Linux supersicher

Auch bei Linux-Systemen können Unbefugte an vertrauliche Daten gelangen, die sie nichts angehen, etwa wenn Sie Ihr Notebook verlieren. Dieser Artikel zeigt, wie Sie sich davor schützen.

Von **Thorsten Eggeling**

Linux kann als besonders sicheres Betriebssystem gelten, weil standardmäßig die Rechte der einzelnen Benutzer auf das Nötigste beschränkt sind. Schreibzugriff ist nur im Home-Verzeichnis und in „/tmp“ erlaubt. Ohne root-Passwort lässt sich weder über die Paketverwaltung Software installieren noch sind Änderungen an den Systemeinstellungen möglich. Noch mehr Sicherheit lässt sich erreichen, wenn Sie das Home-Verzeichnis verschlüsseln. Das ist vor allem bei tragbaren Geräten sinnvoll, damit bei Verlust andere Personen Ihre Daten nicht einsehen können. Außerdem lassen sich die Rechte im Dateisystem so setzen, dass für weitere Nutzer des PCs der Zugriff auf Ihr Home-Verzeichnis verweigert wird. Die Tipps beziehen sich auf Ubuntu 13.04. Bei anderen Linux-Distributionen stehen die Funktionen möglicherweise nicht zur Verfügung oder sind auf anderem Wege zu erreichen.

Zugriffschutz einrichten über Benutzerrechte

Ubuntu legt die Zugriffrechte für die Benutzerverzeichnisse so fest, dass jeder Benutzer den Inhalt fremder Home-Verzeichnisse sehen und die Dateien kopieren oder öffnen kann. Wenn Sie das nicht wünschen, klicken Sie im Dash auf das Icon „Dateien“ und gehen unter „Geräte“ auf „Rechner“. Wechseln Sie in das Verzeichnis „home“. Klicken Sie den Ordner mit Ihrem Anmeldenamen mit der rechten Maustaste an, wählen Sie im Kontextmenü „Eigenschaften“, und gehen Sie jetzt auf die Registerkarte „Zugriffsrechte“. Unter „Andere“ stellen Sie hinter „Zugriff“ den Wert „keiner“ ein und beenden dann die Aktion mit Klick auf „Schließen“.

Wenn andere Benutzer jetzt versuchen, Ihr Home-Verzeichnis zu öffnen, erhalten diese die Meldung „Dieser Ort kann nicht angezeigt werden“ – und der Zugriff wird verweigert. Anders als bei verschlüsselten Ordnern können jedoch Benutzer, die root-Rechte besitzen oder den PC von einer Live-CD starten, jederzeit den Inhalt Ihres Home-Verzeichnisses einsehen.

Home-Verzeichnis verschlüsseln

Ein verschlüsseltes und damit sicheres Home-Verzeichnis lässt sich am einfachsten gleich bei der Ubuntu-Installation anlegen. Wenn Sie bei der Installation das Fenster „Wer sind Sie?“ sehen, setzen Sie ein Häkchen vor „Meine persönlichen Daten verschlüsseln“. Nach der ersten Anmeldung beim neu installierten System erscheint ein Fenster mit dem Hinweis „Ihre Verschlüsselungspassphrase notieren“. Klicken Sie auf „Diese Aktion ausführen“. Danach geben Sie das Anmeldepasswort ein und bestätigen mit der Enter-Taste. Sie sehen dann das von Ubuntu zufällig generierte Passwort für die Verschlüsselung. Notieren Sie dieses, denn Sie benötigen es im Problemfall vielleicht später einmal für die Wiederherstellung eines defekten Dateisystems.

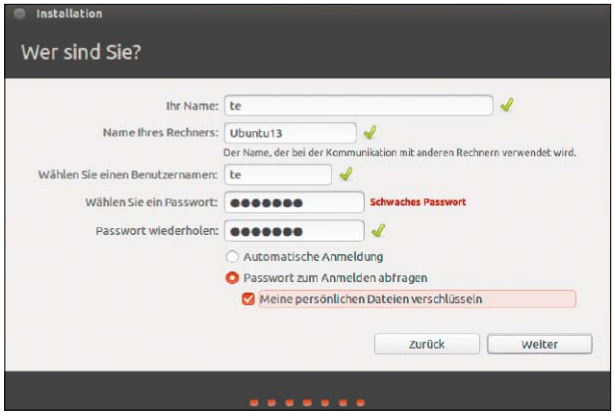
Für den Zugriff auf Ihr Home-Verzeichnis genügt aber die Anmeldung bei Ubuntu mit dem bei der Installation vergebenen Passwort. Die Entschlüsselung erfolgt automatisch im Hintergrund. Vor anderen Benutzern am selben PC ist das verschlüsselte Home-Verzeichnis ebenfalls sicher. Diese erhalten beim Zugriff eine Fehlermeldung, die auf fehlende Rechte hinweist.

Home-Verzeichnis eines neuen Benutzerkontos verschlüsseln: Über die grafische Oberfläche gibt es bisher keine Möglichkeit, neue Benutzer mit einem verschlüsselten Home-Verzeichnis anzulegen. Das müssen Sie über die Kommandozeile erledigen. Öffnen Sie mit der Tastenkombination Strg-Alt-T ein Terminalfenster. Geben Sie die Zeile

```
sudo adduser --encrypt-home
 Benutzername
```

ein. „Benutzername“ ersetzen Sie durch den Namen des Benutzers, den Sie neu erstellen möchten. Tippen Sie das root-Passwort ein, und bestätigen Sie mit der Enter-Taste. Anschließend legen Sie das Passwort für den neuen Benutzer hinter „Geben Sie ein neues Unix-Passwort ein:“ fest. Geben Sie die Benutzerinformationen ein, oder lassen Sie die Zeilen leer und bestätigen einfach mit der Enter-Taste. Die letzte Frage „Sind diese Informationen korrekt?“ bestätigen Sie ebenfalls mit der Enter-Taste. Danach kann sich der neu angelegte Benutzer mit dem von Ihnen festgelegten Passwort anmelden und das verschlüsselte Home-Verzeichnis nutzen. Auch er erhält einen Hinweis, sich die Verschlüsselungspassphrase zu notieren.

Bereits vorhandenes Home-Verzeichnis verschlüsseln: Es ist bei Ubuntu standardmäßig nicht vorgesehen, die Verschlüsselung nachträglich zu aktivieren. Am einfachsten ist es, alle persönlichen Dateien an einem anderen Ort zu sichern, den bisherigen Benutzer zu löschen, dann einen neuen Benutzer mit verschlüsseltem Home-Verzeichnis anzulegen und die gesicherten Dateien danach in das neue Home-Verzeichnis zu kopieren. Eine genaue Anleitung dazu lesen Sie im Folgeartikel auf Seite 34.



Ubuntu bietet Ihnen bei der Installation an, das Home-Verzeichnis zu verschlüsseln. Das gilt jedoch nur für den zuerst eingerichteten Benutzer. Für weitere Benutzer müssen Sie die Verschlüsselung selbst aktivieren.

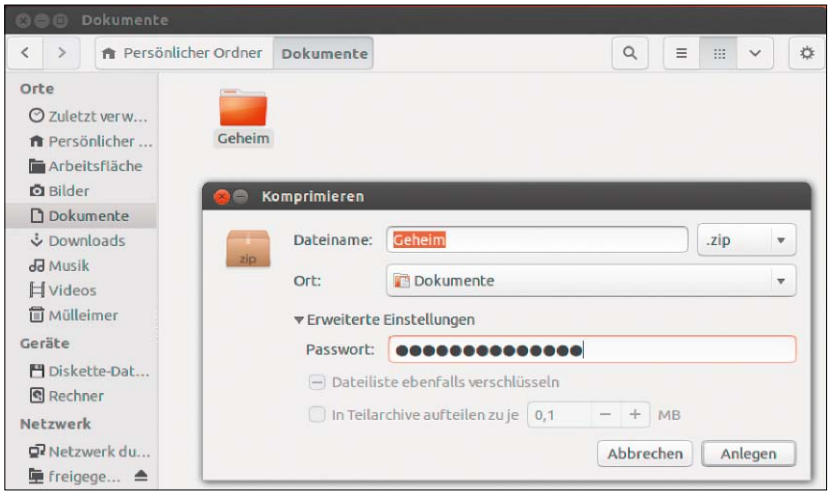
Einzelne Dateien oder Ordner verschlüsseln

Ein komplett verschlüsseltes Home-Verzeichnis ist bequem, weil Sie sich dann weiter um nichts mehr kümmern müssen. Allerdings müssen Sie die Verschlüsselung erst umständlich einrichten, wenn Sie sie nicht schon bei der Installation aktiviert haben.

Wenn es Ihnen vor allem darum geht, einzelne Dateien oder Ordner mit vertraulichen Informationen zu verschlüsseln, gibt es einfachere Wege. Sie können die Dateien beispielsweise in ein ZIP-Archiv packen und mit einem ausreichend langen (mehr als 15 Zeichen) und sicheren Passwort versehen. Der Vorteil verschlüsselter ZIP-Archive ist, dass sie sich per Mail versenden oder auf einem USB-Stick sichern lassen. Sie lassen sich außerdem mit gängigen Archivierungsprogrammen unabhängig vom Betriebssystem entschlüsseln und entpacken.

Und so geht’s: Klicken Sie einen Ordner oder eine Datei mit der rechten Maustaste an und wählen im Kontextmenü „Komprimieren“. Geben Sie einen Dateinamen für das Archiv ein und wählen Sie auf der rechten Seite des Fensters „.zip“. Klicken Sie auf „Erweiterte Einstellungen“ und dann auf „Anlegen“. Danach können Sie die Originaldateien löschen.

Als Alternative zur ZIP-Verschlüsselung bietet sich das sichere und plattformunabhängige Truecrypt an (*www.truecrypt.org*). Damit lassen sich Dateien in verschlüsselten Container ablegen oder ganze Partitionen verschlüsseln (siehe Seite 34).



Für schnelle Verschlüsselung zwischendurch bietet sich ein ZIP-Archiv an. Die Verschlüsselung gilt als unknackbar, wenn Sie ein langes und kompliziertes Passwort wählen.

Datenschutz durch Verschlüsselung

Bildnachweis: © Maxim_Kazmin - Fotolia.com

Linux-Nutzer sehen der Bedrohung durch Malware gelassen entgegen. Aber vergessene Notebooks oder Diebstahl bedrohen die Sicherheit vertraulicher Informationen natürlich auch hier. Lesen Sie hier, wie Sie System und ausgewählte Daten schützen.

Von **Stephan Lamprecht**

Wer produktiv unter Linux arbeitet, hat auf seinem System unzählige Dateien, deren Inhalt unbefugte Dritte nichts angehen. Ob der Computer nun zur Beute eines Diebes wird, verloren geht oder eine Sicherheitslücke von einem Angreifer ausgenutzt wird: In allen Fällen wollen Sie sicherlich Ihre vertraulichen Daten vor neugierigen Blicken geschützt wissen.

Verschlüsseln von Containern oder auf Dateiebene

Betrachten Sie die Verschlüsselung unter einem rein technischen Standpunkt, gibt es mehrere Wege, um den Inhalt einer Datei für einen Dritten unleserlich zu machen: Der einfachste Ad-hoc-Schutz ist die Verschlüsselung von sensiblen Einzeldateien. Dies kann durch einen Kennwortschutz von Büro-Software wie Libre Office geschehen („Datei → Eigenschaften → Schützen“) oder durch ein Packprogramm mit eingebauter Verschlüsselung wie 7-Zip (siehe Seite 32). Dieser Artikel beschreibt nachfolgend nur umfassendere Methoden mit größeren Datenmengen.

Verschlüsselte Container: Hierbei legen Sie die Dokumente in einem Datenspeicher ab, der verschlüsselt ist. Diese Datenspeicher werden als Container-Dateien bezeichnet. Um später wieder auf Ihr Dokument zugreifen zu können, müssen Sie den Container erst öffnen und in das System einbinden. Die Container nutzen Sie wie externe Festplatten. Wenn Sie dabei eine plattformübergreifende Software verwenden, die auf mehreren Betriebssystemen läuft, können Sie die Container auf verschiedenen Systemen verwenden. Dies setzt allerdings voraus, dass Sie ein Dateisystem verwenden, das auf der anderen Plattform verstanden wird. Ein Nachteil dieser Art von Verschlüsselung liegt darin, dass die Container wie einfache Dateien auf dem System liegen. Damit können sie versehentlich gelöscht, verschoben, eventuell auch gestohlen werden.

Verschlüsseltes Dateisystem: Ein weiterer Weg führt über die Verschlüsselung des Dateisystems selbst. Sie verschlüsseln eine Datei, ein Verzeichnis oder sogar eine Festplatte vollständig. Die Dateien bleiben damit auch als solche sichtbar, können aber ohne die passende Entschlüsselungs-Software nicht eingesehen werden.

Neuen Container anlegen

Möchten Sie verschlüsselte Container zur Absicherung Ihrer Dokumente einsetzen, stehen eine Reihe von Program-

Mails verschlüsseln

Damit Ihre Mails nicht im Klartext übers Internet gehen oder auf IMAP-Servern lesbar sind, gibt es seit langem die bewährte PGP-Verschlüsselung. Dazu nehmen Sie einen Mail-Client wie Thunderbird, das Modul Gnupg für die eigentliche Arbeit, ferner das Thunderbird-Add-on Enigmail. Gnupg ist nicht überall Standard, kann aber leicht nachinstalliert werden (unter Ubuntu: *sudo apt-get install gnupg2*). Enigmail suchen und installieren Sie in Thunderbird über „Extras → Add-ons“. Nach dem nächsten Thunderbird-Start gibt es das zusätzliche Menü „OpenPGP“, und der „OpenPGP-Assistent“ führt durch die Einrichtung. Über „OpenPGP → Nachricht verschlüsseln“ versenden Sie abhörsichere Mails. PGP funktioniert allerdings nur bei Mailpartnern, die ebenfalls einen PGP-Schlüssel besitzen.

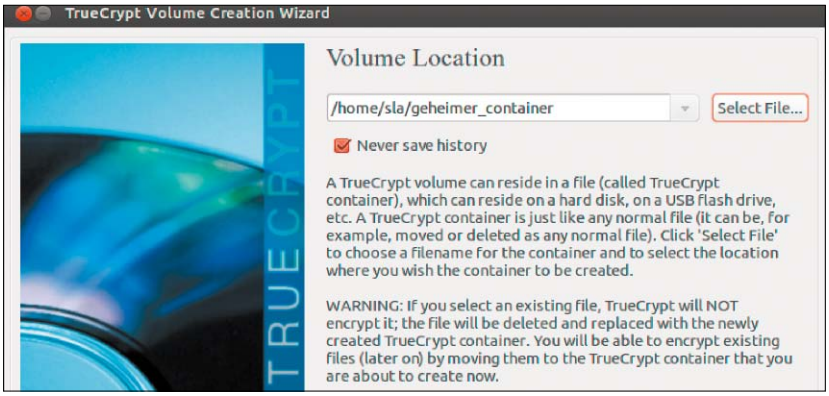
men zur Auswahl, mit denen Sie die Aufgabe erledigen können. Eines der bekanntesten ist Truecrypt. Es ist mit einer grafischen Oberfläche ausgestattet und steht für Linux, Mac-OS und Windows zur Verfügung. Allerdings hat das Programm es bisher nicht in die offiziellen Paketquellen geschafft. Besuchen Sie deshalb die Seite *www.truecrypt.org* und besuchen Sie dort den Bereich mit den Downloads. Am unteren Rand der Seite finden Sie die Auswahl für Linux. Beim Download handelt es sich um ein Archiv. Wenn Sie im Dateimanager doppelt darauf klicken, öffnet sich unter Ubuntu standardmäßig Fileroller. Markieren Sie mit der Maus das Element in dem Archiv, und ziehen Sie es an in einen beliebigen Ordner. Öffnen Sie dann ein Terminal und wechseln damit in das Verzeichnis, in das Sie das Script aus dem Archiv entpackt haben. Mit

```
./truecrypt-7.1a-setup-x86
```

rufen Sie das Installationsprogramm auf. Möglicherweise müssen Sie die Versionsnummer noch anpassen. Klicken Sie auf den Schalter „Install Truecrypt“. Jetzt blendet Ihnen das Programm ein weiteres Fenster ein. Darin finden Sie den Funktionsaufruf, um die Anwendung auch später wieder deinstallieren zu können.

Der eigentliche Installationsvorgang ist sehr einfach. Ist die Einrichtung erfolgreich abgeschlossen, schließen Sie alle noch geöffneten Fenster.

Nach der Installation starten Sie die Software wie jedes andere Programm direkt über das Startmenü Ihres Desktops. Die Software begrüßt Sie mit einem mehr oder weniger leeren Programmfenster. Möchten Sie einen neuen Datenspeicher anlegen, klicken Sie auf „Create Volume“. Damit starten Sie einen Assistenten, der Sie durch die nächsten Schritte führt. Entscheiden Sie sich für „Create an encrypted file container“, und fahren Sie fort. Im nächsten Dialog entscheiden Sie sich für „Standard“. Jetzt müssen Sie einen Namen vergeben und mit einem Klick auf „Select File“ in das Verzeichnis wechseln, in dem Sie den Daten-Container anlegen wollen. Jetzt möchte das Programm von Ihnen wissen, welches Verschlüsselungsverfahren Sie einsetzen wollen.



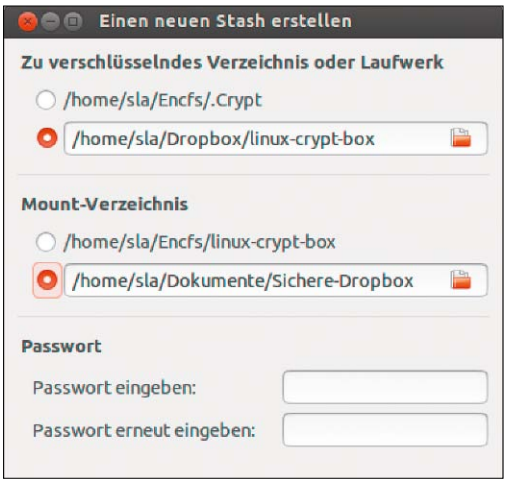
Neuen Container anlegen: In Truecrypt legen Sie zunächst den Namen und den Speicherort für den verschlüsselten Container fest.

Dateisystem bestimmen: Wenn Sie den Truecrypt-Container auf unterschiedlichen Betriebssystemen nutzen wollen, verwenden Sie als Dateisystem „FAT“.

Je komplexer die Verschlüsselung, desto sicherer sind Ihre Daten zwar, aber desto langsamer können Sie auch darauf zugreifen, weil das System intensiver mit der Entschlüsselung beschäftigt ist. Um Sie bei der Auswahl des passenden Verschlüsselungsverfahrens zu unterstützen, können Sie in diesem Dialog auf „Benchmark“ klicken. Im neuen Fenster, das Ihnen Truecrypt zeigt, klicken Sie erneut auf „Benchmark“ und sehen anschließend die (theoretisch) auf Ihrem System möglichen Übertragungsraten bei der Arbeit mit Dateien in Abhängigkeit der Verschlüsselung.

Nachdem Sie sich für ein Verfahren entschieden haben, definieren Sie die Größe des Containers. Vergeben Sie anschließend ein sicheres Passwort. Danach gelangen Sie zur wichtigen Auswahl des Dateisystems des Containers. Sofern Sie die Daten auch mit anderen Betriebssystemen nutzen wollen, verwenden Sie FAT. Ist der Einsatz lediglich auf Ihrem eigenen Rechner geplant, darf es eine der Linux-Varianten sein. Im Dialog für das Formatieren des Containers bewegen Sie die Maus einige Zeit zufällig hin und her, bevor Sie auf „Format“ drücken. Nachdem Sie den Hinweis erhalten haben, dass der Container erfolgreich angelegt wurde, kann er eingesetzt werden.

Dazu klicken Sie im Programmfenster von Truecrypt auf „Select File“. Im nachfolgenden Dialog wählen Sie Ihren Container aus. Jetzt gelangen Sie zum Programmfenster zurück. Klicken Sie dort auf „Mount“. Sie werden dazu aufgefordert, das Passwort einzugeben, das Sie bei der Anlage des Containers vergeben haben. Damit wird der Container geöffnet. Er befindet sich im Da- ›



Encfs – ideal für Daten im Cloud-Speicher: Mit der richtigen Software wird der Umgang mit verschlüsselten Dateisystemen wirklich einfach.

teimanager in der Rubrik „Wechseldatenträger".

Wenn Sie später Ihre Arbeit mit den Dateien beenden, wechseln Sie in das Programmfenster zurück und klicken dort auf „Dismount".

Cloud-Speicher mit encfs absichern

Die jüngsten Berichte über belauschten Datenverkehr im Web sollten hellhörig machen: Sie zeigen, dass von der unbefugten Einsicht in seine Daten wirklich jeder Nutzer betroffen sein kann, der einen Cloud-Dienst nutzt. Wenn Sie auf Ihrem Linux-System Dropbox, Google Drive oder Ubuntu One verwenden, ist es mehr als empfehlenswert, die dort gespeicherten Daten zu verschlüsseln. Als Alternative zu Containern bietet sich hier etwa die direkte Verschlüsselung ganzer Verzeichnisse an. Dokumente und Dateien, die etwa ohnehin aus öffentlichen Quellen stammen und die Sie gern mit anderen teilen wollen, legen Sie einfach uncodiert in der Cloud ab, vertrauliche Informationen hingegen in ein verschlüsseltes Verzeichnis, das weder der Cloud-Betreiber noch unbefugte Dritte einsehen können.

Für diese Aufgabe bietet sich das Encrypted Filesystem (encfs) an. Das verschlüsselte Dateisystem arbeitet nach einem leicht verständlichen Prinzip. Mit einer Software wird das Verzeichnis im Cloud-Speicher verschlüsselt. Dieselbe Software, die für die Ver- und Entschlüsselung genutzt wird, bindet das verschlüsselte Verzeichnis auf Ihrem System wie einen externen Datenträger ein. Darüber können Sie auf Ihrem System im Klartext sehen, was sich in dem Verzeichnis befindet, und Sie öffnen die dort gespeicherten Dateien ganz so, als wenn diese nicht verschlüsselt wären. Auf dem Cloud-Server landen dagegen nur die augenscheinlich unleserlichen Dokumente. Die Verschlüsselung kann direkt auf der Kommandozeile ausgeführt werden.

Aber es gibt auch komfortable grafische Alternativen: Starten Sie unter Ubuntu das Software-Center, und suchen Sie dort nach der Software encfs, und installieren Sie das Programm. Für noch mehr Komfort sorgt der zusätzliche gnome-encfs-manager.

Damit können Sie bereits daran gehen, etwa in der Dropbox ein verschlüsseltes Verzeichnis zu verwenden. Unter Ubuntu suchen Sie in der Dash nach „Gnome Encfs Manager" und starten das Programm. Die Software legt einen Eintrag in den Systemabschnitt der oberen Kontrollleiste ab. Mit einem Rechtsklick auf das Programmsymbol rufen Sie das Kontextmenü auf und wählen dort „Manager zeigen". Klicken Sie auf das Pluszeichen, um einen neuen „Stash" anzulegen. Damit bezeichnet die Software einen verschlüsselten Datenspeicher. Im nachfolgenden Fenster klicken Sie im oberen Teil das Optionsfeld neben der Eingabezeile an und anschließend das Ordnersymbol. Darüber navigieren Sie in Ihre Dropbox und legen dort einen neuen Ordner an. In diesem Verzeichnis landen Ihre verschlüsselten Daten.

In der zweiten Eingabezeile navigieren Sie in ein Verzeichnis in Ihrem Benutzerordner und vergeben einen sprechenden Namen, damit Sie sich merken können, dass sich dort die entschlüsselten Daten befinden. Anschließend vergeben Sie ein Passwort in den beiden vorgesehenen Feldern. Mit „Erstellen" legen Sie das verschlüsselte Verzeichnis an. Das Verzeichnis wird nun sofort eingehängt und ist damit einsatzbereit. Wenn Sie darin Dateien ablegen und sich die Infos der Dropbox-Software ansehen, werden Sie sofort bemerken, dass nur „unleserliche Zeichenfolgen" synchronisiert werden. Mit dem Manager können Sie beliebig viele solcher Verzeichnisse anlegen. Wichtig ist nur, dass Sie das verschlüsselte Verzeichnis wieder aushängen, wenn Sie Ihre Arbeit beendet haben.

Encfs-Verschlüsselung für Windows und Android

Die größere Sicherheit, die Sie durch den Einsatz von encfs bei der Nutzung von Diensten wie Dropbox oder Google Drive gewinnen, können Sie auch mit Android-Tablets oder mit Ihrem Windows-PC behalten. Für beide Plattformen gibt es Programme, die Ihnen beim Einbinden eines verschlüsselten Verzeichnisses helfen. Für Windows finden Sie encfs4win unter *http://members.ferrara.linux.it/freddy77/encfs.html.* Das Archiv enthält neben

Gnome Encfs Manager: Das Tool sollten Sie unbedingt installieren, weil der Manager Übersicht und Bedienung deutlich vereinfacht.

einem Werkzeug für die Kommandozeile auch einen grafischen Aufsatz. Üblicherweise müssen Sie vor der Installation noch die „Dokan Library“ installieren. Nutzen Sie dazu am besten den Link auf der Seite des Entwicklers. Die grafische Oberfläche nistet sich als Symbol im Systemtray unter Windows ein. Mit zwei Mausklicks binden Sie dann das verschlüsselte Verzeichnis wie ein externes Laufwerk ein.

Möchten Sie auf einem Android-Gerät auf Ihren verschlüsselten Datenspeicher zugreifen, laden Sie sich einfach die App Cryptonite, die Sie im Google Store finden.

Homeverzeichnis (nachträglich) verschlüsseln

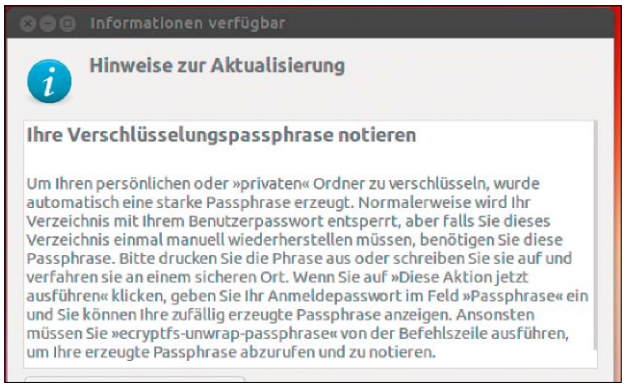
Es ist für einen geübten Dieb oder Hacker keine große Sache, um auf die Daten in einem Benutzerverzeichnis eines gestohlenen Linux-Rechners zuzugreifen. Zuverlässigen Schutz gegen solche Einbrüche bietet nur ein verschlüsseltes Benutzerverzeichnis. Denn ohne das Passwort, das für die Verschlüsselung verwendet wurde, kann der Hacker nicht auf die Daten zugreifen.

Ubuntu bietet dem Anwender während der Installation an, das Benutzerverzeichnis vollständig zu verschlüsseln. Diese Verschlüsselung ist aber auch noch nachträglich möglich.

Doch Achtung: Es gibt Anwender, die auf diesem Wege alle Daten verloren haben. Der Grund dafür ist, dass manche kursierende Anleitung darauf basiert, das System im Wiederherstellungsmodus als Benutzer „root“ zu starten. Auf der Konsole werden dann die Daten eines Anwenders verschoben, der Nutzer gelöscht und wieder neu angelegt. Leider taucht aber immer wieder ein Bug in diesem Zusammenhang auf, so dass im schlimmsten Fall alle Daten verloren sind.

Risikoloser ist folgende Methode:

1. Loggen Sie sich auf dem System ein. Starten Sie den Dateimanager, und lassen Sie sich alle Dateien, auch die versteckten, über das Menü „Ansicht“ anzeigen. Kopieren Sie die Daten auf einen externen Datenträger.



Home-Verzeichnis verschlüsseln: Nach der Umstellung eines Benutzerverzeichnisses werden Sie von Ubuntu mit diesem Hinweis begrüßt.

2. Öffnen Sie dann ein Terminal, und geben Sie dort folgenden Befehl ein:

```
adduser --encrypt-home <Benutzer2>
```

Sie werden aufgefordert, ein Passwort für den neuen Benutzer anzugeben. Bei der Variablen <Benutzer> handelt es sich um den Anmeldenamen. Die Angaben zum vollständigen Namen können Sie später noch nachholen. Legen Sie also einen neuen Benutzer an, der Ihrem ursprünglichen Benutzernamen ähnelt, also zum Beispiel „Benutzer2“, wenn Ihr Anmeldename vorher „Benutzer“ lautete.

3. Mit dem Befehl

```
adduser <Benutzer2> sudo
```

verleihen Sie dem neuen Nutzer den Status eines Administrators.

4. Jetzt können Sie sich erstmals als diesen neuen Nutzer einloggen. Sie erhalten einen Hinweis über die „Verschlüsselungsphrase“. Diese sollten Sie sich mit „Diese Aktion jetzt ausführen“ unbedingt nach Eingabe Ihres Passworts im Terminal ansehen und vor allen Dingen an einem sicheren Ort aufbewahren. Im Zweifel ist diese Passphrase in Form einer hexadezimalen Zeichenfolge bei einem Systemproblem die einzige Möglichkeit, wieder an Ihre Daten zu gelangen.

5. Rufen Sie als neuer Nutzer in den Systemeinstellungen von Ubuntu die Verwaltung der Benutzer auf, und kontrollieren Sie den Status des Kontentyps. Dieses sollte auf „Verwalter“ lauten. Öffnen Sie nun erneut ein Terminal und geben Sie dort folgendes ein:

```
sudo usermod -l <Benutzer3>
 <Benutzer>
```

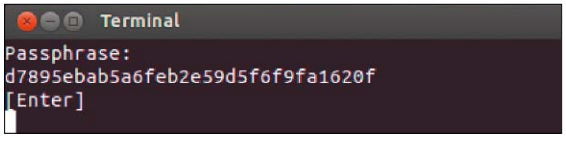
Damit geben Sie Ihrem ersten Benutzer einen neuen Namen. Um im Beispiel zu bleiben, können Sie den Namen also jetzt um die Ziffer „3“ ergänzen. Aus „Benutzer“ wird jetzt also „Benutzer3“.

6. Melden Sie sich jetzt wieder ab, und loggen Sie sich als erster Benutzer ein, den Sie ja gerade umbenannt haben. Wiederholen Sie jetzt das gerade ausgeführte Kommando, und geben Sie dem zweiten Benutzer auf diese Weise Ihren ursprünglichen Anmeldenamen. Aus „Benutzer2“ wird also jetzt wieder „Benutzer“. Melden Sie sich ab und erneut wieder mit dem jetzt ursprünglichen Benutzernamen an, dessen Nutzer jetzt aber über ein verschlüsseltes Home-Verzeichnis verfügt.

Als dieser Benutzer kopieren Sie sich mit Nautilus jetzt von der externen Sicherung alle Dateien zurück. Wenn Sie eine Weile mit dem System gearbeitet haben und es keinen Zweifel mehr gibt, dass die ganze Aktion problemlos funktioniert hat, können Sie auf der Konsole den alten, funktionslosen „Benutzer“ samt Benutzerdaten mit

```
deluser --remove-home <Benutzer>
```

vollständig löschen.



Schlüssel für den Notfall: Im Terminal geben Sie zunächst Ihr Benutzerpasswort ein und erhalten anschließend die hexadezimale Passphrase, die Sie unbedingt gut aufbewahren sollten.