A1 Business

Digitale Identität

Authentisierung – Authentifizierung - Autorisierung

A1. Verantwortung für Ihr Business.

Wer sind wir im Internet ?

- Bevor man einen Dienst im Internet nutzen kann, muss man sich anmelden –**„registrieren“**
- Anmeldung ist notwendig, damit der Dienst den Nutzer „wiedererkennt“, also weiß bspw.:
  - Wer kauft ein oder streamt Musik?
  - Wohin sind die Einkäufe zu liefern?
  - Von welchem Konto wird der Verkaufspreis abgebucht?
  - Wem sind die Quizergebnisse zuzuordnen?

- Anmeldung führt technisch zur Einrichtung einer **digitalen Identität**, für die in der Nutzerdatenbank des Dienstes ein **Account** hinterlegt wird

Was ist eine digitale Identität

Digitale Identität ist eine Sammlung elektronischer Daten, „**Attribute**", die

- Nutzer (physische Identität) charakterisieren und
- Nutzer von anderen Nutzern unterscheidbar macht

Reale Personen, die bei einem Dienst im Internet z.B. einkaufen oder Musik streamenwollen, brauchen dazu eine digitale Identität

- Nutzer (physische Identität) kann im Internet mit (vielen) verschiedenen digitalen Identitäten unterwegs sein

Digitale Identität wird unter anderem durch folgende Attribute charakterisiert:

- **Nutzername** (User Name)
- Email Adresse
- Wohnadresse
- Kontonummer/Bankverbindung
- **Passwort**

Was ist eine digitale Identität

- Nutzer (physische Identität) kann im Internet mit (vielen) verschiedenen digitalen Identitäten unterwegs sein
  - bei jedem Registriervorgang können neue / andere Attribute eingegeben werden, z.B. anderer Nutzername, andere Bankverbindung, anderes Passwort, …
- Bindung einer digitalen Identität an ihren Nutzer muss so missbrauchssicher wie möglich hergestellt werden
- Wenn gewünscht, kann eine digitale Identität auch von
  - Gruppe von Nutzern oder
  - anderen Objekten oder Diensten (Entitäten)

als Zugang zu einem Dienst genutzt werden

Authentisierung und Authentifizierung

Bevor eine neue digitale Identität genutzt werden kann, ist sowohl eine **Authentisierung** als auch **Authentifizierung** notwendig:

Authentisierung für einen Dienst (durch Nutzer)

- der Nutzer erbringt einen Identitätsnachweis
- **genauer**: Nutzer gibt z.B. Passwort und Nutzername ein, oder legt den Finger auf einen Abdruckleser

Authentifizierung(durch Dienst)

- Verifikation des Identitätsnachweises
- **genauer**: Prüfung: Stimmt z.B. das Passwort mit dem hinterlegten des Nutzers überein? Stimmen z.B. die Fingermerkmale mit den hinterlegten überein?

Autorisierung und Rechteverwaltung

Nach der erfolgreichen **Authentifizierung** des Identitätsnachweises durch den Dienst erfolgt die **Autorisierung**.

Autorisierung für einen Dienst bestimmt, welche Angebote und Ressourcen des Dienstes der zuvor authentifizierte Nutzer nutzen darf

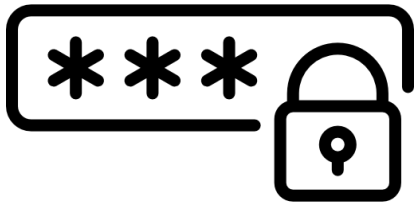
Genauer: Bestimmt, was der zuvor von diesem Dienst authentifizierten digitalen Identität alles erlaubt ist z.B. Datenzugriff, Lese-und/oder Schreibrechte:

- Wer darf Videos im eCampus ansehen?
- Wer darf Videos und Quizzes im eCampus einstellen?
- Wer darf Lehrmaterialien im eCampus hochladen?
- …

Arten der Authentisierung

Es werden 3 Arten der Authentisierung unterschieden

Wissen:



Besitz:

Biometrie:

Multi-Faktor-Authentisierung (MFA) (auch Multi-Faktor-Authentifizierung)

Jede Methode zur Authentisierung hat ihre Vor-und Nachteile

- Um **Nachteile zu kompensieren und Sicherheit zu erhöhen** werden mehrere Methoden kombiniert
- Die Kombination von 2 Methoden bzw. Faktoren wird als **2-Faktor-Authentisierung (2FA)**bezeichnet
  - **Beispiel**: Internetkonto mit 2FA
    1. Faktor Wissen: Passwort
    2. Faktor Biometrie: Überprüfung Gesichtsbiometrie mittels Webcam
- Nutzt man mehr als zwei Faktoren spricht man von **Multi-Faktor-Authentisierung (MFA)**

    3. Faktor Besitz: bestimmtes Smartphone mit SIM, dass einen Einmalcode per SMS zur Eingabe erhält

Authentisierung mittels Wissen

Authentisierung mittels Wissen prüft Kenntnis eines Geheimnisses

- **Textgeheimnisse**
  - Passwort
  - PIN
- **Grafische Geheimnisse**
  - Kenntnis bestimmter Punkte in einem Bild
  - Bilder auswählen, auf denen Freunde zu sehen sind

Vorteile:

- weit verbreitet - jeder kennt es, einfache Anwendung
- Geheimnis ist jederzeit änderbar
- keine spezielle Hardware nötig

Nachteile:

- Sicherheit abhängig von der Komplexität
  - je komplexer desto besser
  - aber um so schwieriger zu merken
- zu viele Geheimnisse sind schwer merkbar
- andere können das Geheimnis erraten oder systematisch herausfinden/ermitteln

Authentisierung durch Besitz

Authentisierung mittels Besitz prüft Vorhandensein eines bestimmten Objektes

- Smartphone
- Ausweis / Mitgliedskarte
- Handy-Signatur
- …

→ „Vorzeigen“ und Zugriff ist gewährt

Vorteile:

- kein Wissen nötig

Nachteile:

- kann man verlieren
- kann gestohlen werden und Dieb bekommt damit direkten Zugriff auf digitale Identität
- oft wird dazu zusätzliche Hardware oder eine eigene App am Smartphone benötigt

Authentisierung durch Biometrie

Authentisierung mittels Biometrie prüft körperliche Eigenschaften

- Physiologische Merkmale
  - Fingerabdruck
  - Gesichtsform
  - Iris
  - …
- Verhalten
  - Laufverhalten
  - Tippverhalten
  - Bewegungsmuster
  - …

Vorteile:

- weder Wissen noch Besitz nötig
- Biometrische Merkmale sind für jede Person einzigartig

Nachteile:

- Erfassung braucht spezielle Hardware
- kann sensible Informationen enthalten
- Prüfung basiert auf Wahrscheinlichkeiten – Angriff möglich mit Fälschung, die „gut genug" ist
- wenn Merkmal einmal kompromittiert, lässt es sich nicht/schwer ändern, z.B. Fingerabdruck
- Verletzungs-und Alterungsprozesse muss bei Konzeption von Systemen bedacht werden

Multi-Faktor-Authentisierung als sichere Methode um Identitätsdiebstahl zu verhindern

- **Multi-Faktor-Authentisierung ist um eine Spur unbequemer, jedoch bietet es die kombinierten Vorteile jedes einzelnen Faktors**
- **Passwörter sind gut – kombiniert mit Multi-Faktor-Authentisierung sind sie deutlich sicherer**
- **Mulit-Faktor-Authentisierung ist eine Gewohnheitssache und wird immer mehr zum Standard**
- **Im Business, im Privaten, im IT-Umfeld**