Zwei-Faktor-Authentifizierung

1 Worum geht es?

Aus Sicherheitsgründen sollte bzw. muss der Zugang zur Nextcloud mit einem zweiten Faktor abgesichert werden.

2 Voraussetzungen und Vorbemerkungen

Als Admin sollten folgende Apps installiert und aktiviert werden:

- Two-Factor TOTP Provider
- Two-Factor Email

Damit sind die Möglichkeiten geschaffen, den benötigten zweiten Faktor per „Time-based one-time password“ (TOTP) oder per E-Mail zu erhalten.

Für die Aktivierung der Zwei-Faktor-Authentifizierung gibt es zwei verschiedene Möglichkeiten:

- Alle Benutzenden können selbst die Zwei-Faktor-Authentifizierung aktivieren.
- Admins können für alle Benutzenden die Zwei-Faktor-Authentifizierung verbindlich vorgeben. Dies sollte jedoch erst dann erfolgen, wenn alle Benutzenden wenigstens eine Möglichkeit eingerichtet haben.

Im Schulalltag wird empfohlen, allen Benutzenden eine Frist zum Einrichten der Zwei-Faktor-Authentifizierung einzuräumen und dies dann für alle Benutzenden vorzugeben.

3 Zwei-Faktor-Authentifizierung als Benutzender oder Benutzende einrichten

Nach der Anmeldung wechselt man über den Avatar zu Einstellungen > Sicherheit. Dort finden sich die Optionen E-Mail, TOTP (Authenticator app) und Backup-Code.

3.1 Backup-Codes erzeugen

Für das „Worst-Case Szenario“, dass man sich nicht mit dem zweiten Faktor anmelden kann, gibt es die Möglichkeit, Backup-Codes zu erzeugen, mit denen man sich einmal pro Code anmelden kann. Diese Liste druckt man aus und verwahrt sie an einem sicheren Ort.

3.2 Zweiten Faktor per E-Mail erhalten

Voraussetzung für die Verwendung dieser Methode ist, dass die Nextcloud für den Versand vom E-Mails vorbereitet ist.

Um den Erhalt des zweiten Faktors per E-Mail zu aktivieren sind noch folgende Schritte im Bereich Einstellungen > Sicherheit notwendig:

1. Auf die Schaltfläche „Zwei-Faktor Authentifizierung per E-Mail einschalten“ klicken. An die eingegebene E-Mail-Adresse wird eine E-Mail mit einem Zahlencode gesendet.
2. Den Code eingeben und „Code bestätigen“ klicken.

3.3 Zweiten Faktor per TOTP erhalten

Voraussetzung ist, dass ein Gerät zum Erhalt eines zweiten Faktors per TOTP vorhanden ist. Am meisten verbreitet sind Lösungen mit einer App z.B. auf dem Smartphone.

Um den Erhalt des zweiten Faktors TOTP zu aktivieren sind noch folgende Schritte im Bereich Einstellungen > Sicherheit notwendig. Die Einrichtung wird am Beispiel der Einrichtung einer App am Smartphone erklärt.

1. TOTP aktivieren.
2. Ein Sicherheitsschlüssel und ein QR Code wird erzeugt. Mit dem QR Code kann ein Konto in der Smartphone-App hinzugefügt zu werden. Mit dem Sicherheitsschlüssel können andere Möglichkeiten konfiguriert werden, den zweiten Faktor zu erhalten.
3. Nun öffnet man die App, diese erzeugt einen sechsstelligen Code, der sich alle 30 Sekunden ändert. Diesen Code gibt man im Feld unter dem QR Code als Testcode ein, und klickt auf die Schaltfläche „Überprüfen“.

4 Zwei-Faktor-Authentifizierung als Admin für alle Benutzenden vorgeben

Als Admin kann man für alle Benutzenden die Zwei-Faktor-Authentifizierung vorgeben. Die geschieht unter *Administrationseinstellungen* > *Bereich Verwaltung* > *Sicherheit*. Hier aktiviert man „Zwei-Faktor-Authentifizierung erzwingen“.

Alle im System vorhandenen Benutzenden können sich nun nur noch mit Benutzernamen, Passwort und zweitem Faktor anmelden.

4.1 Übergangslösung für neu angelegte Benutzende

Bei neu angelegten Benutzenden ergibt sich aber das Problem, dass diese die noch keine Zwei-Faktor-Authentifizierung konfiguriert haben – aber eine Anmeldung ohne zweiten Faktor nicht möglich ist. Dieses Problem kann jedoch umgangen werden, indem diese temporär von der Vorgabe zur Verwendung der Zwei-Faktor-Authentifizierung ausgenommen werden.

1. Erstellen Sie eine neue Gruppe „Neu“ in der Benutzerverwaltung und fügen Sie neue Benutzende dieser Gruppe hinzu.
2. Fügen Sie die Gruppe „Neu“ zu den „Ausgeschlossenen Gruppen“ in der Konfiguration der Zwei-Faktor-Authentifizierung hinzu.
3. Nun können neu angelegte Benutzende die Zwei-Faktor-Authentifizierung konfigurieren. Wenn dies erledigt ist, entfernt man sie aus der Benutzergruppe „Neu“.