Multi-Faktor-Authentifizierung (MFA)

Zusammenfassung

Diese Seite gibt einen Einstieg in das Thema „Multi-Faktor-Authentifizierung“ (kurz MFA) und adressiert die wichtigsten Fragen für Nutzerinnen und Nutzer an der Universität.

Diese Anleitung richtet sich besonders an folgende Zielgruppen:

- Studierende
- Mitarbeitende
- Lehrende
- Gäste der Friedrich-Schiller-Universität

Was ist eine Multi-Faktor-Authentifizierung?

Die Multi-Faktor-Authentifizierung, kurz MFA, ist eine Authentifizierungsmethode, die auf einer mehrstufigen Anmeldung basiert. Dazu muss bei einem Login in ein System zusätzlich zu einem Passwort ein zweiter, unabhängiger Identitätsnachweis (d. h. ein „Faktor“) erbracht werden. Dies erfolgt z. B. durch die Eingabe eines Bestätigungscodes, einer PIN oder die Freigabe des Logins in einer App auf dem Smartphone. Im Alltag ist dies zum Beispiel vom Onlinebanking bekannt, aber auch Online-Shopping, E-Mail-Dienste oder Soziale Medien sind Bereiche, in denen viele Anwenderinnen und Anwender bereits täglich mit MFA interagieren, um ihre Konten zu schützen.

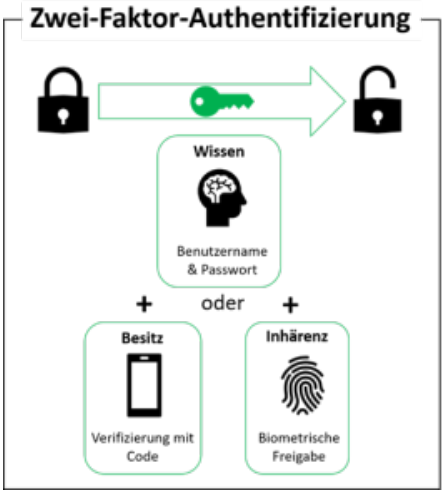
Welche Vorteile hat die MFA-Nutzung?

In einer Zeit zahlreicher Cyberangriffe auf Hochschulen und andere Bildungseinrichtungen gewinnt der Schutz unserer Online-Aktivitäten zunehmend an Bedeutung. Hinter der MFA steht eine Absicherung gegen die Gefahr, dass ein einzelner Authentifizierungsfaktor, zum Beispiel ein gestohlenes Passwort oder ein abgeschriebener PIN-Code, bereits den Fremdzugriff auf ein System ermöglicht. Muss eine Nutzerin bzw. ein Nutzer jedoch mehrere Nachweise der eigenen Identität erbringen, wird das Eindringen Unbefugter deutlich erschwert. Insbesondere der Gefahr durch Phishing wird hierdurch entgegengewirkt und das Risiko erheblich gesenkt. MFA ist heutzutage eine der effektivsten Methoden zur Sicherung von Online-Konten und wird von vielen großen Unternehmen und Organisationen aktiv genutzt.

Welche Arten von Faktoren gibt es?

Es gibt drei Hauptkategorien von Faktoren, die für eine MFA eingesetzt werden können:

1. ***Wissensfaktor*** (etwas, das der Benutzer weiß): Hierunter fällt als Beispiel die Nutzung eines Passwortes oder einer persönlichen Identifikationsnummer (PIN).
2. ***Besitzfaktor*** (etwas, das der Benutzer besitzt): Dies kann ein Smartphone sein, das einen Einmalcode als SMS oder in einem Anruf empfängt oder durch eine App selbst generiert. Dieser Code ist dann zusätzlich zum Passwort einzugeben. Eine andere Variante ist die Nutzung eines Hardware-Tokens, der für den Login zusätzlich in den USB-Anschluss einzustecken ist.
3. ***Inhärenzfaktor*** (etwas, das der Benutzer ist): Dies umfasst alle biometrischen Verifizierungsmethoden wie Fingerabdruckscan, Iris- oder Retina-Scan, Gesichts- und Stimmerkennung.



Bei der MFA wird eine Kombination dieser Faktoren verwendet, um einen möglichst effektiven Schutz zu erreichen. Zum Beispiel sollte ein Benutzer neben seinem Passwort (Wissensfaktor) auch einen Einmalcode von einer Authentifizierungs-App auf seinem Smartphone (Besitzfaktor) eingeben oder seine Fingerabdrücke mit einem biometrischen Scanner (Inhärenzfaktor) verifizieren.

Welche Faktoren werden künftig an der Universität genutzt?

Dies wird im Rahmen der Einführungsstrategie (s. unten) erarbeitet.

Einführungsstrategie an der Universität Jena

Die Einführung einer MFA an unserer Universität erfordert eine sorgfältige Planung, in der zukünftige Nutzerinnen und Nutzer einbezogen werden. Angestrebt wird eine **Authentifizierung mit einem zweiten Faktor aus der Besitzkategorie** (s. „Welche Arten von Faktoren gibt es?“).

Im Zuge der Einführungsstrategie eines zweiten Faktors streben wir eine umfassende Einbindung und Berücksichtigung verschiedener Aspekte an:

- Akzeptanz bei künftigen Nutzerinnen und Nutzern
- Barrierefreiheit
- Langfristige Stabilität
- Technische Umsetzbarkeit
- Kosten

Mit der MFA-Einführung wird ein entsprechender Support für die Anwenderinnen und Anwender aufgebaut und ein Monitoring für den Betrieb und technische Entwicklungen etabliert. Abhängig von Möglichkeiten und Bedarf wird die Lösung kontinuierlich weiterentwickelt.

Haben Sie Fragen, Kommentare oder Hinweise?

Fragen und Hinweise können Sie direkt an die Stabsstelle für Informationssicherheit (informationssicherheit@uni-jena.de) richten

Titel: "Multi-Faktorauthentifzierung (MFA)"

Stand: 27.05.2022

blocked URL