Datensicherheit

Vorlesung 1: 24.11.2025

Wintersemester 2025/2026 h_da

Heiko Weber, Lehrbeauftragter

Inhalt der Vorlesung laut Modulhandbuch

Inhalt:

- Sicherheitsbegriffe und -ziele
- Bedrohungen der IT-Sicherheit
- verschiedene Techniken der System- und Netzwerksicherheit
- Informationssicherheits- und Datenschutz-Management

Ziele:

Nach Abschluss der genannten Lehrveranstaltungen sind die Studierenden in der Lage,

- die grundlegenden Sicherheitsbegriffe und -ziele zu benennen und Bedrohungen der IT-Sicherheit vorherzusagen;
- verschiedene Techniken der System- und Netzwerksicherheit zu unterscheiden;
- Bewertungskriterien für IT-Sicherheit zu benennen und anzuwenden;
- die Relevanz von systematischen Sicherheits- und Datenschutz-Systemen zu erklären; und
- Aufgaben im technischen Umfeld zu den Lehrinhalten eigenständig zu bearbeiten und die Zusammenhänge mit den juristischen Fragestellungen zu beurteilen.

Teil 2: Datensicherheit
Themenübersicht der Vorlesung

1. Einführung / Grundlagen / Authentifizierung & Autorisierung
2. Kryptografie / Verschlüsselung & Signaturen / Vertrauen / Blockchain
3. Softwaresicherheit / Schadsoftware
4. Netzwerksicherheit / TLS / PGP & S/MIME / Firewalls & Netzwerksegmentierung
5. Hacking / Phishing / Einführung in den Datenschutz / Anonymität / Darknet
6. Datenschutzgesetze / Technische & Organisatorische Maßnahmen
7. Organisationssicherheit / Managementsysteme

Teil 2: Datensicherheit
Themenübersicht der Vorlesung

1. **Einführung / Grundlagen / Authentifizierung & Autorisierung**
2. **Kryptografie / Verschlüsselung & Signaturen / Vertrauen / Blockchain**
3. **Softwaresicherheit / Schadsoftware**
4. **Netzwerksicherheit / TLS / PGP & S/MIME / Firewalls & Netzwerksegmentierung**
5. **Hacking / Phishing / Einführung in den Datenschutz / Anonymität / Darknet**
6. **Datenschutzgesetze / Technische & Organisatorische Maßnahmen**
7. **Organisationssicherheit / Managementsysteme**

Folgende Begriffe werden analog verwendet:

Datensicherheit

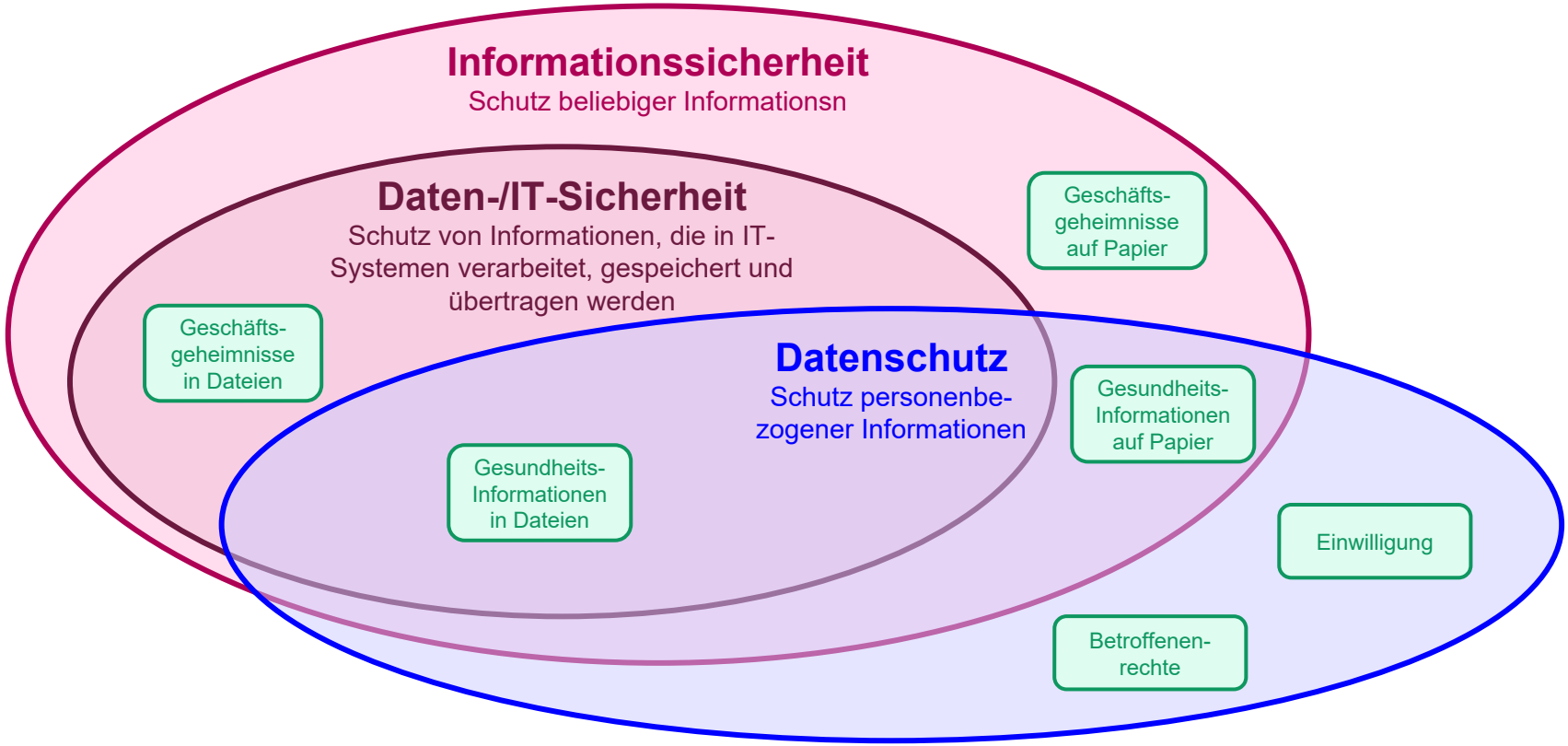
Informationssicherheit

IT-Sicherheit

Daten = Informationen

Daten werden in IT-Systemen verarbeitet

Informations-/Daten-/IT-Sicherheit und Datenschutz



Was bedeutet Datensicherheit?

- Daten = Informationen, die von einem Computersystem erzeugt, gespeichert oder verarbeitet werden.
- Diese Daten sollen geschützt werden gegen:
  - unerlaubtes Erstellen neuer Daten (create)
  - unerlaubtes Lesen der Daten (read)
  - unerlaubtes Verändern der Daten (update)
  - unerlaubtes Löschen der Daten (delete)
- Unter Datensicherheit versteht man die verschiedenen Aspekte, die involviert sind, um den Schutz von Daten zu gewährleisten.
- Abgrenzung zu Datenschutz:
  da geht es speziell um den Schutz personenbezogener Daten

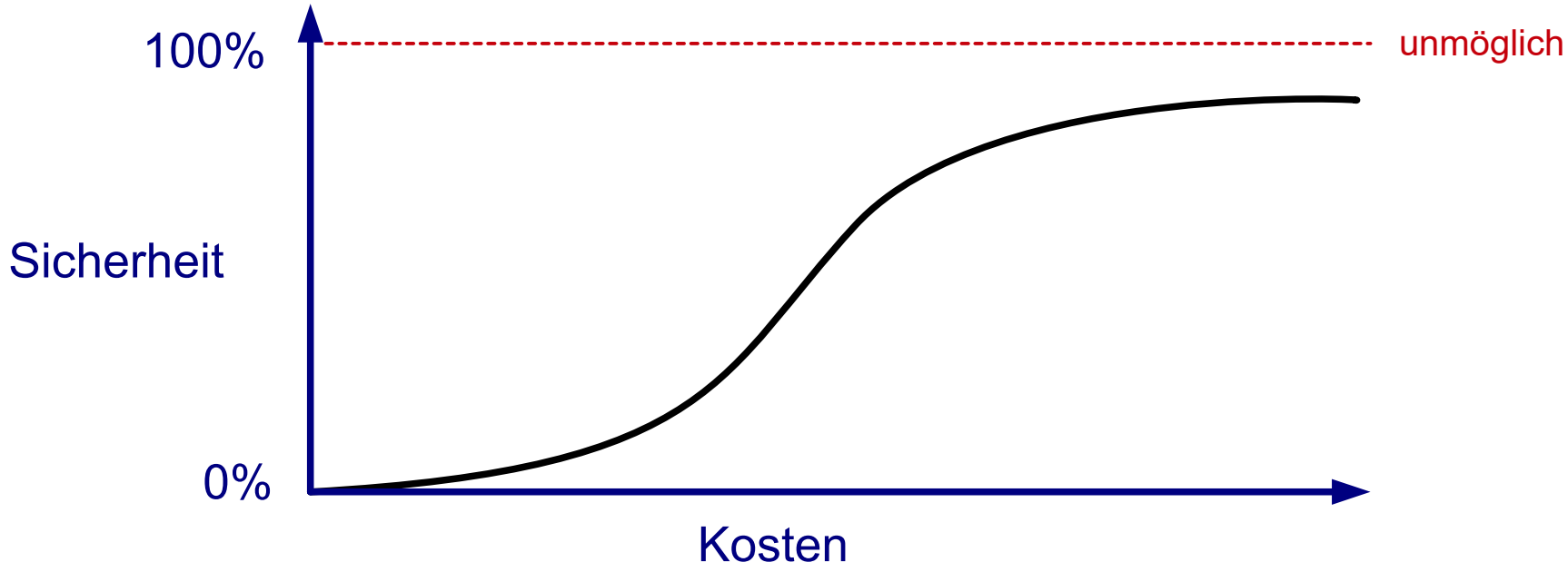
Verlust von Datensicherheit

Datensicherheit schützt gegen:

- Datendiebstahl (z. B. Wirtschaftsspionage)
  - Folgen können sein:
    - finanzieller Verlust (Zugriff auf Finanzdaten)
    - Vertrauensverlust (Zugriff auf Kundendaten)
    - Geschäftsaufgabe (Entzug von Lizenzen)
- Datenmanipulation (z. B. durch einen Hackerangriff)
- Ausfall von Systemen (z.B. durch unbeabsichtigte Fehlbedienung)
- Überwachung (z. B. durch Sicherheitsbehörden)
- und weitere...

Wie sicher können IT-Systeme sein?

- 100% Sicherheit ist unmöglich
- Sicherheit ist immer eine Abwägung zwischen Risiken und Aufwand bzw. Benutzbarkeit



Schutzziele der Datensicherheit

Vertraulichkeit	Confidentiality
Integrität	Integritity
Verfügbarkeit	Availability
Authentizität	
Nichtabstreitbarkeit	

Vertraulichkeit

- Der Zugriff auf Daten ist so zu schützen, dass nur Berechtigte sie einsehen können.
- Dies gilt sowohl für gespeicherte Daten als auch für Daten während der Übertragung. Zudem gilt es auch für Informationen über Kommunikationsvorgänge.
- Besonders wichtig bei Systemen, bei denen personenbezogene Daten oder interne/geheime Informationen verarbeitet werden.
- Beispiel:
  Die Noten und Matrikelnummer von Studentin A dürfen nicht ohne ihre Einwilligung von Student B eingesehen werden.

Integrität

- Daten und Systeme dürfen keine unzulässigen oder undefinierten Zustände annehmen – d.h. sie müssen gegen unzulässige Manipulation geschützt sein.
- D.h. die Daten müssen verlässlich sein – sie dürfen nicht unbefugt verändert worden sein, weder auf dem Speichermedium noch während der Übertragung.
- Beispiel:
  Die Noten von Studentin A werden von den Dozent_innen an das Fachbereichssekretariat abgegeben, wo sie in die Notendatenbank eingetragen werden. Die Noten die in der Notendatenbank landen, müssen genau die Noten sein, wie sie von den Dozent_innen abgegeben wurden.

Verfügbarkeit

- Daten und Systeme müssen im Rahmen der üblichen Nutzung betriebsbereit sein und es muss auf die Daten wie vorgesehen zugegriffen werden können.
- Besonders wichtig in Produktionssystemen oder zentralen Infrastruktursystemen (z. B. Stromnetze, Notrufsysteme, Internet).
- Beispiel:
  Das Online-Belegsystem für die Vorlesungen muss in der Phase zur Anmeldung für die Kurse erreichbar und funktionsfähig sein und muss die Anmeldungen korrekt speichern.

Authentizität

- Die Echtheit und Glaubwürdigkeit der Daten muss gewährleistet sein.
- Beispiel:
  Dozentin A schickt die Notenliste für eine Vorlesung an das Fachbereichssekretariat – es muss sichergestellt werden, dass diese Notenliste tatsächlich von Dozentin A stammt, bevor sie in die Notendatenbank eingetragen wird.

Nichtabstreitbarkeit

- Sicherstellen, dass der Ursprung von Daten auch nicht abstreiten kann, der Ursprung der Daten gewesen zu sein.
- Beispiel:
  In einem Newsletter für Schnäppchen trägt sich eine Person mit E-Mail-Adresse ein. Es muss sichergestellt werden, dass diese Person auch Inhaber_in der E-Mail-Adresse ist, bevor die erstellen Newsletter an die Person verschickt werden (z. B. mit Double Opt-In).

Identifizierung / Authentifizierung / Autorisierung

Identifizierung

Der Prozess, bei dem festgestellt wird, wer eine Entität vorgibt zu sein.

Dazu gehört die Angabe eines eindeutigen Identifikators, wie Benutzername, E-Mail-Adresse, Token, usw.

Unterscheidet eine Entität von einer anderen.

Authentifizierung

Der Prozess der Überprüfung, ob die behaupteten Eigenschaften einer Entität korrekt sind.

Dazu gehören Informationen, die zur Überprüfung der Authentizität der Behauptung verwendet werden können, wie z. B. ein Passwort, ein geheimer Schlüssel, eindeutige biometrische Merkmale usw.

Sicherstellen, dass die Entität authentisch ist.

Autorisierung

Der Prozess der Zuweisung und Überprüfung von Zugriffsberechtigungen für eine bestimmte Entität.

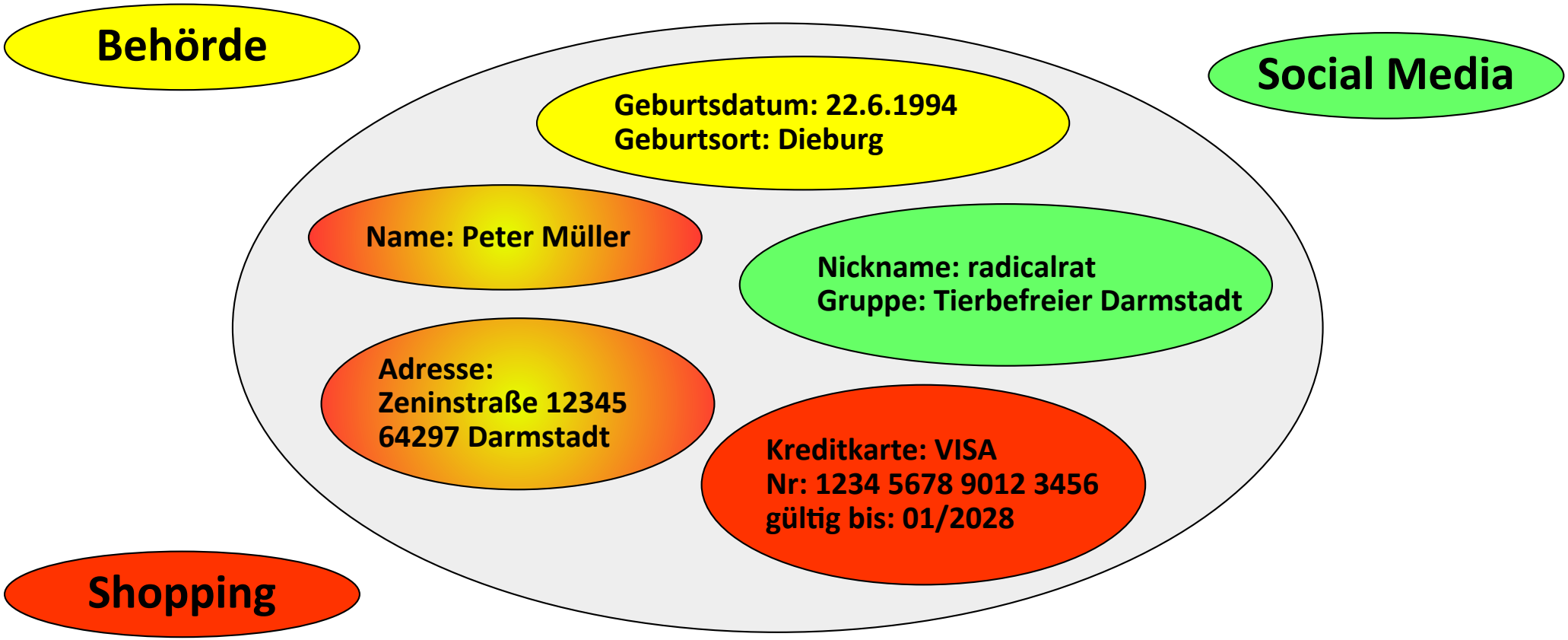
Die Überprüfung, ob der beabsichtigte Vorgang in einem IT-System für eine bestimmte Entität zulässig ist.

Sicherstellung der zulässigen Operationen einer Entität.

Identitäten

- im realen Leben:
  - eine Person hat normalerweise genau eine Identität
- in der digitalen Welt:
  - eine Person kann über mehrere digitale Identitäten verfügen
- digitale Identität
  - Teilmenge der Attribute einer Person in digitaler Form
  - Attribute: unterscheidbare, messbare, physische oder abstrakte Eigenschaften einer Person

Beispiel für digitale Identitäten



Identifizierung und Authentifizierung

- **Identifizierung**
  - Erkennen einer Entität, basierend auf behaupteten oder festgestellten Eigenschaften.
- **Authentifizierung**
  - Überprüfen, ob die behaupteten Eigenschaften einer Entität korrekt sind.
  - Prüfen, ob die behauptete Identifizierung korrekt ist.

Methoden zur Identifizierung und Authentifizierung

- **was jemand hat**
- **was jemand weiß**
- **was jemand ist**

Methoden zur Identifizierung und Authentifizierung

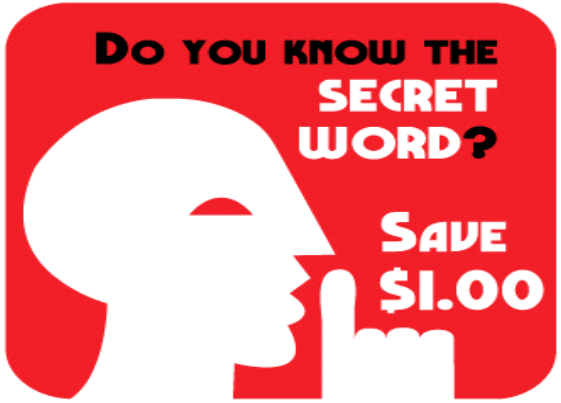
- **was jemand hat**
  - Ring, Pin, Secure Token, Personalausweis, digitales Zertifikat, ...
- **was jemand weiß**
- **was jemand ist**

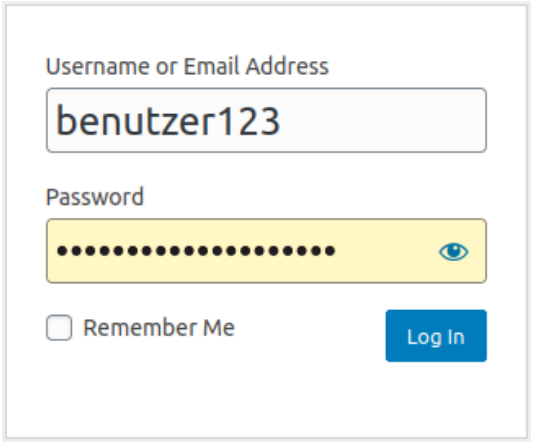
```
-----BEGIN KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyJbdXrdsvj4ueiln26qo
SefYCsaqnYFoshikZYXr6Og3xiu3gxfZDGCh2AWwA9v5PS2yC0XyPjDemxHgzY6y
r6kuIOL[illegible]
nOoNM/kJ[illegible]
kPuwW3[illegible]
48Kjii/lzf7rfa3Z7iSkDOofiJzZ7+T969dZgq6KAmZnIocJOj6FTfsZMm+tGbUC
9wIDAQAB
-----END KEY-----
```

ZERTIFIKAT

Methoden zur Identifizierung und Authentifizierung

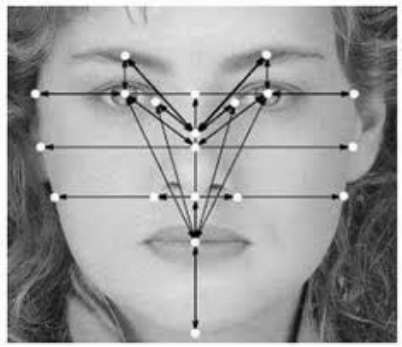
- **was jemand hat**
  - Ring, Pin, Secure Token, Personalausweis, digitales Zertifikat, ...
- **was jemand weiß**
  - Passwort, Antwort auf Sicherheitsfrage, Code, ...
- **was jemand ist**

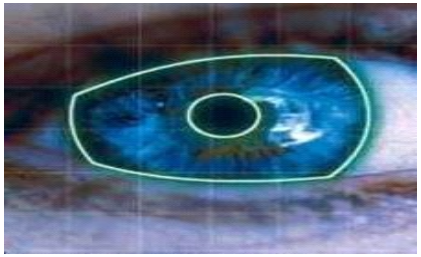




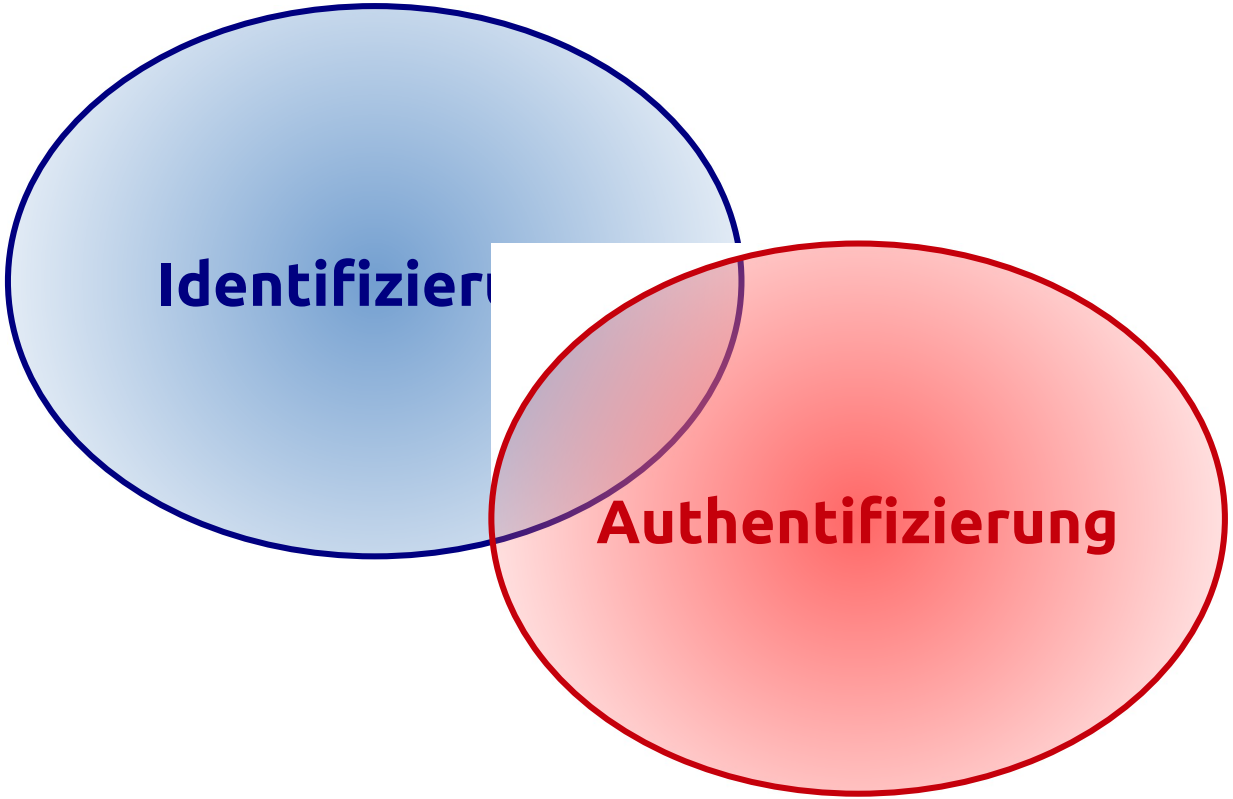
Methoden zur Identifizierung und Authentifizierung

- **was jemand hat**
  - Ring, Pin, Secure Token, Personalausweis, digitales Zertifikat, ...
- **was jemand weiß**
  - Passwort, Antwort auf Sicherheitsfrage, Code, ...
- **was jemand ist**
  - Biometrie



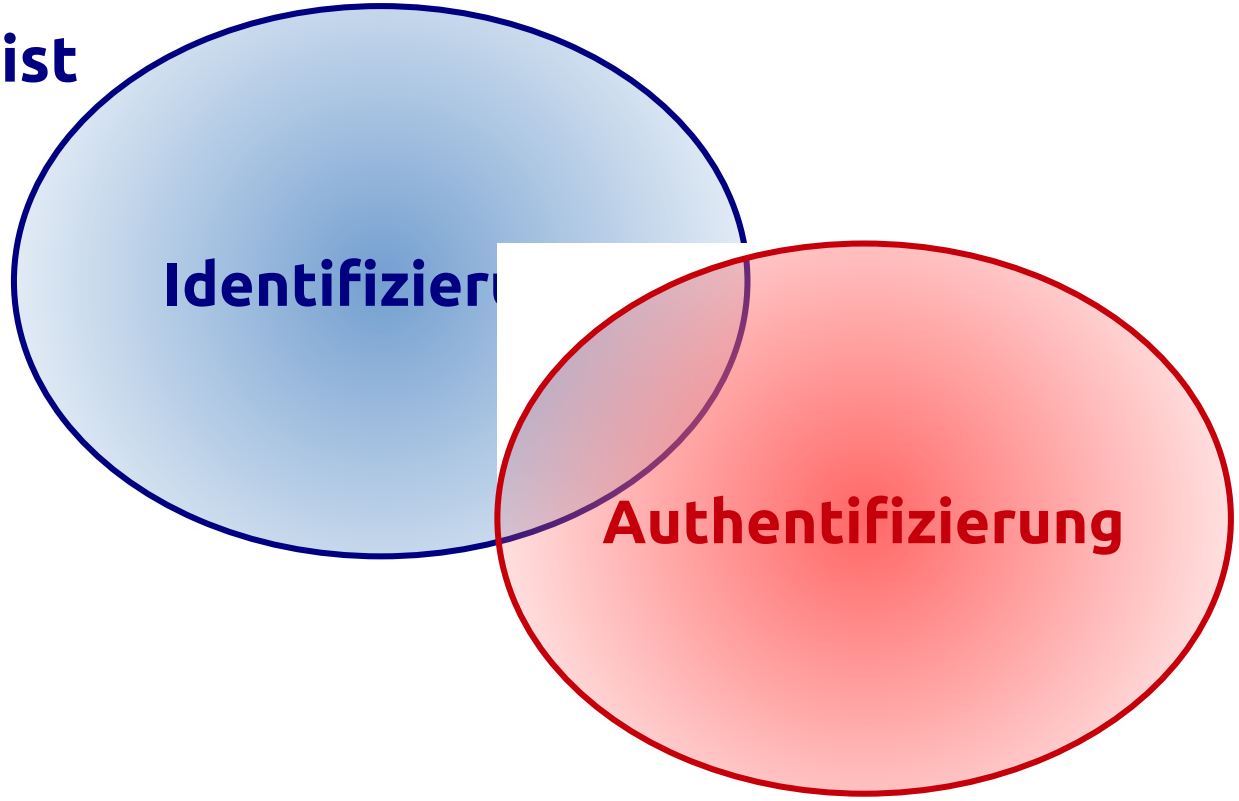


Methoden zur Identifizierung und Authentifizierung



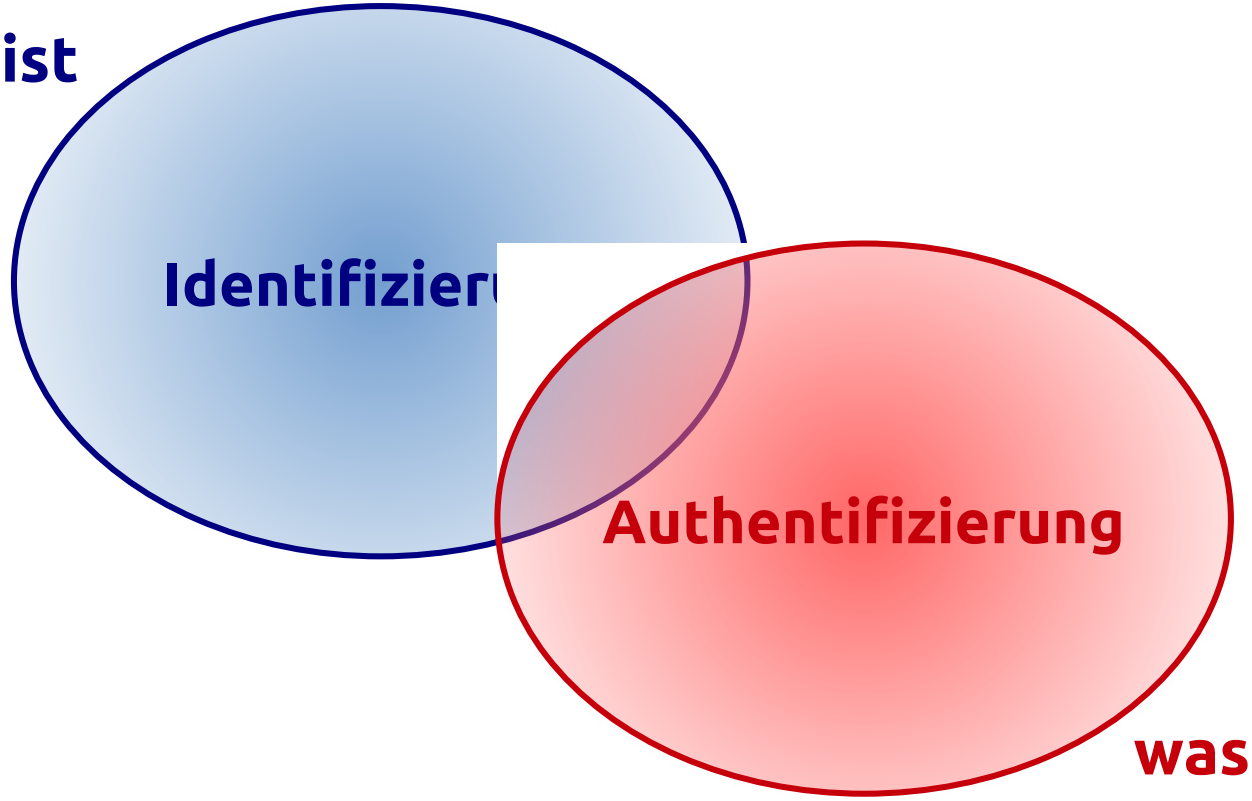
Methoden zur Identifizierung und Authentifizierung

was jemand ist
Biometrie



Methoden zur Identifizierung und Authentifizierung

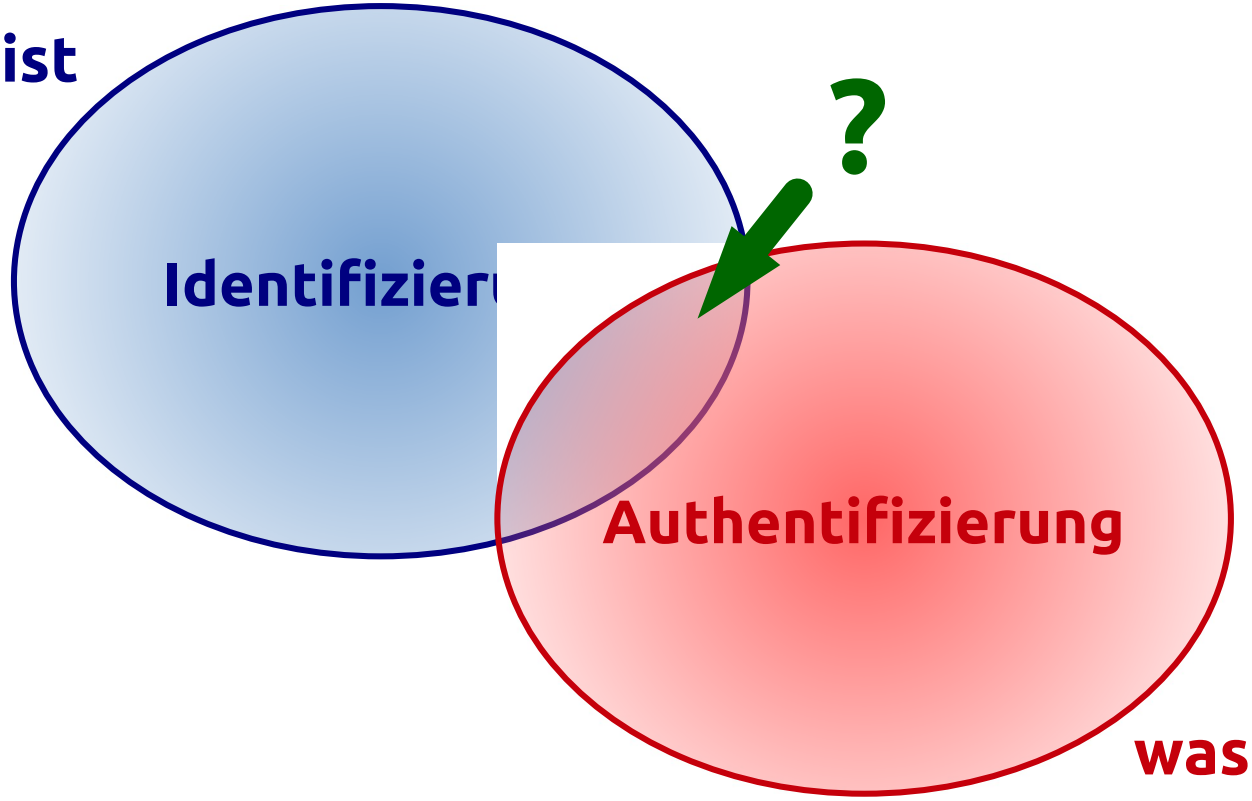
was jemand ist
Biometrie



was jemand weiß
Passwort

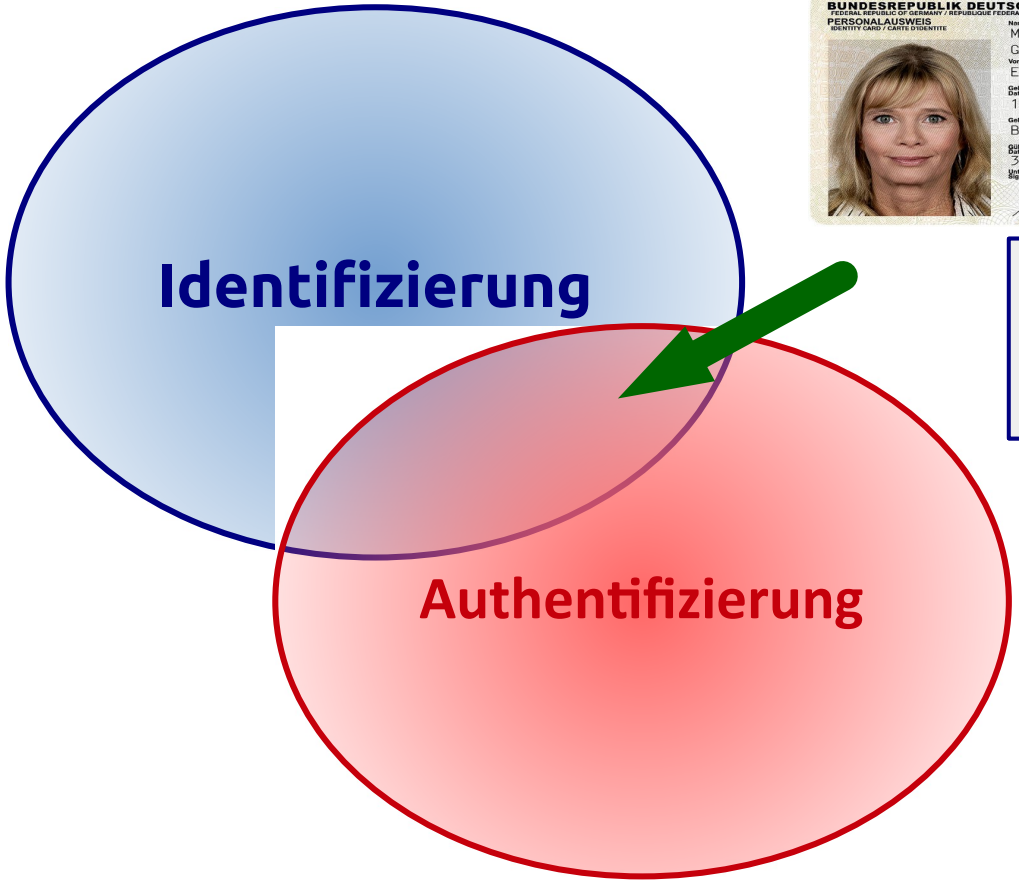
Methoden zur Identifizierung und Authentifizierung

was jemand ist
Biometrie



was jemand weiß
Passwort

Methoden zur Identifizierung und Authentifizierung



z. B. qualifizierte digitale Signatur

Authentifizierung

- **Anforderungen an Informationen für die Authentifizierung**
  - veränderbar (Revokation, im Falle von Verlust)
  - geheimhaltbar (schwer zu raten, sicher gegen brute-force)
- **häufig verwendet:**
  - Passwörter
  - digitale Zertifikate (z. B. auf einer SmartCard)
- **auch verwendet:**
  - biometrische Daten (Fingerabdrücke, Iris-Scans, …)
  - problematisch, weil
    - unveränderbar
    - leicht kopierbar, da meist öffentlich zugänglich
    - oft nicht eindeutig zuzuordnen

Wie sicher sind Passwörter?

Cyberkriminalität: Fahnder entdecken 18 Millionen gestohlene E-Mail-Passwörter

Von Michael Fröhlingsdorf, Hubert Gude und Jörg Schindler

REUTERS

Quelle: http://www.spiegel.de

TECHNIK

Ein Screenshot zeigt: Einige Passwörter sind viel zu simpel.
(Foto: Screenshot)

Donnerstag, 11. September 2014

Kein großes Problem für Google

5 Millionen Gmail-Passwörter geklaut

Im Internet kursiert eine Liste mit rund fünf Millionen Gmail-Adressen plus Passwörtern. Wurde Google geknackt oder ist die Sache so harmlos, wie das Unternehmen mitgeteilt hat?

Quelle: http://www.n-tv.de

Cloud-Speicher

7 Millionen Dropbox-Passwörter gestohlen

Erst vor kurzem sorgten die geleakten Nacktfotos einiger Promis aus deren persönlichem iCloud-Speicher für Aufsehen, jetzt sind Hacker auch an zahlreiche Zugangsdaten von Dropbox-Nutzern gelangt. 7 Millionen Accounts sollen betroffen sein, hunderte wurden bereits öffentlich einsehbar gemacht - gehackt wurde die Plattform laut Aussage von Dropbox aber nicht.

Dropbox | (c) Unternehmen

Als im September diverse Prominente hilflos dabei zusehen mussten, wie ihre persönliche Fotosammlung im Netz verteilt wurde, da lag der Verdacht nahe, dass Apples iCloud tatsächlich gehackt wurde. Dem ist nicht so, beteuert Apple, stattdessen haben sich die für die Leaks verantwortlichen Hacker durch Trial-&-Error-

Quelle: http://www.areamobile.de

Häufige Probleme bei Passwörtern

- schwache Passwortregeln
- schlechte Passworterneuerungsverfahren
- schlechter Schutz gegen Brute-Force-Angriffe
- unveränderbare Passwörter
- unsichere Speicherung der Passwörter
- unsicherer Transport der Passwörter

Häufige Probleme bei Passwörtern:
Schwache Passwortregeln

- durch Cloud-Angebote kann für sehr wenig Geld sehr hohe Rechenleistung gekauft werden, so dass Hunderttausende bis Millionen verschiedene Passwortkombinationen pro Sekunde ausprobiert werden können
- Passwörter mit 8 Zeichen oder weniger sind heute nicht mehr sicher genug
- viele Menschen wählen zu einfache Passwörter

Häufige Probleme bei Passwörtern:
Schlechte Passwörter

Die Top 10 der geleakten Passwörter in 2024:

1. `123456`
2. `password`
3. `12345`
4. `12345678`
5. `abc123`
6. `123456789`
7. `1234567`
8. `qwerty`
9. `iloveyou`
10. `password1`

Quelle: https://identeco.de/de/blog/whitepaper_passwords_germany_2024/

Häufige Probleme bei Passwörtern:
Schlechte Passworterneuerungsverfahren

- schlechte Passworterneuerungsverfahren bei vergessenen Passwörtern
  - schlechte Sicherheitsfragen
    - z. B. Name eines Haustiers oder Geburtsdatum
  - automatisches Zurücksetzen bei Eingabe der E-Mail-Adresse
    - kann benutzt werden, um Accounts Anderer zu sperren
- Passwortänderung ohne Eingabe des alten Passworts
  - vergessen auszuloggen und schon hat jemand das Passwort geändert

Häufige Probleme bei Passwörtern:
Schlechter Schutz gegen Brute-Force-Angriffe

- **Brute-Force-Angriff =** alle möglichen Kombinationen ausprobieren
- es darf zeitlich nicht möglich sein, alle möglichen Passwortkombinationen auszuprobieren
  - Verzögerung einbauen, wenn falsches Passwort eingegeben wurde
  - Sperren des Accounts ist schlecht, weil somit ein_e Angreifer_in einfach alle Accounts sperren kann, indem er/sie falsche Passwörter gezielt eingibt

Häufige Probleme bei Passwörtern:
Unveränderbare Passwörter

- manche Software und Hardware nutzt feste Passwörter für interne oder administrative Zugänge
- Problem:
  - durch Reverse-Engineering, kann der Quellcode von Software lesbar gemacht werden, also können die Passwörter extrahiert werden
  - wenn die Passwörter einmal bekannt sind, gibt es keine Möglichkeit sie zu ändern, um sich zu schützen

Häufige Probleme bei Passwörtern:
Unsichere Speicherung der Passwörter

- Passwörter sollten niemals im Klartext gespeichert werden
- optimalerweise sollten sie mit einer Einwegfunktion (Hash-Funktion) gespeichert werden, so dass es unmöglich ist, das Originalpasswort zu ermitteln
  - es gibt spezielle Hash-Funktionen, die für die Speicherung von Passwörtern optimiert sind (Details dazu kommen in der Vorlesungseinheit über Kryptographie)

Häufige Probleme bei Passwörtern:
Unsicherer Transport der Passwörter

- niemals Passwörter im Klartext im Netzwerk übertragen!
- Abhören/Mitprotokollieren findet fast überall statt
  - insbesondere in öffentlichen WLAN-Zugangspunkten
- nur bei Webseiten mit HTTPS Passwörter eingeben

Sichere Passwörter

- leicht für einen Menschen zu merken
- schwer für eine angreifende Person zu raten
- möglichst lang

- schwer zu merken und leicht für einen Computer zu erraten:
  `g7X4D3b5`
- leicht zu merken und schwer für einen Computer zu erraten:
  `montagsHOLEichMIReineLAUGENBRETZELamBAHNHOF_:-)`

Multi-Faktor-Authentifizierung (MFA)

- Um die Schwachstellen beim Einsatz von reinen Passwörtern zu adressieren, wird ein weiterer Faktor hinzugenommen.
- Passwort: etwas was man weiß
- zusätzlicher Faktor:
  - etwas was man hat
    - Zeit-basierte TAN (z.B. RSA token)
    - TAN via E-Mail oder SMS
    - TAN via Smartphone-App (z.B. Authenticator-App)
    - digitale Zertifikate (z.B. Benutzer-Zertifikat, Geräte-Zertifikat)
  - etwas was man ist
    - Biometrische Informationen (z.B. Fingerabruck oder Gesichts-Scan)

Passwortlos

- da es mittlerweile auch immer mehr Angriffe auf die gängigen Verfahren für Multi-Faktor-Authentifizierung gibt, bieten auch immer mehr IT-System-Anbieter Verfahren an, die komplett ohne Passwörter auskommen, die an das Authentifizierungssystem übermittelt werden müssen
- Passwortlose Technologien sind zum Beispiel
  - Pass Keys
  - Hello for Business (bei Microsoft-Systemen)
- Passwortlose Technologien sind in der Regel an spezielle IT-Systeme gebunden und deswegen nicht so leicht zu realisieren wie reine Passwörter, bieten aber einen sehr guten Schutz vor dem Abgreifen der Authentifizierung durch einen Angreifer