Allgemeine Informationen zu 2-Faktor-Authentifizierung

Was ist Zwei-Faktor-Authentifizierung überhaupt?

Zwei-Faktor-Authentifizierung, auch 2FA genannt, ist ein Sicherheitsverfahren, das die Anmeldung durch die Kombination von zwei unterschiedlichen, unabhängigen Faktoren absichert. Die Faktoren müssen aus verschiedenen Kategorien stammen z.B. Wissen (Passwort/Pin), Biometrie (Fingerabdruck) oder Besitz (DUO Token). An der TU Braunschweig, werden wir die DUO App für das mobile Endgerät, eine Desktop Anwendung für Laptops/Rechner und DUO Token anbieten.

Wieso wird 2FA an der TU-Braunschweig eingeführt?

In erster Linie wird durch den zweiten Faktor die Sicherheit der IT-Infrastruktur erhöht. Der Schutz der IT-Systeme der TU-Braunschweig soll verbessert werden, sodass die Vertraulichkeit, die Integrität sowie die Verfügbarkeit der Daten erhöht wird. Ziel ist es, unbefugten den Zugriff auf die Benutzerkonten zu erschweren.

Das Präsidium hat sich für die Einführung einer 2-Faktor-Authentifizierungslösung entschieden. Auslöser für die Implementierung sind unter anderem der beobachte Missbrauch des zentralen E-Mail-Systems zur Versendung von Phishing und SPAM durch unbefugten Zugriff auf E-Mail-Konten. Sowie die Verwendung von gestohlenen Zugängen für Online-Betrug. Der Abfluss von Informationen aus Filesystemen und Datenbanken sollen hierdurch verhindert werden.

Wie funktioniert 2FA an der TU-Braunschweig?

Zuerst erfolgt die Freischaltung des Users über "Meine Daten (BDD)", in der freiwilligen Phase für den zweiten Faktor. Nach maximal 45 Minuten kann die Person sich entweder beim OWA anmelden oder klickt in der Aktivierungsmail auf den Link und durchläuft den Prozess der Einrichtung, z.B. für das mobile Endgerät. Für nähere Erklärungen/Beschreibungen gibt es dazu eine Anleitung im books (Zwei-Faktor-Authentifizierung (2FA) mit DUO). Wenn der User diesen Prozess durchlaufen hat, kann der der zweite Faktor benutzt werden bzw. der zweite Faktor ist einsatzbereit.

Ist das mobile Endgerät veraltetet oder sprechen andere Gründe gegen eine Nutzung, kann der User auf die Desktop Anwendung ausweichen. Im Ausnahmefall wird dem User ein Token ausgestellt.

Folgende Systeme sind aktuell durch die 2-Faktor-Authentifizierung abgesichert:

- Outlook Web Access (OWA)
- Virtual Private Network (VPN)
- Single Sign-On (SSO)

Revision #8
Created 2025-11-24 08:42:50 UTC by Katharina Ziegner
Updated 2026-04-10 05:43:19 UTC by Katharina Ziegner