Wie mach man SSH noch sicherer?

Indem man noch zum Faktor „Wissen“ (Passwort) den Faktor „Besitzen“ (Handy mit App) hinzufügt.

Ubuntu 15.04

Paket installieren

```
sudo apt-get install libpam-google-authenticator
```

SSH konfigurieren

- In der Datei `sudo nano /etc/pam.d/sshd` direkt unter **@include common-auth** folgende Zeile einfügen

  ```
  auth required pam_google_authenticator.so
  ```

- In der Datei `/etc/ssh/sshd_config` überprüfen, ob die folgenden Werte eingetragen sind

  ```
  ChallengeResponseAuthentication yes
  PasswordAuthentication yes
  UsePAM yes
  ```

- SSH-Server neu starten

  ```
  systemctl restart ssh
  ```

- Fertig

Schlüssel generieren

```
google-authenticator
```

Alle Fragen, die während der Schlüsselerzeugung gestellt werden, müssen mit 'yes' beantwortet werden

Token-App

Es gibt für Android mehrere Apps, die den ausgegebenen QR-Code verarbeiten können
Ich habe mich für freeOTP entschieden, da es von RedHat entwickelt wurde und sehr gute Bewertungen hat.

Im Endeffekt ist es egal, welche App man benutzt. Das Vorgehen fast immer gleich: App öffnen → QR-Code einlesen oder Secret Key eingeben → fertig

Quellen

- http://linuxlove.eu/secure-a-ssh-login-with-google-authenticator-on-ubuntu-15-04/
- https://pthree.org/2014/04/14/two-factor-authentication-with-openssh/
- https://sysconfig.org.uk/two-factor-authentication-with-ssh.html
- http://www.blackmoreops.com/2014/06/26/securing-ssh-two-factor-authentication-using-google-authenticator/