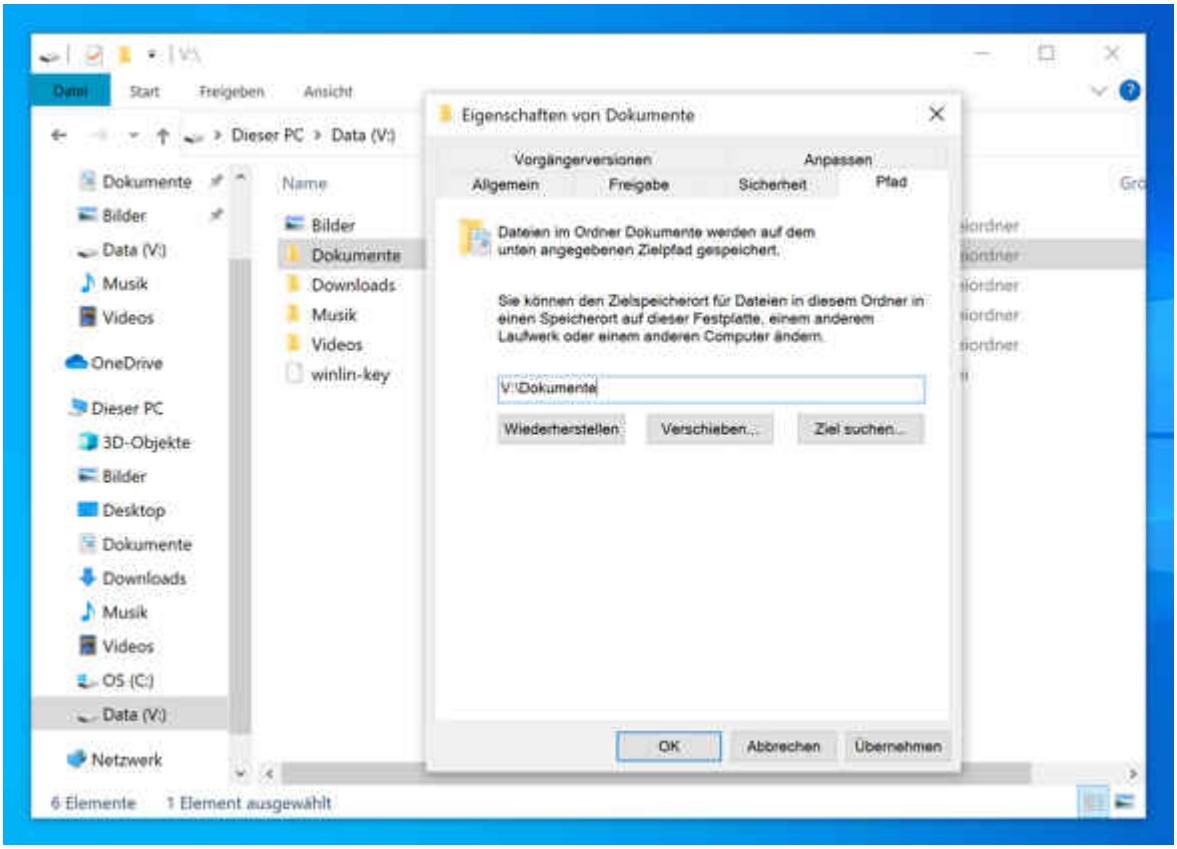
Damit VeraCrypt Sie zukünftig nicht mehr mit der Frage nach dem Passwort oder der Schlüsseldatei behelligt, importieren Sie über „Settings/Default Keyfiles…“ und dort über „Add

Files…“ den Schlüssel winlin-key als Standardschlüssel. Außerdem aktivieren Sie die Option „Try first to mount with an empty password“, ansonsten erwartet VeraCrypt später weiterhin eine manuelle Passworteingabe. Damit ist das Einrichten der verschlüsselten Datenpartition unter Windows abgeschlossen.

Auf neuen Pfaden

Wenn Sie die Windows-eigenen Ordner für Bilder, Downloads und so weiter verwenden, können Sie diese auf die VeraCrypt-Partition verlegen. Zum Ändern der Standardpfade legen Sie zunächst mit dem Explorer auf der VeraCrypt-Partition einzelne Verzeichnisse für Bilder, Dokumente, Musik, Videos und Downloads an. Den Desktop dürfen Sie dort nicht speichern, denn dieser baut sich unter Umständen schon auf, noch bevor die Partition eingebunden ist – das führt dann zu hässlichen Fehlermeldungen.

Um den Standardpfad für Bilder auf V:\Bilder zu ändern, klicken Sie im Explorer mit der rechten Maustaste im linken Navigationsbereich unterhalb von „Dieser PC“ auf „Bilder“ und wählen aus dem Kontext-Menü „Eigenschaften“. Im Register „Pfad“ klicken Sie nun auf „Verschieben“ und wählen das Verzeichnis V:\Bilder als neuen Ort aus. Sobald Sie auf „Übernehmen“ klicken, fragt Sie der Explorer, ob er die vorhandenen Daten dorthin verschieben soll – sagen Sie „Ja“. Genauso gehen Sie mit allen anderen Ordnern vor, die Sie auf die gemeinsame Datenpartition verlegen wollen. Jetzt ist Ihre gemeinsame Datenpartition voll integriert.



Indem Sie die Standardpfade auf die gemeinsam genutzte Datenpartition verschieben, sind Ihre Bilder, Dokumente, Downloads und vieles mehr auch unter Linux abrufbar.

Bei der Einrichtung unter Linux haben Sie die Wahl zwischen VeraCrypt mit GUI, womit Sie dann auch komfortabel USB-Sticks verschlüsseln können, und der reinen Kommandozeilenversion – die genügt, um die Datenpartition einzubinden, die Verwaltung von Partitionen sollten Sie besser unter Windows erledigen. VeraCrypt spielen Sie aber erst ein, nachdem Sie bereits Linux verschlüsselt neben Windows und neben der bereits eingerichteten Datenpartition installiert haben. Der Artikel auf Seite 22 beschreibt, worauf Sie bei Debian 11 und Ubuntu 22.04 LTS achten müssen. Die nachfolgende Anleitung zur Einrichtung von VeraCrypt gilt für beide Distributionen.

Linux schlüsselfertig

Laden Sie sich das zu Ihrer Distribution passende Paket, mit oder ohne GUI, aus dem Download-Bereich von veracrypt.fr herunter. Danach öffnen Sie ein Terminal, um es mit folgenden Befehlen zu installieren:

```
sudo dpkg -i Downloads/veracrypt*.deb
sudo apt -f install
```

Der zweite Befehl dient dazu, die Paketabhängigkeiten automatisch aufzulösen. Im nächsten Schritt legen Sie den Mount Point für die Datenpartition an, außerdem ein Verzeichnis für Schlüssel und kopieren dann den VeraCrypt-Schlüssel winlin-key vom USB-Stick in das neue Verzeichnis:

```
sudo mkdir /data
sudo mkdir -m 700 /etc/crypto
sudo cp /media/*/*/winlin-key \
  /etc/crypto
```

Automagie

Damit ist VeraCrypt betriebsbereit und Sie können sich darum kümmern, dass die Datenpartition künftig beim Systemstart automatisch entschlüsselt und eingebunden wird. Dazu ergänzen Sie folgende Zeile am Ende der Datei /etc/crypttab:

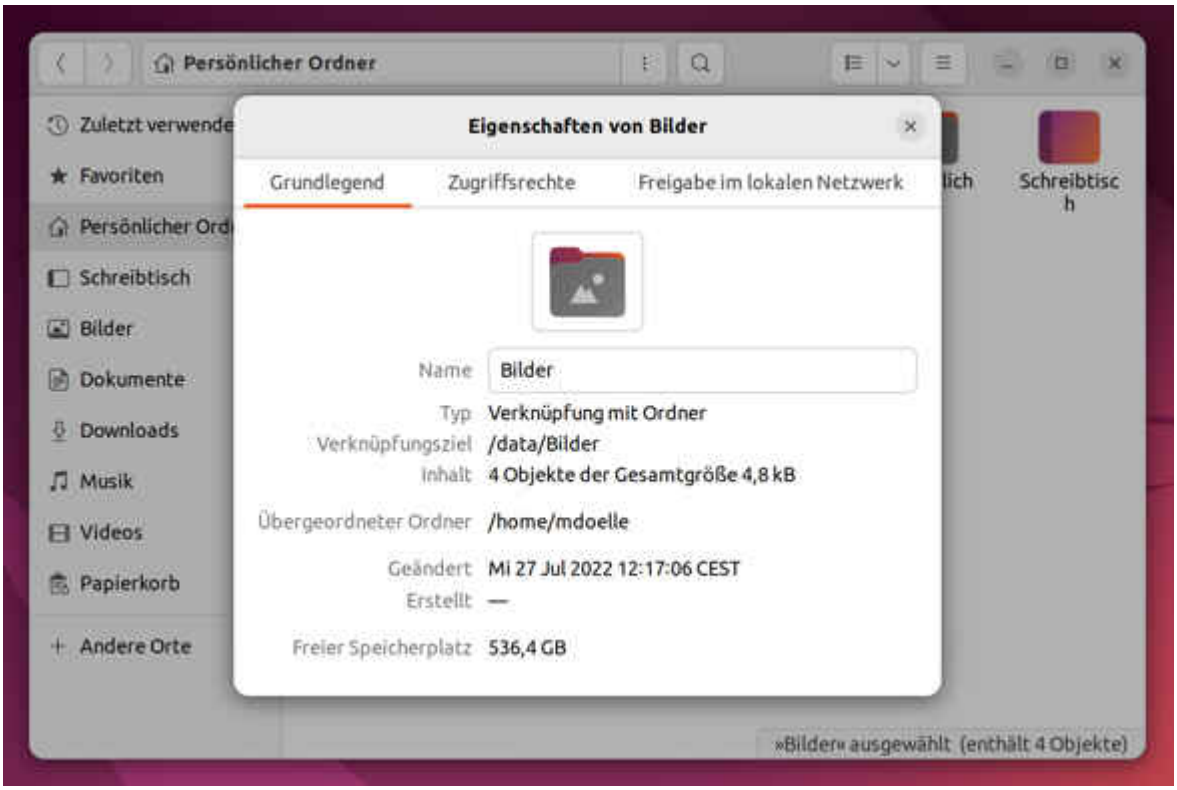
```
winlin-data  /dev/sda3  /dev/nulltcrypt-veracrypt,tcrypt-keyfile=/etc/crypto/winlin-key
```

Den Gerätenamen /dev/sda3 ersetzen Sie durch den Gerätenamen Ihrer Datenpartition, den Sie mit dem Befehl lsblk herausfinden. Damit wird die Datenpartition entsperrt und bekommt den Namen „winlin-data“. Die folgende Zeile am Ende der Datei /etc/fstab bindet die Datenpartition schließlich unterhalb von /data ein:

```
/dev/mapper/winlin-data          /data          auto uid=1000,gid=1000,nodev,nofail 0 0
```

Nach dem nächsten Neustart ist die Datenpartition für den ersten Benutzer im System mit der User-ID 1000 beschreibbar unter /data eingebunden. Verschieben Sie nun den Inhalt des Verzeichnisses „Bilder“ in Ihrem „Persönlichen Ordner“ (Home-Verzeichnis) nach /data/Bilder, etwa per Drag & Drop mit zwei Fenstern des Dateimanagers Nautilus.

Anschließend löschen Sie das nun leere Verzeichnis Bilder. Um einen symbolischen Link zum Bilderverzeichnis auf der gemeinsamen Datenhalde anzulegen, ziehen Sie das Verzeichnis /data/Bilder aus dem anderen Nautilus-Fenster per Drag & Drop in Ihren „Persönlichen Ordner“ und halten dabei die Alt-Taste gedrückt. Beim Loslassen wählen Sie dann aus dem Kontextmenü „Verknüpfung erstellen“. Damit verweist der Ordner Bilder in Ihrem Home-Verzeichnis auf das Verzeichnis /data/Bilder, wo auch Ihre Bilder aus Windows gespeichert sind. Diesen Vorgang wiederholen Sie für Dokumente, Musik, Videos und alle anderen Verzeichnisse, deren Daten Sie künftig auf der gemeinsamen Datenpartition speichern wollen.



Durch symbolische Links für Bilder, Dokumente und andere Verzeichnisse verweisen Sie alle Linux-Anwendungen auf die gemeinsam genutzte Datenpartition als Speicherort, sodass Sie sie auch unter Windows öffnen können.

Welche Anwendung wofür?

Zwei verschlüsselte Betriebssysteme mit gemeinsamer Datenpartition sind eine tolle Arbeitsgrundlage – doch womit arbeitet man konkret? Das hängt davon ab, was Sie individuell

benötigen oder wo Ihre Vorlieben liegen. Falls Sie regelmäßig mit Kollegen an MS-Office-Dokumenten oder Präsentationen arbeiten, werden Sie nicht an Microsoft Office unter Windows vorbeikommen. Unter Linux genügt Ihnen LibreOffice oder OpenOffice, mit denen Sie bei Bedarf einen flüchtigen Blick in ein Office-Dokument werfen können.

Spielt Kompatibilität keine große Rolle, können Sie sich das Geld für Microsoft Office sparen und auch unter Windows zur Open-Source-Variante Ihres Linux-Office-Pakets greifen. Dann haben Sie den Vorteil, dass es keine Konvertierungsprobleme mit Ihren eigenen Office-Dateien gibt und die Bedienung weitgehend einheitlich ist.

Es muss aber nicht immer das gleiche Programm sein: Falls Sie allenfalls mal den Anfang und das Ende eines Screen-Recordings wegschneiden, genügen dazu die jeweiligen Bordmittel von Windows und Linux. Erst wenn Ihre Projekte etwas ambitionierter werden, lohnt es sich, wenn Sie sich in das wesentlich leistungsfähige Kdenlive einarbeiten, das es für beide Betriebssysteme kostenlos gibt. Videoproducer hingegen werden kaum an Adobe Premiere für Windows vorbeikommen, benötigen dann aber unter Linux keinen speziellen Videoeditor.

Ähnlich ist es bei der Foto- und Bildbearbeitung: Wer das beruflich macht oder große Ambitionen hat, wird früher oder später Photoshop und die Adobe Creative Suite benutzen müssen. Dann hat es aber wenig Sinn, sich zusätzlich in Gimp einzuarbeiten – unter Linux genügt dann die Vorschau, um sich Bilder anzusehen. Benötigen Sie hingegen nicht den Leistungsumfang eines Adobe Photoshop, kann Gimp eine Alternative für Windows und Linux sein. Auch dann profitieren Sie von der einheitlichen Bedienung.

Als Browser empfehlen wir Ihnen Firefox: Haben Sie einen kostenlosen Account angelegt, können Sie per Firefox Sync von den Lesezeichen bis hin zu den gerade geöffneten Tabs und Websites alles zwischen Windows und Linux synchronisieren, was

Sie für den Alltag brauchen. Je mehr Sie synchronisieren (und damit verschlüsselt in die Cloud übertragen) lassen, desto leichter fällt es Ihnen später, ad hoc von Windows nach Linux zu wechseln und umgekehrt – denn Sie können nahtlos da weiter surfen, wo Sie auf dem anderen Betriebssystem gerade waren.

Sofern Sie Ihre E-Mails per IMAP bei Ihrem Provider abholen, können Sie genauso gut Thunderbird unter Windows und Linux einsetzen wie zwei verschiedene Programme: Wenn beide Programme die Entwürfe in dem dafür vorgesehenen IMAP-Ordner zwischenspeichern, können Sie sogar E-Mails unter Linux fertig schreiben, die Sie unter Windows begonnen haben – und umgekehrt.

Auch bei manchen Spielen haben Sie die Wahl, die Wikinger-Variante von Minecraft, Valheim, zum Beispiel gibt es im Steam Store sowohl für Windows als auch für Linux. Sie können sich für eine der beiden Varianten entscheiden, oder aber die Spielstände über die Steam Cloud zwischen Windows und Linux synchronisieren lassen. Diese Lösung ist auch besser, als aufwendig die Speicherpfade der Spielstände unter Windows und Linux so zu verändern, dass sie auf der gemeinsamen Datenpartition landen: Nicht alle Windows-Spiele kommen mit den Dateien der anderen Plattformen zurecht, die Cloud-Synchronisation von Steam hingegen ist eigens darauf ausgelegt.

Fazit

Man muss sich nicht zwischen Windows und Linux entscheiden. Beide Betriebssysteme haben ihre Berechtigung und sind letztlich nur die Basis, auf der man seine eigentliche Arbeit erledigt – mit dem am besten dafür geeigneten Werkzeug. Die gemeinsame verschlüsselte Datenpartition und Funktionen wie Firefox Sync machen es Ihnen leicht, für eine bestimmte Aufgabe das jeweils andere Betriebssystem zu booten und dabei an der gleichen Stelle weiterzuarbeiten, an der Sie aufgehört haben. *(mid@ct.de)*