

Zwei Faktor Authentisierung (2FA)

Warum sollte ich 2FA nutzen

Die Verwendung von [Zwei-Faktor-Authentisierung](#) (2FA) ist aus mehreren Gründen äußerst wichtig für die Online-Sicherheit:

Erhöhter Schutz bei Passwortdiebstahl: Selbst wenn Angreifer das Passwort kennen, können sie ohne den zweiten Faktor nicht auf das Konto zugreifen.

1. **Verhinderung von Identitätsdiebstahl:** 2FA trägt dazu bei, die eigene Identität und persönliche Informationen zu schützen, indem es unbefugten Zugriff erschwert. Bei Banken ist die 2FA schon Standard, da es die Sicherheit bei Finanztransaktionen gewährt. Die 2FA ist besonders für Online-Banking und Online-Einkäufe wichtig, um sicherzustellen, dass nur man selbst auf das eigene Konto zugreift.
2. **Schutz von Daten in der Cloud:** 2FA verhindert unbefugten Zugriff auf sensible Daten, die in der Nextcloud gespeichert sind. 2FA ist effektiv gegen automatisierte Angriffe: 2FA kann 100% der automatisierten Bot-Angriffe stoppen.
3. **Vielfältige Methoden:** Es gibt verschiedene 2FA-Methoden, darunter SMS, Authenticator-Apps, biometrische Verfahren und Hardware-Tokens, die je nach Bedarf und Präferenz genutzt werden können. In der Nextcloud der SPD Chemnitz sind die Verfahren mit einer Authenticator-App und mit einem Hardware-Token frei geschaltet.

Durch die Verwendung von 2FA wird die Sicherheit der Online-Konten erheblich geschützt und damit auch der Zugriff auf die persönlichen und geschäftlichen Daten vor unbefugtem Zugriff.

Wenn man keine Zwei-Faktor-Authentifizierung (2FA) verwendet, setzt man sich mehreren erheblichen Sicherheitsrisiken aus:

1. **Erhöhte Anfälligkeit für Passwortdiebstahl:** Ohne 2FA können Angreifer mit nur einem gestohlenen Passwort vollen Zugriff auf das Konto erlangen.
2. **Leichteres Ziel für Phishing-Angriffe:** Cyberkriminelle können einen einfacher dazu verleiten, Anmeldedaten preiszugeben, da kein zweiter Faktor erforderlich ist.
3. **Höheres Risiko von Identitätsdiebstahl:** Ohne die zusätzliche Sicherheitsebene von 2FA ist es für Angreifer einfacher, eine Online-Identität zu stehlen und zu missbrauchen.

4. **Anfälligkeit für automatisierte Bot-Angriffe:** 2FA stoppt 100% der automatisierten Bot-Angriffe. Ohne sie sind die eigenen Benutzerkonten diesen Angriffen schutzlos ausgeliefert.
5. **Gefährdung sensibler Daten:** Besonders bei Finanz- und Cloud-Diensten kann der fehlende Schutz durch 2FA zu unbefugtem Zugriff auf sensible persönliche und finanzielle Daten führen.
6. **Erhöhtes Risiko von Kontoübernahmen:** Ohne 2FA ist es für Hacker einfacher, die Kontrolle über Online-Konten zu übernehmen.
7. **Geringerer Schutz vor SIM-Swapping:** Obwohl SIM-Swapping auch bei 2FA ein Risiko darstellt, bietet die Verwendung von Authentifizierungs-Apps anstelle von SMS einen zusätzlichen Schutz, den Sie ohne 2FA nicht haben.
8. **Erhöhte Verwundbarkeit bei Datenlecks:** Wenn Ihre Anmeldedaten durch ein Datenleck kompromittiert werden, haben Sie ohne 2FA keine zusätzliche Schutzschicht gegen unbefugten Zugriff.

Zusammenfassend lässt sich sagen, dass die Nichtverwendung von 2FA die Online-Sicherheit erheblich gefährdet. Obwohl 2FA möglicherweise als unbequem empfunden wird, überwiegen die Sicherheitsvorteile bei Weitem die geringfügigen Unannehmlichkeiten bei der Nutzung.

Einrichtung

Im Handbuch der Nextcloud ist die Einrichtung mit einer Authentifizierungs-App gut beschrieben, weshalb ich hierauf gerne verweise:

https://docs.nextcloud.com/server/29/user_manual/de/user_2fa.html#.

Unter Einstellungen - Sicherheit findest Du alles, was die Sicherheit Deines Nextcloud-Kontos angeht. Hier kannst Du Dein Passwort ändern und ganz unten auf der Seite richtest Du ein App-Passwort ein, wie [hier](#) beschrieben.

Zwei-Faktor-Authentifizierung

Wenn Du einen Haken auf TOTP aktivieren setzt, erscheint ein TOTP-Passwort und ein QR-Code. In Deiner Authentifizierungs-App (Ich kann folgende empfehlen: [2FA Proton Authenticator](#) und [FreeOTP+](#)) kannst Du entweder mit dem Passwort einen neuen Token anlegen oder Du scannst einfach den QR-Code. Nachdem der QR-Code gescannt wurde, erzeugt die Authentifizierungs-App einen sechstelligen Sicherheitscode, den Du zur Bestätigung in die Nextcloud eintippst. Schon ist eine 2FA eingerichtet. Zukünftig kannst Du Dich nur noch in der Nextcloud anmelden, wenn Du als zweiten Authentifizierungs - Faktor den sechstelligen Code aus Deiner App eintippst. Der erste Faktor ist also Dein Passwort (**etwas, was Du weißt**), und der Zweite ist ein Code, der auf Deinem Handy generiert wird (**etwas, was Du hast**).

Zwei-Faktor-Authentifizierung ⁱ

Verwende neben deinem Passwort einen zweiten Faktor, um die Sicherheit für dein Konto zu erhöhen. Wenn du Anwendungen von Drittanbietern verwendest, um dich mit Nextcloud zu verbinden, stelle bitte sicher, dass die Zwei-Faktor-Authentifizierung aktiviert ist.

TOTP (Authenticator app)

☒ TOTP aktivieren

Sicherheitsschlüssel

Die folgenden Sicherheitsschlüssel sind für WebAuthn Zwei-Faktor-Authentifizierung konfiguriert:

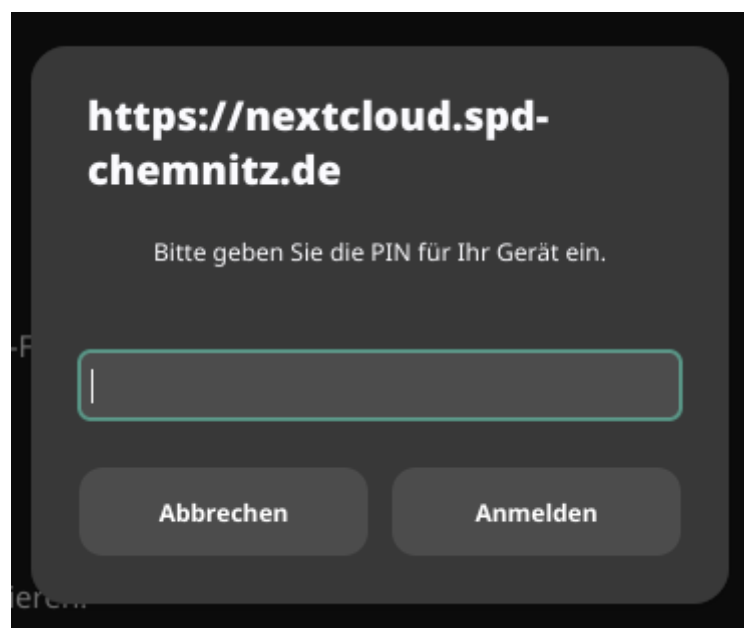
 nitro-2 ...

 nitrokey ...

Sicherheitsschlüssel hinzufügen

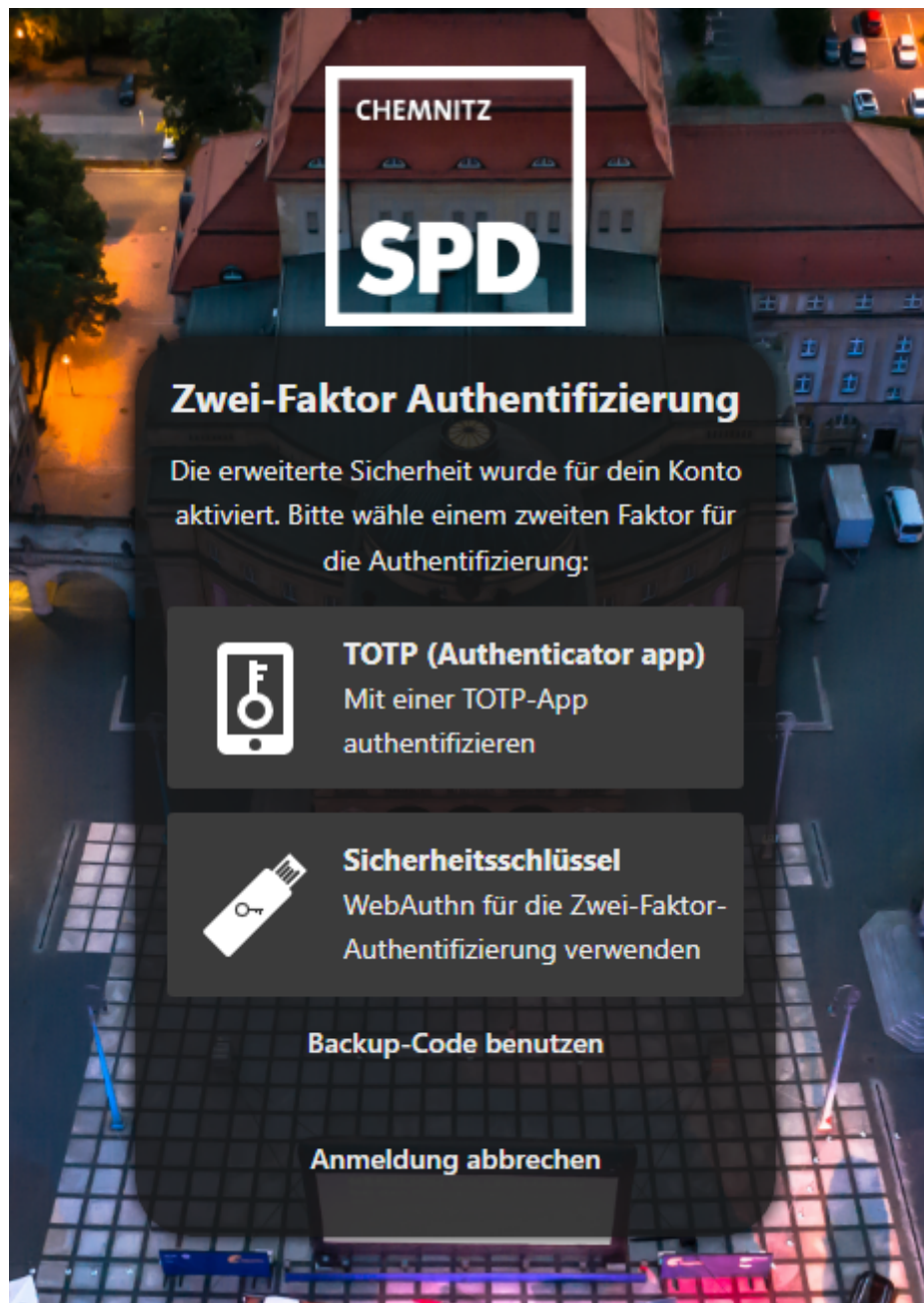
Eine weitere Möglichkeit für eine 2FA ist der Hardware-Token mit einem FIDO2-Stick wie [Yubikey](#) oder [Nitrokey](#). Wie Du auf Deinem Key eine PIN vergibst, kannst Du der Dokumentation Deines Sticks entnehmen. Eine PIN musst Du vergeben haben, denn ansonsten kannst Du den Key für die Nutzung als zweiten Authentifizierungs - Faktor nicht einrichten.

Stecke den Key in den USB-Anschluss. Er sollte kurz aufleuchten. Drücke auf den Button: „Sicherheitsschlüssel hinzufügen“. Es sollte ein Menü von Deinem Browser geöffnet werden, in dem Du die PIN des Keys eintippst. Das Menü von Firefox sieht so wie auf dem Bild aus.



The image shows a browser dialog box with a dark background. At the top, the URL **https://nextcloud.spd-chemnitz.de** is displayed. Below the URL, the text "Bitte geben Sie die PIN für Ihr Gerät ein." is shown. In the center, there is a text input field with a light blue border and a vertical cursor. At the bottom, there are two buttons: "Abbrechen" on the left and "Anmelden" on the right.

Bestätige die PIN-Eingabe und Dein Stick sollte aufleuchten. Du musst den Stick berühren, dieser Authentifizierungs - Methode einen Namen geben und abspeichern. Nun hast Du zwei Methoden für einen zweiten Authentifizierungs - Faktor: dein Handy oder der Hardware-Key. Wenn Du Dich zukünftig in der Nextcloud mit Deinem Nutzernamen und Deinem Passwort anmeldest, erscheint folgender Bildschirm und Du kannst den zweiten Faktor zur Anmeldung wählen.



Authentifizierung ohne Passwort

Mit einem Yubikey oder Nitrokey kannst Du Dich auch ohne Passwort anmelden. Stecke den Hardware-Key in einen freien USB Platz, und drücke auf den Button: WebAuthn-Gerät hinzufügen. Die Einrichtung ist identisch wie bei 2FA Einrichtung mit dem Key. Nach dem Einrichten kannst Du zukünftig im Anmeldebildschirm, statt Dein Nutzernamen und Passwort einzugeben, den Button „Mit einem Gerät anmelden“ drücken. Im folgenden Anmeldebildschirm tippst Du nur noch Deinen

Nutzernamen ein und identifizierst Dich mit Deinem Key. Aber Vorsicht, wenn Du den Key sowohl als zweiten Faktor und zur passwortlosen Anmeldung eingerichtet hast: Denn das bedeutet, dass Du wieder nur einen einzigen Faktor zur Anmeldung verwendest. Wer den Key hat, kann sich in Deinem Konto anmelden!

Authentifizierung ohne Passwort

Richte dein Konto für die Authentifizierung ohne Passwort nach dem FIDO2-Standard ein.

Die folgenden Geräte sind für dein Konto eingerichtet:

✎ nitro ...

✎ nitro-2 ...

WebAuthn-Gerät hinzufügen

Backup-Code

Wenn Du eine 2FA eingerichtet hast, ist es notwendig Backup-Codes anzulegen. Wenn Dein Handy gestohlen wurde oder Du es verloren hast, fehlt Dir der zweite Faktor und Du kannst Dich nicht mehr in der Nextcloud anmelden! Die Backup-Codes sind Dein zweiter Faktor für diesen Fall. Auf dem Bild siehst Du den Button „Backup-Codes erneuern“, da ich schon welche angelegt habe. Wenn Du noch keine angelegt haben solltest, steht auf dem Button „Backup-Codes anlegen“ oder so ähnlich. Drücke auf den Button und in einem Fenster werden Dir 10 Codes angezeigt. Kopiere diese in eine Datei, speichere sie ab und verwahre sie an einem sicheren Ort.

🔒 Backup-Code

Backup-Codes wurden erzeugt. 0 von 10 Codes wurden benutzt.

Backup-Codes erneuern

Wenn du Backup-Codes erneuerst, werden alte automatisch ungültig.

Bei der Anmeldung in die Nextcloud kannst Du nun auf dem Bildschirm zur Eingabe des zweiten Faktors zur Anmeldung den Button „Backup Code“ klicken und Du hast weiterhin Zugang zur Nextcloud.

Zusammenfassung

Auch wenn das alles sehr kompliziert klingt, ist es das bei Weitem nicht. Ein zweiter Faktor zur Anmeldung erhöht die Sicherheit deutlich, selbst schwache Passwörter, die leicht zu knacken sind, werden somit sicherer, weil es zur Anmeldung immer eines zweiten Faktors bedarf. Generell solltest Du bei jedem Konto, bei dem eine 2FA eingerichtet werden kann, diese auch nutzen. Vor welchen Gefahren Du Dich mit einer 2FA schützen kannst habe ich weiter oben beschrieben. Wichtig zu beachten bleibt nur: Auch eine 2FA bietet keinen 100 % Schutz vor Datendiebstahl. Es gibt ausgeklügelte Methoden, um auch an den zweiten Faktor zu kommen: Missbrauch von Session Cookies, [Browser-in-the-Browser-Angriffe](#) oder Device Code Phishing um nur einige zu nennen. Der Aufwand ist hier aber bedeutend höher als nur ein Passwort auszuspionieren!

Version #3

Erstellt: 2026-07-04 08:44:29 UTC von alfredo

Zuletzt aktualisiert: 2026-08-11 12:48:03 UTC von alfredo