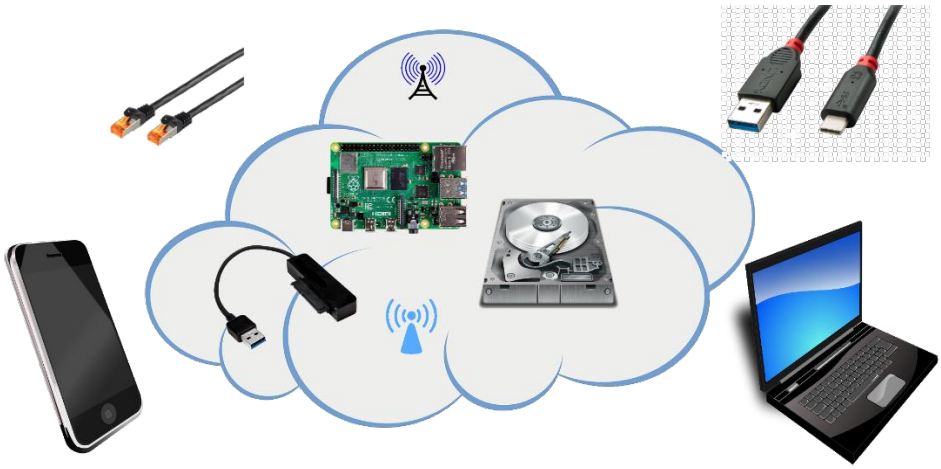


08.09.2021

Inhalt dieses Tutorials

1.0.0 Hard-und Software
1.1.0 Benötigte Hardware
1.2.0 Benötigte Software
1.3.0 Installation Betriebssystem
1.3.1 Image auf die SD-Karte schreiben mit Win32DiskImager
1.3.1.1 Image auf die SD-Karte schreiben mit Raspberry Pi Imager (bevorzugt)
1.3.2 SSH-Zugriff aktivieren
1.4.0 Erster Start und Grundeinstellungen
1.4.1 neuen Standarduser anlegen
1.4.2 Root Passwort vergeben
1.4.3 User Pi deaktivieren
1.4.4 Software updaten
1.4.5 Grundeinstellungen
1.5.0 Absicherungsmöglichkeiten
1.5.1 SSH-Zugriff absichern
1.5.1.1 Root-Login verbieten
1.5.1.2 SSH-Public Key Authentifizierung

1.0.0 Hard- und Software

1.1.0 Was benötige ich an Hardware?

- Einen Raspberry Pi (Empfehlung von mir Raspberry Pi 4 Modell B 4 GB Ram)
- Original Raspberry Pi 4 Netzteil mit USB-C Anschluss und 5.1V,3A
- Eine Micro-SD Karte mindestens 8GB (Empfehlung 16 GB)
- Ein LAN-Kabel zum Anschluss an den Router

1.2.0 Welche Software wird benötigt?

- Raspberry Pi Imager Raspberry Pi Imager
- Ein Tool zum Aufbauen einer SSH-Verbindung mit eurem Raspberry Putty

1.3.0 Installation des Betriebssystems

Vorbereitung

Als erstes ladet ihr euch die erforderliche Software herunter.
Installiert die Programme Raspberry Pi Imager und Putty.

1.3.1 SD-Karte installieren mit Raspberry Pi Imager

Die einfachste Methode ist das flashen der SD-Karte mit dem Raspberry Pi Imager
Es muss kein Image vorab heruntergeladen werden.

Vorgehensweise:
Den Imager von der Webseite raspberrypi.org herunterladen und installieren.
Den Imager starten, das gewünschte Betriebssystem auswählen.
Empfehlung Bei Nutzung eines Monitors oder einem VNC-Viewer Raspberry Pi OS
Wenn der Pi ohne Monitor oder VNC-Viewer genutz wird, reicht Raspberry Pi OS Light
(zu finden unter (Raspberry Pi OS (other))
Die SD-Karte auswählen
Mit der Tastenkombination Strg+Shift und x erreicht ihr ein weiteres Menü in dem ihr den ssh-Zugang aktivieren, einen anderen Hostnamen erstellen, ein anderes Passwort erstellen, WIFI aktivieren sowie die Spracheinstellungen ändern könnt.
Nach Klick auf den Button <write> wird das ausgewählte Image automatisch heruntergeladen und auf die SD-Karte oder SSD geflasht.
Nach erfolgreichem Schreiben und verifizieren wird die SD/SSD automatisch „ausgeworfen“

Nun könnt ihr die SD-Karte aus dem Kartenleser entfernen.

1.4.0 Erster Start und Grundeinstellungen

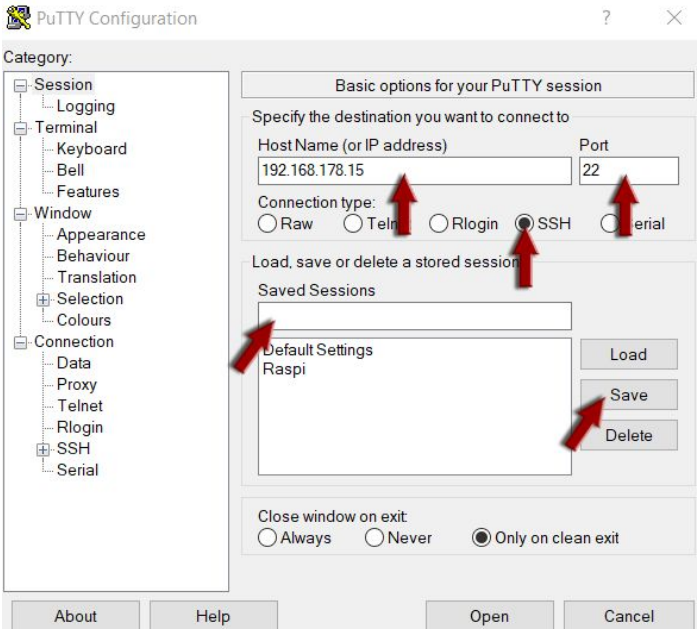
Jetzt steckt ihr die SD-Karte in den Raspberry Pi, verbindet diesen per LAN-Kabel mit eurem Router und schließt das Netzteil an.
Jetzt bootet der Raspi automatisch. Lasst ihm für den ersten Start 2-3 Minuten Zeit.
Als nächstes solltet ihr die IP-Adresse in Erfahrung bringen, die eurem Pi vom Router zugeteilt wurde.
Dazu öffnet ihr die Konfigurationsseite eures Routers. In meinem Fall eine Fritz Box.
Unter Netzwerk müsste euch euer Pi als „raspberrypi“ mit der vergebenen IP-Adresse angezeigt werden.
Diese solltet ihr, wenn möglich in den Einstellungen so einstellen, dass immer die gleiche IP-Adresse vergeben wird. In der Fritz Box und vielen anderen Routern ist das möglich.

Diese IP-Adresse merkt ihr euch nun.
Das Router Fenster könnt ihr nun schließen.
Alternativ könnt ihr die IP auch über die Eingabeaufforderung (cmd) herausfinden.
Öffnet die Eingabeaufforderung mit der Windows-Taste und R und gebt cmd ein. In der Eingabeaufforderung gebt ihr nun den Befehl ein

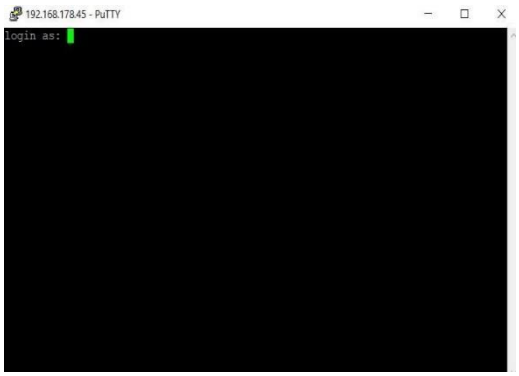
ping -4 Hostname Sofern ihr den Hostnamen beim flashen mit dem Imager nicht geändert habt, lautet er raspberrypi
Jetzt wird euch die IP-Adresse angezeigt.

Startet nun das Programm „Putty

In folgendem Fenster gebt ihr die IP-Adresse eures Pi ein, wählt den Port 22 und als „Connection type“ SSH.
Damit die Daten nicht immer neu eingegeben werden müssen, gebt ihr unter „Saved sessions“ einen Namen für die Verbindung ein und klickt auf „Save“
Diese Verbindung erscheint jetzt im unteren Fenster. Diese könnt ihn nun jederzeit laden und mit „open“ oder einfach per Doppelklick auf den Namen öffnen

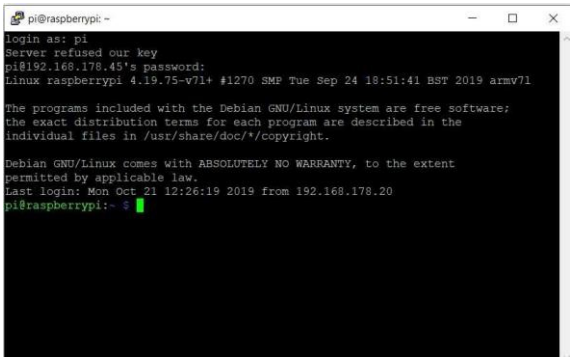


Nun öffnet sich das Terminal von Putty



Hier gebt ihr nun den Benutzer ein (Standard ist pi) und drückt auf <ENTER>.
Dann wird nach dem Passwort gefragt. (Standard ist raspberry) sofern nicht im Imager geändert Dieses gebt ihr ebenfalls ein und bestätigt mit <Enter>

Hinweis!
Im Terminal gibt es bei einer Passworteingabe keine Rückmeldung. Das heißt, ihr könnt diese Eingabe nicht sehen, keine Sternchen oder Punkte …. und der Cursor bewegt sich auch nicht weiter. Das ist normal und gilt für jede Passworteingabe.



Nach der Eingabe drückt ihr wieder <ENTER> und ihr seid eingeloggt.

Da der Standard-User pi und das Passwort jedem potenziellen Angreifer bekannt ist, solltet ihr jetzt einen neuen Standard-User anlegen, und den User pi nebst Passwort deaktivieren.

Das ist zwar nicht zwingend erforderlich, erhöht aber die Sicherheit.
Wenn ihr den User pi behalten wollt, dann benutzt aber ein sicheres Passwort.

1.4.1 Neuen Standard-User anlegen

Gebt dazu folgenden Befehl ein

```
sudo useradd -m username
```

Erklärung des Befehls.
Mit „sudo“ wird der nächste Befehl mit Root-Rechten ausgeführt. Das werden wir aber gleich noch ändern. (alle Befehle, die ins System eingreifen, müssen mit Root-Rechten ausgeführt werden) Der Parameter „-m“ fügt automatisch ein Homeverzeichnis hinzu. „username“ müsst ihr auf euern neuen Usernamen ändern.

Jetzt weist ihr dem neuen User ein Passwort zu

Bitte tut euch selber einen Gefallen und verwendet keine 0815-Passwörter

```
sudo passwd username
```

Mit dem folgenden Befehl fügt ihr den neu erstellten User der Gruppe „users“ hinzu.

```
sudo usermod -g users username
```

Damit habt ihr einen User angelegt, der zur Gruppe „users“ gehört und keinerlei Root-Rechte hat und auch **keine** sudo-Befehle ausführen kann.
Wie ihr euch mit dem User trotzdem als „root“ anmelden könnt, erkläre ich jetzt.

1.4.2 Root-Passwort vergeben.

Da der user „root“ noch kein Passwort hat, müsst ihr jetzt ein Root-Passwort vergeben, sonst könnt ihr euch später nicht mehr als „root“ anmelden.

Dieses Passwort sollte besonders sorgfältig ausgewählt werden und sich vom Userpasswort erheblich unterscheiden, da der Root-Benutzer alle Rechte besitzt und großen Schaden anrichten kann. Dieses Passwort sollte auch nur der „Administrator“ kennen.

Gebt also folgenden Befehl ein.

```
sudo passwd root
```

wie immer 2x das Passwort blind eingeben.

Jetzt solltet ihr Putty schließen und euch danach mit eurem neuen Usernamen anmelden.
Ihr könnt euch jetzt als Root anmelden, indem ihr den Befehl

```
su
```

eingebt, gefolgt von dem Root-Passwort, welches ihr gerade angelegt habt.

1.4.3 User-Konto „pi“ deaktivieren

Da ihr jetzt ein neues User-Konto besitzt, und euch damit anmelden könnt, und euch mit „su“ als root anmelden könnt, solltet ihr jetzt den Standard-User „pi“ deaktivieren.

Jetzt könnt ihr mit

```
usermod -L pi
```

und

```
passwd -l pi
```

Den User pi und das Passwort von pi deaktivieren.
Der User pi hat jetzt keine Rechte mehr und kann sich auch nicht mehr einloggen.
Für interne Prozesse (auch Cronjobs) kann der Benutzer noch weiterhin verwendet werden.

1.4.4 Software updaten

Wie bei jedem anderen Computer ist es auch beim Raspi wichtig, das System aktuell zu halten, um eventuelle bekannte Sicherheitslücken zu schließen und die Software auf dem neuesten Stand zu halten.

Denkt bitte daran, dass ihr für alle Installationen als „root“ angemeldet sein müsst, sonst ist eine Installation nicht möglich.

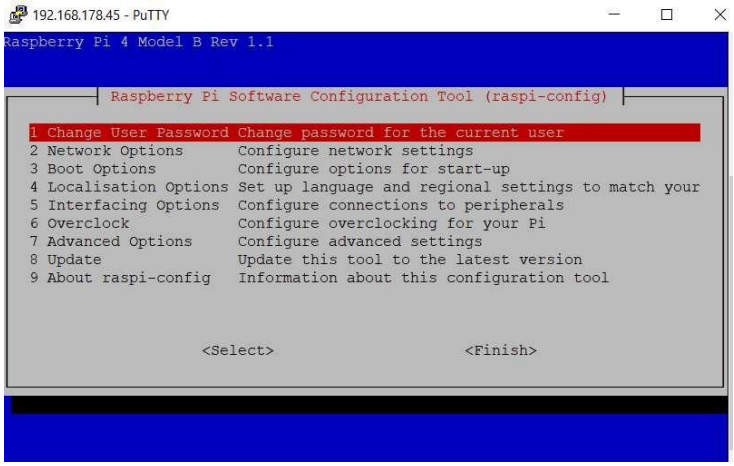
Gebt den folgenden Befehl ein und bestätigt mit ENTER.

```
apt update && apt full-upgrade -y
```

1.4.5 Grundeinstellungen

```
raspi-config
```

Es öffnet sich nun folgendes Fenster.



Unter Punkt 1 könntet ihr ebenfalls das Passwort des angemeldeten Users ändern, aber das habt ihr ja eben schon gemacht.
Unter Punkt 2 könnt ihr euer Wlan aktivieren und eure Zugangsdaten eingeben, falls ihr das nicht schon mit dem Imager aktiviert habt.

Bei einer Nutzung des Pi als
Cloudserver würde ich eine Verbindung per LAN-kabel bevorzugen, da der Pi 4 Gbit-Lan unterstützt.

Außerdem schafft ihr euch durch die Aktivierung des Wlans eine erneute Schwachstelle.
Wenn ihr das Wlan nicht unbedingt benötigt, lasst es abgeschaltet. Ebenso
verhält es sich mit Bluetooth.

Unter Punkt 4 solltet ihr jetzt die Regionalen Einstellungen vornehmen.
Ihr wählt Punkt 4, im nächsten Fenster den ersten Punkt (change locale) und wählt anschließend mit den Pfeil -Tasten die Einstellung de_DE.UTF-8 UTF-8

markiert die Einstellung mit der Leertaste wechselt mit der TAB-Taste auf ok und bestätigt mit ENTER.
Anschließend noch einmal die Einstellung de_DE... auswählen und bestätigen. Dann
kommt ihr wieder zurück auf die Hauptseite.

1.5.0 Absicherungsmöglichkeiten für euren Raspi

Eine 100% Absicherung für euren Raspi wird es nicht geben. Die gibt es nicht bei Windows, die gibt es nicht in einer öffentlichen Cloud oder wo auch immer. Immer wieder tauchen hier und da Sicherheitslücken auf, die geschlossen werden müssen. Aber ihr könnt es einem potenziellen Angreifer schwerer machen.

1.5.1 SSH absichern

Ändert euren SSH-Port von 22 auf einen möglichst 5-stelligen. Möglich bis 65536. Das ist zwar auch kein 100% Schutz, aber für manchen Hobby -Angreifer schon eine Schwelle. Einzustellen in der Datei (/etc/ssh/sshd_config.) Den Standardport 22 umschreiben und die Raute am Anfang löschen. Anschließend mit „service ssh restart“ neustarten.

1.5.1.1 Root-Login verbieten

Standardmäßig ist der Root-Login nicht erlaubt. Solltet ihr ihn dennoch einmal eingeschaltet haben, solltet ihr ihn wieder abschalten.

```
nano /etc/ssh/sshd_config
```

“Permit Rootlogin“ auf “no” setzen Datei speichern und schließen.

1.5.1.2 SSH-Zugang nur mit einer Public Key-Authorisierung

Das heißt, es wird ein Schlüsselpaar erstellt wobei sich der eine Teil auf eurem Pi und der zweite Teil auf eurem Rechner befindet.
Ein Einloggen per SSH ist dann nur noch mit dem entsprechenden Schlüssel möglich.
Dabei geht ihr folgendermaßen vor.
Macht als erstes ein Backup von eurer SD-Karte und verwahrt dieses gut auf.
Ihr loggt euch per ssh als User ein. Nicht als root anmelden. Gebt in der Konsole folgende Befehle ein

```
cd /home/username
```

```
mkdir .ssh
```

```
ssh-keygen -b 4096
```

Jetzt wird ein key mit einer Länge von 4098 Zeichen erstellt.
Das dauert jetzt einen Moment bis der key erstellt ist.
Dann kommt eine Abfrage, wo der key gespeichrt werden soll. Als Auswahl steht da bereits der (/home/Username/.ssh/id_rsa) Das einfach mit ENTER bestätigen.

Jetzt solltet ihr eine Passphrase eingeben. Das ist zwar nicht zwingend notwendig, erhöht aber noch einmal die Sicherheit. Die Passphrase dient dazu den key abzusichern, falls der in falsche Hände gelangen sollte. Merkt euch die Passphrase gut.

Wechseln ins Verzeichnis .ssh

```
cd /home/username/.ssh
```

Den Verzeichnis-Inhalt ansehen

```
ls -la
```

Hier seht ihr nun 2 Dateien „id_rsa“ und „id_rsa.pub“
Damit die Datei “id_rsa.pub als Schlüssel erkannt wird gebt ihr folgenden Befehl ein

```
cat id_rsa.pub >> authorized_keys2
```

```
ls -la
```

Jetzt habt ihr in dem Ordner .ssh 3 Dateien
„id_rsa“ „id_rsa.pub“ und „authorized_keys2“

Jetzt verschiebt ihr die Datei id_rsa nach /home/user/
Diese benötigt ihr auf dem Gerät, von dem ihr euch mit eurem Raspi verbindet.

```
mv /home/user/.ssh/id_rsa /home/user/
```

Die Datei „id_rsa.pub“ wird nicht mehr benötigt und sollte gelöscht werden.

```
rm /home/user/.ssh/id_rsa.pub
```

Die Berechtigung für die Datei „authorized_keys2“ ändert ihr mit folgendem Befehl

```
chmod 600 /home/user/.ssh/authorized_keys2
```

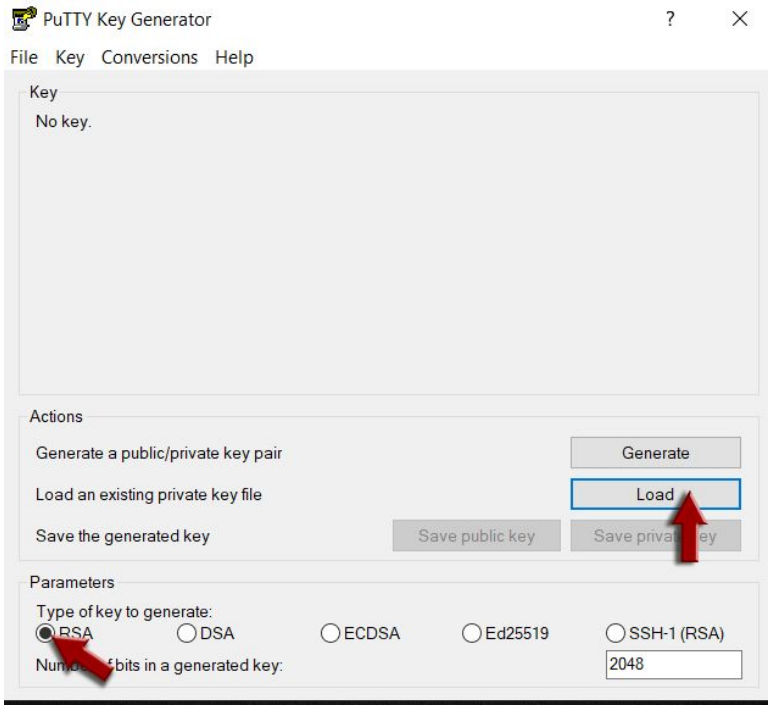
Jetzt meldet ihr euch wieder als root an und editiert die Datei

nano /etc/ssh/sshd_config

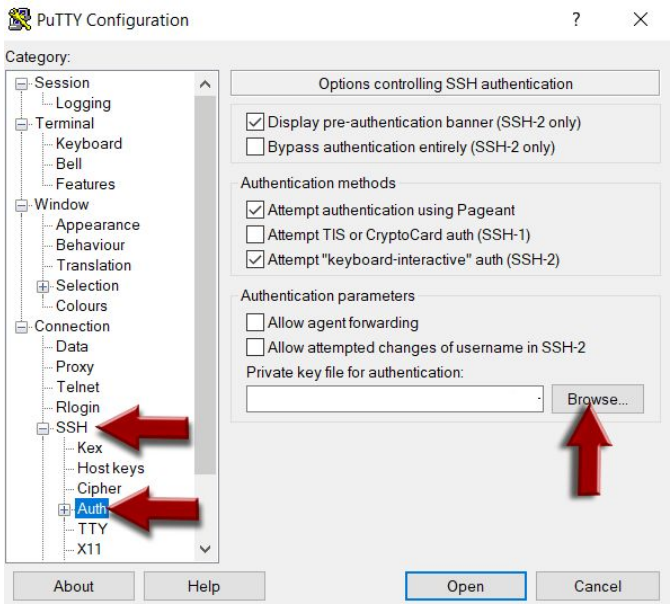
Sucht dort die Zeile „PubkeyAuthentication yes und entfernt die Raute am Anfang.
Datei speichern und schliessen.

Die Datei id_rsa im Verzeichnis /home/user müsst ihr nun auf euren Rechner verschieben. Das geht zum einen mit sftp Dazu könnt ihr ein Programm wie Winscp oder Filezilla benutzen.
Die Datei schiebt ihr dann erst einmal auf euren Desktop.

Da wir uns mit Putty einloggen und putty mit dem Schlüsselformat nichts anfangen kann, müssen wir die Datei erst mit dem Putty Generator in ein entsprechendes Format konvertieren.
Dazu geht ihr in windows 10 links in die Windows Startleiste, öffnet den Putty Ordner und startet das Pogramm „PUTTYgen“



Dann wählt ihr als Typ „RSA“ aus, klickt auf Load, wechselt im Verzeichnis auf Desktop und klickt unten auf „All Files“ weil die Datei keine Endung hat, wählt dann die Datei aus und klickt auf öffnen.
Jetzt müsst ihr die vorhin bei der Erstellung erstellte Passphrase eingeben.
Ohne diese Passphrase könnt ihr die Datei nicht konvertieren oder euch später einloggen.
Nach erfolgreicher Eingabe wird der key erzeugt.
Diesen speichert ihr jetzt mit dem Button „save privat key“ in einem Verzeichnis eurer Wahl. Als Namen könnt ihr angeben was ihr wollt mit der Endung „ppk“ z.B. raspberry.ppk Jetzt könnt ihr alle offenen Verbindungen schließen und dann startet ihr Putty.
Ihr ladet jetzt einfach euer Profil mit dem ihr euch sonst einloggt, klickt dann links unter Connection auf SSH und dann auf Auth.



Dann könnt ihr rechts den Pfad zu der soeben gespeicherten Datei auswählen.
Nun klickt ihr wieder links oben auf Sessions. Gebt einen Namen für die Session ein und klickt auf speichern.

Wenn ihr euch jetzt einloggen wollt klickt ihr auf open, meldet euch mit eurem Usernamen an. Dann wird der key geladen. Jetzt müsst ihr noch eure Passphrase eingeben, welche ihr bei der Keyerstellung angelegt habt und ihr seid eingeloggt.
Hättet ihr keine Passphrase vergeben, würde Putty nicht danach fragen. Das ist also ein Plus an Sicherheit.
Wenn sich jetzt jemand einloggen will, muss er im Besitz des Keys sein und die Passphrase kennen.
Jetzt müsst ihr aber noch die Anmeldung mit Passwort in euren ssh-Einstellungen verbieten. Vergewissert euch aber vorher, dass ihr euch mit dem Key anmelden könnt, damit ihr euch nicht selbst aussperrt.
Dann öffnet ihr die sshd_config Datei auf eurem Pi.

nano /etc/ssh/sshd_config

Dort sucht ihr nach dem Eintrag
"PasswordAuthentication" Hier die Raute entfernen und auf „no" setzen
Dann der Eintrag
„usePAM" Den Wert auch auf „no" setzen
Dann noch den Eintrag
„ChallengeResponseAuthentication" Der sollte auf „no" stehen.

Jetzt einmal den pi neu starten mit
systemctl reboot

von dem Key solltet ihr Sicherheitshalber eine Kopie machen und zusammen mit der Passphraseund dem Backup welches ihr direkt vorher gemacht habt sicher verwahren.
Im Falle eines verlorenen oder versehentlich gelöschten Keys, oder einer vergessenen Passphrase habt ihr euch sonst selbst ausgesperrt, da ihr euch dann weder als User noch als Root einloggen könnt.