

Laptop / PC Verschlüsselung

- **Windows** und **MacOS** bieten mittlerweile Verschlüsselung;
 - aber: nicht open-source, kann teilweise durch iCloud etc. umgangen werden
- **Linux**: Verschlüsselung mit Best Practices nach heutigem Stand nicht knackbar, aber: muss manuell bei Installation ausgewählt werden

Co

min

Install

Install (as superuser)

Installation type

This computer currently has Linux Mint 19.1 Tessa (19.1) on it. What would you like to do?

☐

Erase Linux Mint 19.1 Tessa (19.1) and reinstall

Warning: This will delete all your Linux Mint 19.1 Tessa (19.1) programs, documents, photos, music, and any other files.

☐

Erase disk and install Linux Mint

Warning: This will delete all your programs, documents, photos, music, and any other files in all operating systems.

☐

Encrypt the new Linux Mint installation for security

You will choose a security key in the next step.

☐

Use LVM with the new Linux Mint installation

This will set up Logical Volume Management. It allows taking snapshots and easier partition resizing.

☒

Something else

You can create or resize partitions yourself, or choose multiple partitions for Linux Mint.

Quit

Back

Continue

Verschlüsselung

2

[Done](#) [Help!](#)

Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

20 GiB

**ATA QEMU HARDDISK**

sda / 20 GiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

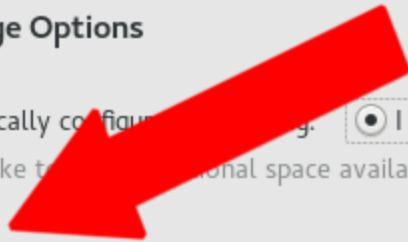
[Add a disk...](#)*Disks left unselected here will not be touched.*

Other Storage Options

Partitioning

☐ Automatically configure partitioning. ☒ I will configure partitioning.☐ I would like to use the maximum available space available.

Encryption

☒ Encrypt my data. You'll set a passphrase next.



Preparation

- ✓ Network Autoseup
- ✓ Installer Update
- ✓ Repositories Initialization
- ✓ Welcome
- ✓ Network Activation
- ✓ System Analysis
- ✓ Online Repositories
- ✓ Add-On Products

→ Disk

- Time Zone
- User Settings

Installation

- Installation Overview
- Perform Installation

Release Notes...

Suggested Partitioning

Initial layout proposed with the default Guided Setup settings.

Changes to partitioning:

- Create GPT on /dev/sda
- Create partition /dev/sda1 (8.00 MiB) as BIOS Boot Partition
- Create partition /dev/sda2 (37.99 GiB) for / with btrfs
- Create partition /dev/sda3 (2.00 GiB) for swap
- 9 subvolume actions ([see details](#))

Guided Setup

Expert Partitioner ▼

Help

Abort

Back

Next

Partitioning Scheme

☒ Enable Logical Volume Management (LVM)

☒ Enable Disk Encryption

Password

●●●●●●●●

Verify Password

●●●●●●●●

Passwörter

- Passwörter können durch eine sogenannte Dictionary-Attack angegriffen werden.
=> Keine Wörter in Passwörtern, sondern zufällige Zeichen

password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
	Instantly	Instantly	-	-
	Instantly	Instantly	Instantly	-
	Instantly	Instantly	Instantly	Instantly
	Instantly	Instantly	Instantly	Instantly
	Instantly	Instantly	Instantly	Instantly
	Instantly	Instantly	Instantly	Instantly
	Instantly	Instantly	1 min	6 min
	Instantly	22 min	1 hrs	8 hrs
	2 min	19 hrs	3 days	3 wks
	1 hrs	1 mths	7 mths	5 yrs
	1 day	5 yrs	41 yrs	400 yrs
	3 wks	300 yrs	2,000 yrs	34,000 yrs

Secure Boot

- Secure Boot verhindert den Systemstart, wenn etwas an eurem Bootloader verändert wurde.
- Wird nur von manchen, großen Distributionen unterstützt.
 - Debian, Ubuntu, SUSE, Fedora
- Wollt ihr eine andere Distribution benutzen, müsst ihr Secure Boot im BIOS ausschalten

- Deaktiviert Option für Entschlüsselung über iCloud
- Passwort **nicht** verlieren, kann auf neuen Macs nicht ohne weiteres zurückgesetzt werden!

iOS

- Verschlüsselung ist Standard und allgemein sicher
- ABER: iCloud-Backups sind für Cops einfach zugänglich
=> iCloud-Backups deaktivieren
- (und iPhones sind teuer)

Android

- Verschlüsselung ist seit Android 3 verfügbar
- Bei manchen Herstellern standardmäßig an, manchmal muss Verschlüsselung in den Geräteeinstellungen angeschaltet werden