Zwei-Faktor-Authentifizierung (2FA)

Die Zwei-Faktor-Authentifizierung ist die anerkannte und empfohlene Methode zur Absicherung von Remote-Zugriffen auf Netzwerke und Web-Applikationen. Aktuelle Lösungen verwenden als zweiten Faktor meist sogenannte One Time Passwords bzw. Passcodes (OTP) oder Einmalpasswörter. Diese werden für jeden spezifischen Anmeldevorgang generiert und können nur zur einmaligen Authentifizierung genutzt werden.

Die Hochschule Fulda setzt die 2-Faktor-Authentifizierung für horstl-Benutzer*innen mit umfangreichen Rechten ein. Beschäftigte können zwischen einem **Hardware-Token (Yubikey)** oder einem **App-Token (Smartphone-App)** wählen. Für Lehrbeauftragte ist der APP-Token vorgesehen. Zunächst verwenden nur Lehrbeauftragte im Studiengang Soziale Arbeit (Präsenz) die Zwei-Faktor-Authentifizierung.

Anleitung zur Einrichtung und Installation des APP-Token (Smartphone)

Für die Ersteinrichtung ist es erforderlich, dass mit den Benutzer*in ein Termin zur Registrierung des APP-Token verabredet wird. Hierbei ist es erforderlich, dass der Benutzer*in sich ausweisen kann. Der Termin kann persönlich oder über eine Videokonferenzlösung realisiert werden.

Für die Installation der 2FA ist es erforderlich, aus dem App-Store Ihres Betriebssystems eine spezielle Anwendung auf Ihrem Smartphone herunterzuladen. Die Hochschule Fulda empfiehlt hier die Nutzung der kostenfreien Apps **2FAS Authenticator** oder **privacyIDEA Authenticator**.

Installation 2FAS Authenticator
Installation privacyIDEA

Ausgabe Hardware-Token (Yubikey) für Beschäftigte

Hardware-Token für Beschäftigte können über die horstl-Berechtigungsanträge angefordert werden. Die horstl-Berechtigungsanträge stehen im Intranet zur Verfügung.

Kontakt

Für Fragen zur Zwei-Faktor-Authentifizierung stehen Ihnen die Kolleg*innen des Teams Campus Managements im Rechenzentrum (Bereich Anwendungen) zur Verfügung. Gerne können Sie eine E-Mail an cms-support@hs-fulda.de schreiben.

Verlustmeldung

Bitte senden Sie eine E-Mail an cms-support@hs-fulda.de, wenn Sie Ihren Hardware-Token (Yubikey) oder Ihr Smartphone (bei Verwendung einer APP) verloren haben. Der Token oder das Smartphone wird gesperrt und eine Neuausgabe bzw. Neuregistrierung in die Wege geleitet.

Zusätzliche Informationen zum TAN-Verfahren

Die Hochschule Fulda bietet zur Nutzung von 2FA aktivierten Diensten, die TAN-Verfahren

Time-based One-time Password (TOTP)

Zeitbasierte Algorithmen verwenden die Zeit zusammen mit einem gemeinsamen privaten Schlüssel um ein Passwort zu generieren. Daher bieten zeitbasierte Einmalpasswörter zusätzliche Sicherheit, denn selbst wenn das herkömmliche Passwort eines Anwenders gestohlen wird oder kompromittiert wird, kann ein Angreifer ohne das TOTP, das schnell abläuft, keinen Zugriff erhalten. TOTP ist ein anerkannter Standard der Internet Engineering Task Force (IETF).

TOTP Parameter

- OTP-Länge = 6
- Zeitschritt = 30 sec
- Hash-Algorithmus = sha256

Yubico One-time Password

Jeder Yubikey enthält ab Werk bereits einen einzigartigen, geheimen Schlüssel, über den auf Knopfdruck dynamisch Passwörter generiert werden können. Dieser Schlüssel wird aber in unserem Fall individuell neu geschrieben und per Schlüsselfile dem 2FA - Server mitgeteilt. Im Grunde funktioniert dieser Mechanismus ähnlich wie alle üblichen OTP Verfahren: Ein Zähler im Yubikey und auf dem 2FA -Server wird bei jedem Login inkrementiert. Beide Seiten berechnen einen Soll-Schlüssel und vergleichen diesen miteinander. Der Hauptunterschied: Der Key ist fest eingebrannt, kann nicht ausgetauscht werden und eine Authentifizierung ist nur gegenüber 2FA -Server möglich. Dazu kommt noch eine Komfortfunktion: Der Yubikey tippt das Passwort selbstständig ein.

Die YubiKey OTP-Schlüssel besteht aus den folgenden Feldern, die mit einem eindeutigen AES-128-Bit-Schlüssel verschlüsselt sind. Das Ergebnis ist die 32-stellige Modhex-Zeichenfolge, welche an die 12-stelligen öffentlichen ID angeschlossen ist.

Mnemonisch	Byte-Offset	Größe	Beschreibung
uid	0	6	Private (geheime) ID
verwendungCtr	6	2	Verwendungszähler
tstp	8	3	Zeitstempel
sessionCtr	11	1	Sitzungsnutzungsindikator
rnd	12	2	Zufallszahl