Computer verschlüsseln

Hier erfährst du:

- Wie du dein System / deinen Computer verschlüsseln kannst unter Linux, Windows und MAC
- Welche Vorbereitung vor der Verschlüsselung wichtig sind (Backup!)
- Argumente warum Verschlüsselung des Systems viele Sicherheitslücken schließt.
- Was das portable sichere Betriebssystem TAILS für dich tun kann!

Warum ich mein System verschlüsseln sollte

- Weil du mit Verschlüsselung dich und auch andere schützen kannst.
- Weil du es damit Repressionsbehörden und allen anderen die an deine Daten wollen so schwer wie möglich machst. Auch wenn du denkst, dass du nichts „Problematisches“ auf deinem Computer hast: Wenn Verschlüsselung weit verbreitet ist, kann das auch die Leute schützen, die vielleicht berechtigterweise „etwas zu verbergen“ haben.
- Weil auf einem verschlüsselten Computer/Betriebssystem nicht nur deine Daten, sondern auch die Daten von installierten Programmen geschützt sind: Chatverläufe, Browserhistory, Bearbeitungsgeschichten von Dokumenten, … .
- Weil auf deinem Computer so viele Daten abgespeichert sind, dass mensch selbst kaum mehr Überblick hat (denke etwa an die berühmten „Cookies“).
- Weil deine Privatsphäre geschützt ist: Wird dein Computer gestohlen oder geht verloren, wenn du ihn verkaufst oder verschenkst oder er geht einfach kaputt und funktioniert nicht mehr: Niemand kann ansehen, was du auf dem Computer gespeichert oder gemacht hast.

Lies dir doch auch unser Plädoyer für das Verschlüsseln deines Computers durch.

Anleitungen

Empfehlenswert: Broschüre „beschlagnahmt“
Unsere Anleitungen sind von anderen Quellen zusammengeklau(b)t, verändert und selber geschrieben. Hingewiesen sei hier auf die allgemein ziemlich coole Broschüre beschlagnahmt und besonders auf einen Artikel darin zum Thema Dateien verschlüsseln.

Vorbereitung

o Passwortsicherheit beachten
Die beste Verschlüsselungstechnologie nützt dir nichts, wenn das Passwort das du wählst leicht zu knacken ist. Ein vier-stelliges Zahlenpasswort z.B. benötigt lediglich Minuten, um es durch einen Computer und entsprechende Software knacken zu lassen. Aber auch (scheinbar) komplizierte Passworte sind ein Risiko, weil du es entweder vergisst oder aufschreiben musst.

Lies dir unsere Tipps zum Thema durch, damit du dir Passworte zulegen kannst, die einfach zu merken und sehr sicher sind.

o Backup machen
Bevor du deinen Computer und deine Daten verschlüsselst, solltest du deine Daten sichern, also ein sogenanntes Backup machen.

Ein sicheres Backup sollte verschlüsselt sein.
Weil wo ist der Sinn, wenn der Computer verschlüsselt ist, aber du eine Datensicherung auf einer unverschlüsselten Festplatte in der Schublade liegen hast?

Daher haben wir zum Thema Datensicherung und Backup einen eigenen Artikel geschrieben.

Linux (Debian, Ubuntu und co.)

Verschlüsselung mit Neuinstallation verbinden.
Linux ist die Basis für viele Betriebssyteme. Du hast vielleicht Debian, Ubuntu, Linux-Mint oder eine andere Variante (Distribution). Zwischen den Distributionen kann es Unterschiede geben in der Art wie die Verschlüsselung eingerichtet wird und bei fast allen kann die Verschlüsselung auch mit etwas Aufwand auf einem bestehenden System eingerichtet werden. Einfachheitshalber empfehlen wir, eine Neuinstallation deines Betriebssystems durchzuführen und die Verschlüsselung von Grund auf einzurichten. Mit den meisten Linux-Distributionen wirst du bei der Neuinstallation von einem Assistent durch die vollständige und sichere Verschlüsselung geführt.

Beispielhaft steht für eine Linux-Installation Ubuntu. Andere Distributionen können (leicht) davon abweichen.

⇒ Installationsprozess starten
⇒ Im Fenster “Art der Installation” einen Haken bei “Encrypt the new Ubuntu installation for security” setzen und weiter zum nächsten Schritt
⇒ Passwort eingeben (siehe dazu Kapitel „Passwortsicherheit“)
⇒ Haken bei “Overwrite empty disk space” setzen
⇒ Mit “Install Now” die eigentliche Installation starten.

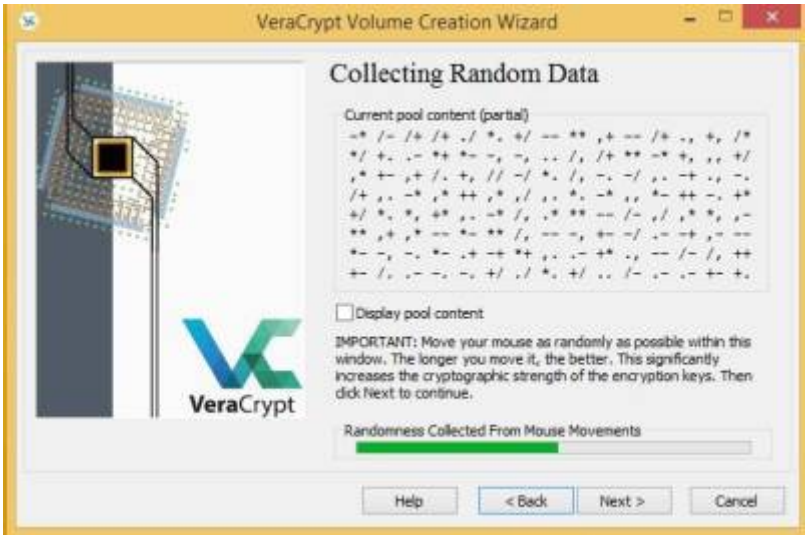
Basic Security Tips for Linux/Ubuntu by "security in a box" [english] Ausführliche Tipps und Anleitungen für Sicherheitseinstellungen in Ubuntu [englisch].

Windows via VeraCrypt

Zur Verschlüsselung von Windows-Computern und externen Datenträgern empfehlen wir Veracrypt. Veracrypt ist OpenSource und funktioniert sowohl auf Linux, Windows als auch auf MacOS.

⇒ VeraCrypt installieren und starten
⇒ “Create Volume” klicken
⇒ “Encrypt the system partition” anwählen und “Next” klicken
⇒ “Normal” anwählen, “Next”
⇒ “Encrypt the whole drive”
⇒ Single- oder Multiboot auswählen. Wenn du nicht weißt worum es geht wähle einfach ersteres

⇒ Algorithmen auswählen (AES und SHA-256 sind in Ordnung)
⇒ Passwort eingeben (siehe dazu Kapitel „Passwortsicherheit“)
⇒ Die Maus möglichst zufällig durch das Fenster bewegen bis der grüne Balken voll ist, dann “Next”
⇒ “Next”
⇒ Entsprechend der Anweisungen eine Rescue Disk erstellen. Wenn du kein CD-Laufwerk hast, kannst du auch einen USB-Stick verwenden. Mit der CD bzw. dem USB-Stick kannst du das System nicht wiederherstellen, wenn du dein Passwort vergessen hast. Sie dienen nur dazu das System zu retten falls Dateien beschädigt wurden, die VeraCrypt zum entschlüsseln benötigt. Du solltest den Datenträger also gut aufbewahren, aber falls die Cops ihn kriegen sind deine Daten trotzdem noch sicher.



Durch willkürliche Mausbewegung werden Zufallsdaten für die Verschlüsselung erzeugt.

⇒ “1-Pass” Wipemode auswählen
⇒ “Test” klicken. Der Rechner wird nun neustarten und du kannst dich das erste Mal mit deinem Passwort anmelden. Wenn ein “PIM” verlangt wird, drücke einfach Enter. Wenn alles funktioniert hat, kann es weitergehen.
⇒ VeraCrypt sollte sich automatisch gestartet haben. Jetzt auf den Button “Encrypt” klicken.
⇒ Notfallanweisungen lesen, ggf. drucken und mit “Ok” bestätigen
⇒ Abwarten bis alles verschlüsselt ist.

Tastaturlayout kann sich ändern!
Achtung beim Hochfahren/Entschlüsseln des Computers: Beim Passwort eingeben ist die Tastatur möglicherweise auf US-Tastaturlayout gestellt. Achtet also beim Eingeben von Sonderzeichen oder Buchstaben wie *y* oder *z* darauf.

Mac und Windows

Die Windows und Mac Verschlüsselungen sind so genannte proprietäre Software, d.h. sie sind nicht offen einsehbar und im Gegensatz zu OpenSource-Software ist vieles darin nicht nachvollziehbar. Diese Firmen haben im Moment aber auf jeden Fall ein starkes Interesse gute Verschlüsselungslösungen zu unterstützen und anzubieten.

Apple MAC: FileVault2

Apple stellt für seine (neueren) MAC-Betriebssysteme Verschlüsselung mit dem Namen FileVault2 zur Verfügung. Apple bietet dafür gute Anleitungen und beschreibt auch mit welchen Betriebssystemen die Verschlüsselung möglich ist. Link zur Anleitung von Apple Dein Passwort das du bisher für deinen Login verwendet hast, ist auch dein Verschlüsselungspasswort. Es wird kein extra Passwort benötigt. Wie immer gilt: Wähle ein sicheres Passwort. Es gibt auch Veracrypt für Mac, führt aber manchmal zu Problemen, darum können wir das leider nicht uneingeschränkt empfehlen.

Microsoft Windows: Bitlocker (Windows 10 Pro, Windows 11)

Microsoft bietet eine Geräteverschlüsselung für die meisten seiner Betriebssysteme an und auch eine weitergehende Verschlüsselung über Bitlocker. Du kannst direkt die Anleitung auf der Seite von Microsoft verwerden.

Dein Passwort das du bisher für deinen Login verwendet hast, ist auch dein Verschlüsselungspasswort. Es wird kein extra Passwort benötigt.

Wie immer gilt: Wähle ein sicheres Passwort! Wir empfehlen trotz der von Microsoft angebotenen Möglichkeiten die Festplattenverschlüsselung mit Veracrypt, wie bereits oben beschreiben. Aber auch eine Bitlocker-Verschlüsselung ist besser als keine!

Tails - Das Sichere Betriebssystem auf dem USB-Stick

Tails ist ein sicheres Betriebssystem für die Hosentasche und das du einfach an einen Computer angestecken und starten kannst. Auf Tails sind viele auf diesem Wiki beschriebenen Programme bereits installiert sind und zahlreiche Sicherheitslösungen bereits eingebaut.

Wir stellen Tails in einem eigenen Artikel vor, wo du mehr Informationen findest.

Tails macht in vielen Situationen Sinn:

- Wenn du keinen Computer hast.
- Wenn du den Computer den du nutzt nicht nach sicheren Standards einrichten kannst.
- Wenn du Zweifel an der Sicherheit der Computer hast die du nutzt.
- Wenn du deine Arbeitsmittel und Daten gerne auf sichere Weise mit dir herumtragen magst.
- Wenn du sicher und anonym arbeiten willst, auch wenn es nicht immer bequem ist.

Zum Weiterlesen - Links und Empfehlungen

- Broschüre All Computers are Beschlagnahmt. Wie sichere ich meine Daten vor Einsicht durch die Behörden?. Aus dieser Quelle haben wir auch einiges für dieses Wiki herauskopiert! Danke!

- What you should know about encryption [english]
- How you set up Linux encrypted [english]