Octoprint

Software-Entwicklerin: ‚Foosel' Gina Häußge, → https://octoprint.org/

Octoprint ist ein Webgui für 3D-Drucker, die GCODE verarbeiten können.

- Druckjobs hochladen, starten, pausieren, …
- Beobachten mit Kamerabild (pi-cam oder USB-Kamera)
- GCODE-Previewer
- Viele Plugins (Spaghetti Detective, OpenGL-Preview, …)
- Als Image „Octopi" für Raspberry Pi verfügbar, alternativ Installation auf Rapsberry Pi OS Paketweise.

Experiment: Tor (das „Darknet") als VPN für Octoprint

1. Damit Sie auch einen lokalen Dienst haben, den Sie im VPN ansprechen können, installieren Sie z.B. den Apache Webserver: **sudo apt install apache2**. Nun sollte auf Port 80 ein http-Dienst laufen, den Sie mit einem Browser unter **http://ip-adresse-des-pi/** ansprechen können.

Diesen Webserver, der im Internet natürlich nicht sichtbar ist (von außen kommt man nicht ins Kurs-WLAN) wollen wir nun per Tor von anderen Netzen aus, auch in anderen Intranets, zugänglich machen!

2. Installieren Sie auf Ihrem Raspberry Pi den Tor-Proxy: `sudo apt install tor`

3. Konfigurieren Sie in der Datei `/etc/tor/torrc` gemäß der Vorlage einen „Hidden Service" für den Webserver. Sie können auch den Port für den SSH-Zugang freigeben, spätestens jetzt sollten Sie dann aber ein anderes Passwort für den „pi"-Benutzer setzen!

In diesem Beispiel heißt das Verzeichnis für die von tor selbst erzeugten Daten **/var/lib/tor/website**.

4. Das Verzeichnis **/var/lib/tor/website** muss noch angelegt werden und braucht die passenden Rechte:

sudo mkdir /var/lib/tor/website

sudo chown debian-tor.debian-tor /var/lib/tor/website

sudo chmod 700 /var/lib/tor/website

5. Starten Sie den tor-Service neu: **sudo /etc/init.d/tor restart**

6. **Gratulation, Sie haben nun einen Server im „Darknet". ;-)**

Kopieren Sie sich die generierte Onion-Adresse Ihres Servers für Copy & Paste in eine Datei:

cat **/var/lib/tor/website/hostname**.

Hinweis: In der von der Tor-Foundation zur Verfügung gestellten Default-Konfiguration sowie in Debian ist tor lediglich als lokaler Proxy (Entry-Node) konfiguriert, nicht als „Man in the Middle" und auch nicht als „Exit-Node". „Exit Nodes" sind diejenigen Computer, die am Ende der Kette von

verschlüsselten und anonymisierten Anfragen stehen, sie sind für die „angerufenen“ Rechner als einzige sichtbar dadurch können ihre Betreiber nach deutschem Recht u.U. haftbar gemacht werden für die Übertragung möglicherweise illegaler Inhalte. Belassen Sie es daher bitte bei der Default-Konfiguration als reiner Proxy bzw. Anonymisierer für Ihre eigenen IP-Adressen.

Um nun auf Ihren tor-vernetzten Webserver zuzugreifen, verwenden Sie den Tor-Browser auf Ihrem Computer (ggf. installieren, + https://www.torproject.org/de/download/) und geben Sie einfach die Onion-Adresse Ihres Servers ein, die Sie sich im letzten Schritt notiert haben.

Der Zugriff auf den SSH-Port erfordert etwas mehr Konfiguration. Mit Putty, das Sie ja nun schon für den Zugriff auf den Pi per Serielle Schnittstelle und SSH kennen (https://www.chiark.greenend.org.uk/sgtat

lässt sich für den anonymisierten SSH-Dienst ein Proxy konfigurieren, der, nach Start von Tor auf dem eigenen Rechner, standardmäßig auf Port 9050 läuft.

Als „Host“ ist hier natürlich die Onion-Adresse des eigenen Rechners anzugeben.