Absichern des SSH-Logins mit 2-Faktor-Authentifizierung (TOTP)

Installation

Installieren des **libpam-google-authenticator** Pakets:

```
apt install libpam-google-authenticator
```

Einrichtung

> Die Erstellung des Geheimschlüssels und der Notfallscodes erfolgt immer für den aktuell angemeldeten Benutzer, in dieser Anleitung für den Benutzer root.

Starten des **google-authenticator**:

```
google-authenticator
```

```
Do you want authentication tokens to be time-based (y/n)
```

Ob mit Zeitbasierten Token (TOTP) gearbeitet werden soll, mit **y** beantworten.

> Die angezeigete URL **NICHT** per Browser aufrufen, da sonst der Geheimschlüssel an Google übertragen wird!

> Den QR-Code mit den gewünschten Geräten scannen und den Geheimschlüssel in einem Passwort-Manager hinterlegen.

```
Do you want me to update your "/root/.google_authenticator" file? (y/n)
```

Ob die Datei **/root/.google_authenticator** aktualisiert werden soll, mit **y** beantworten.

```
Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n)
```

Ob auf einen Login alle 30 Sekunden beschränkt werden sollen, mit **y** beantworten.

```
By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n)
```

Ob von 3 auf 17 erlaubten Codes erweitert werden soll, mit **n** beantworten.

```
If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n)
```

Ob auf maximal 3 Loginversuche pro 30 Sekunden beschränkt werden soll, mit **y** beantworten.

Änderungen an der /etc/pam.d/sshd

Am Beginn der Datei /etc/pam.d/sshd die Zeilen **auth required pam_unix.so** und **auth required pam_google_authenticator.so** hinzufügen:

```
patch -u /etc/pam.d/sshd << EOF
@@ -1,4 +1,6 @@
 # PAM configuration for the Secure Shell service
+auth required pam_unix.so
+auth required pam_google_authenticator.so

 # Standard Un*x authentication.
 @include common-auth
EOF
```

> Um die Reihenfolge der Eingabe auf TOTP Token vor Passwort zu ändern, ist die Position der Zeilen **auth required pam_unix.so** und **auth required pam_google_authenticator.so** zu vertauschen.

Änderungen an der /etc/ssh/sshd_config

In der **/etc/ssh/sshd_config** den Schlüssel auf **KbdInteractiveAuthentication yes** ändern:

```
sed -i 's/ChallengeResponseAuthentication no/KbdInteractiveAuthentication yes/g'
/etc/ssh/sshd_config
sed -i 's/KbdInteractiveAuthentication no/KbdInteractiveAuthentication yes/g'
/etc/ssh/sshd_config
```

> In älteren Installationen wird noch **ChallengeResponseAuthentication** verwendet, dieses wurde durch **KbdInteractiveAuthentication** ersetzt.

Den ssh-Server neu starten:

```
systemctl restart sshd
```

Revision #25
Created 2026-03-17 19:01:17 UTC by Admin
Updated 2026-07-07 10:44:00 UTC by Admin