Auch Owncloud lässt sich per fail2ban absichern

Logging aktivieren

Zunächst muss man das Loglevel auf 2 (WARN) oder weniger gesetzt werden. Dies geschieht entweder per Default (Default-Wert = 2), oder indem man in der Config-Datei folgende Zeile setzt. Dabei gelten folgende Levels: 0=DEBUG, 1=INFO, 2=WARN, 3=ERROR (default is WARN)

config.php

```
'loglevel' => '2',
```

Jetzt loggt owncloud jeden Fehlerhaften Login-Versuch. Leider wird die IP nicht angezeigt. Dies ändert man, indem man folgende Zeile in die Config-Datei einfügt

config.php

```
'log_authfailip' => true,
```

Jetzt wird auch die IP im Log-File angezeigt

Fail2ban-Regel erstellen

Als nächstes sollte man das folgende rule-file nach `/etc/fail2ban/filter.d` kopieren.

owncloud.conf

```
# Fail2Ban configuration file
#
# Author: Patrick Schindelmann
#
# $Revision$
#

[Definition]

# Option:  failregex
# Notes.:  regex to match the password failures messages in the
logfile. The
#          host must be matched by a group named "host". The tag
"<HOST>" can
#          be used for standard IP/hostname matching and is only an
```

```
alias for
#          (?:::f{4,6}:)?(?P<host>[\w\-.^_]+)
# Values:  TEXT
#
failregex = ^{"app":"core","message":"Login failed: user '.*' , wrong
password, IP\:<HOST>.*

# Option:  ignoreregex
# Notes.:  regex to ignore. If this regex matches, the line is ignored.
# Values:  TEXT
#
ignoreregex =
```

Zum aktivieren muss folgender Eintrag in die Datei `/etc/fail2ban/jail.local` eingetragen werden

jail.local

```
[owncloud]

enabled  = true
port     = http,https
filter   = owncloud
logpath  = <owncloud-Verzeichnis>/data/owncloud.log
maxretry = 6
findtime = 6000
```

Zum Schluss muss noch fail2ban neu gestartet werden und man ist gegen Bruteforce-Attacken gegen ownCloud geschützt.

From:
https://wiki.da-checka.de/ - **PSwiki**

Permanent link:
https://wiki.da-checka.de/doku.php/wiki/sicherheit/owncloud_fail2ban?rev=1400342806

Last update: **2014/05/17 18:06**