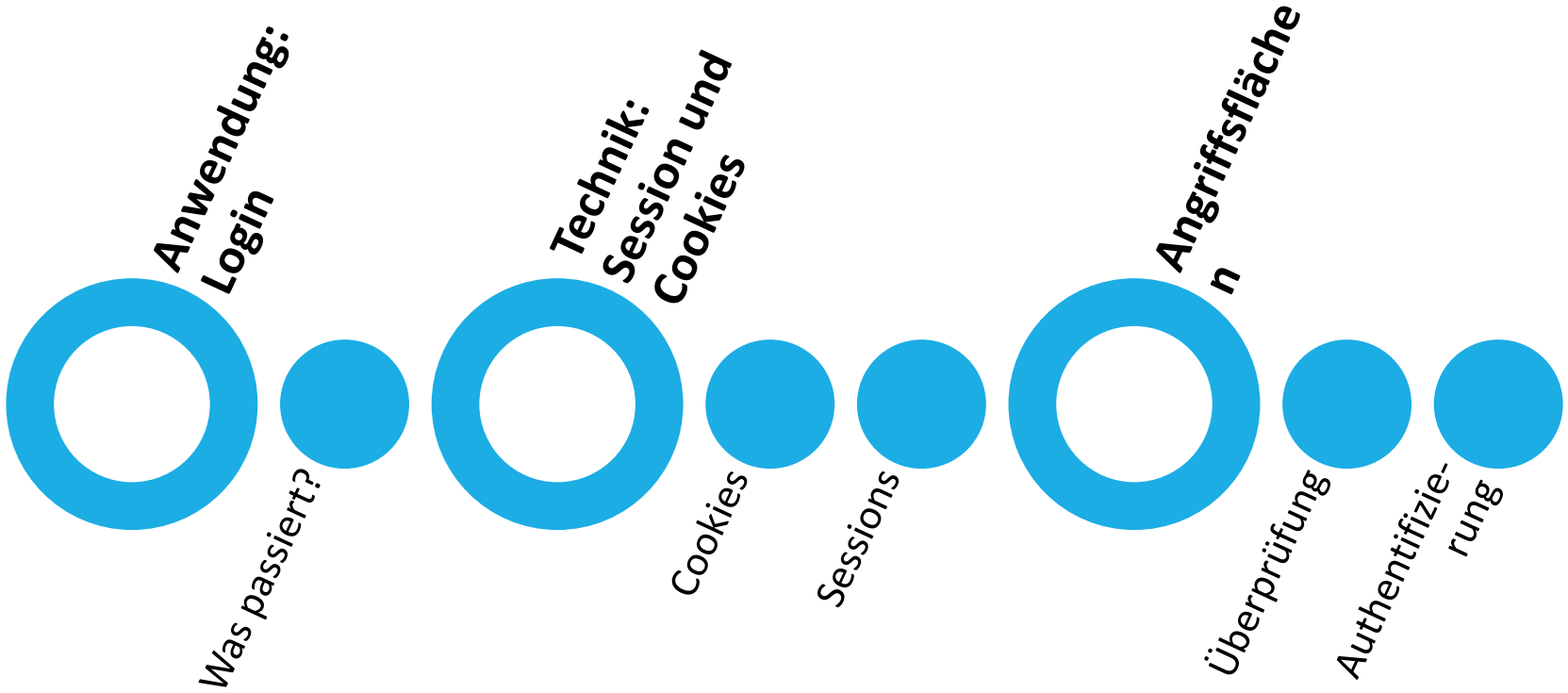
Programm diese Woche



Kompetenz

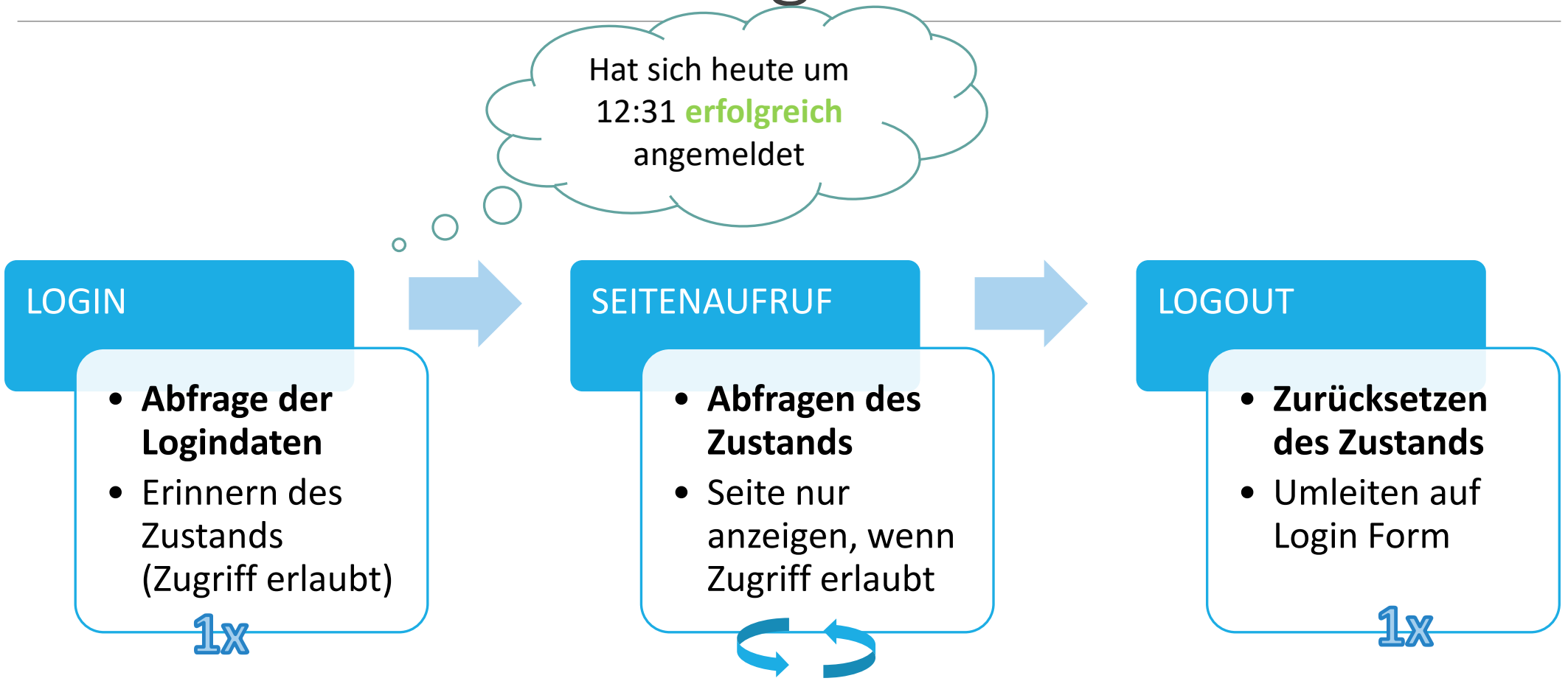
«einen sicheren, passwortgeschützten Bereich mit Login aufbauen unter Berücksichtigung der spezifischen Gefahren»

- Sessions und Cookies für temporäre Datenspeicherung nutzen
- Passworte sicher ablegen
- Gefahren durch Sessions und Cookies kennen
- Geeignete Massnahmen anwenden, um Gefahren durch User Input zu minimieren

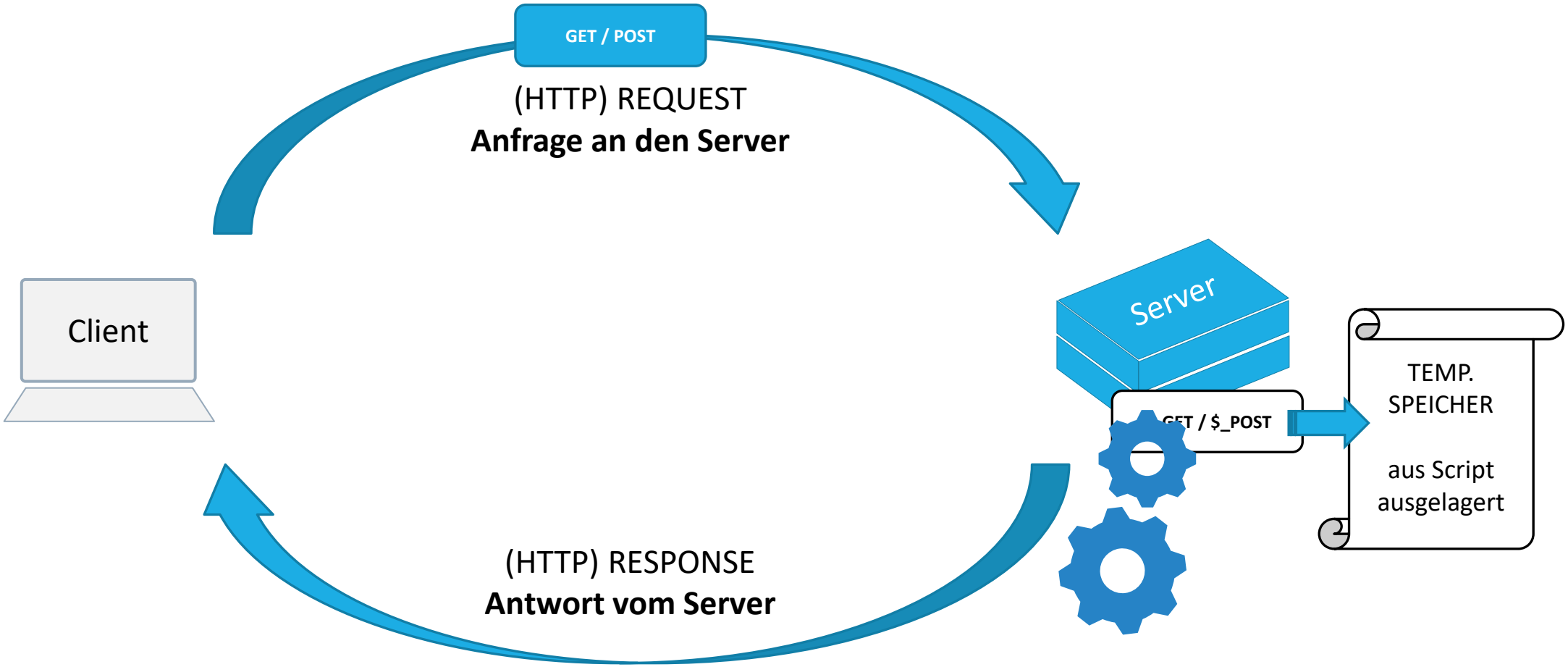
Login: jetzt für später

WAS GESCHIEHT WÄHREND UND NACH DEM LOGIN?

Der Authentifizierungs-Prozess



Login und danach...

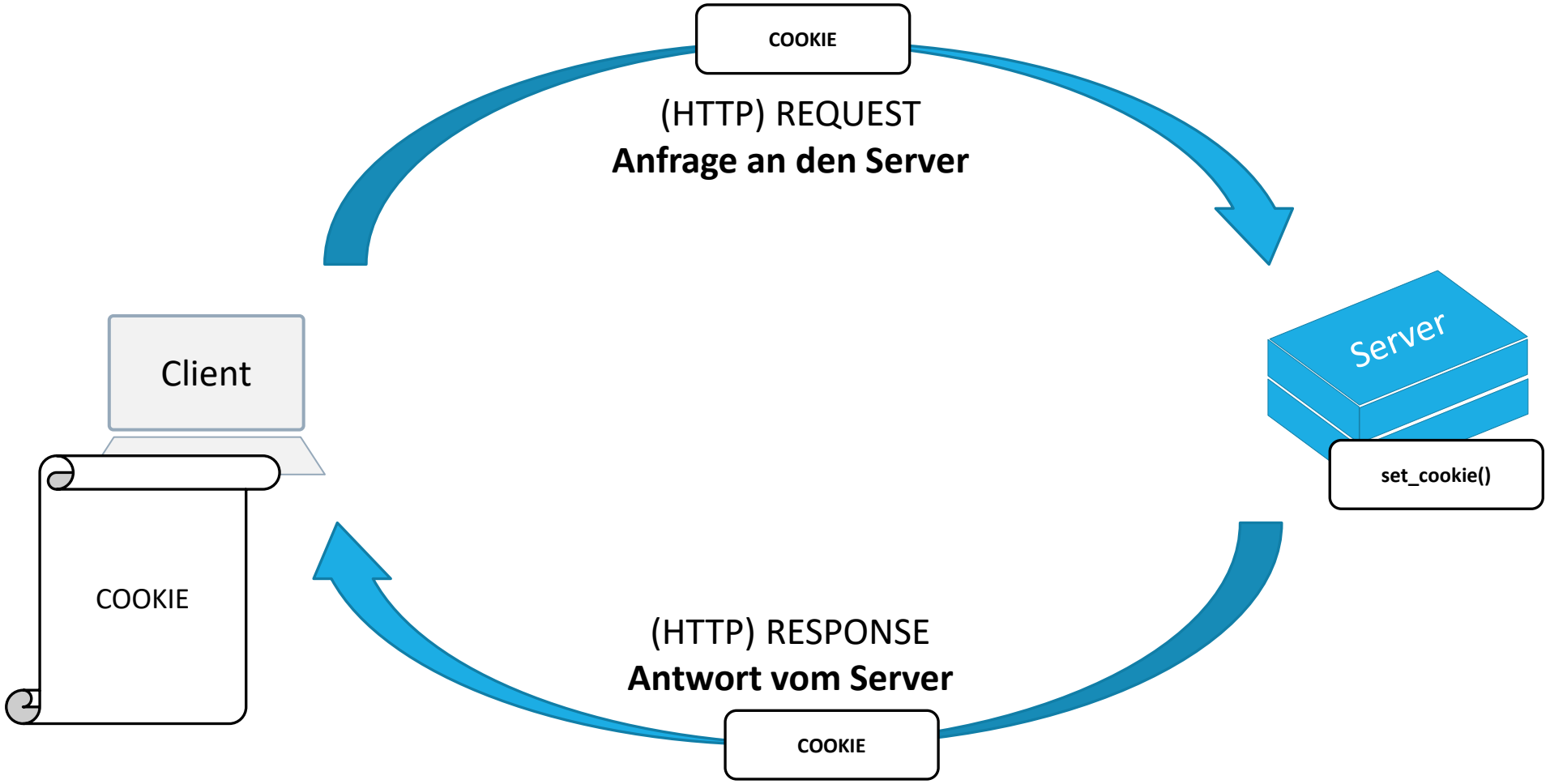


CLIENT	SERVER

Session und Cookies

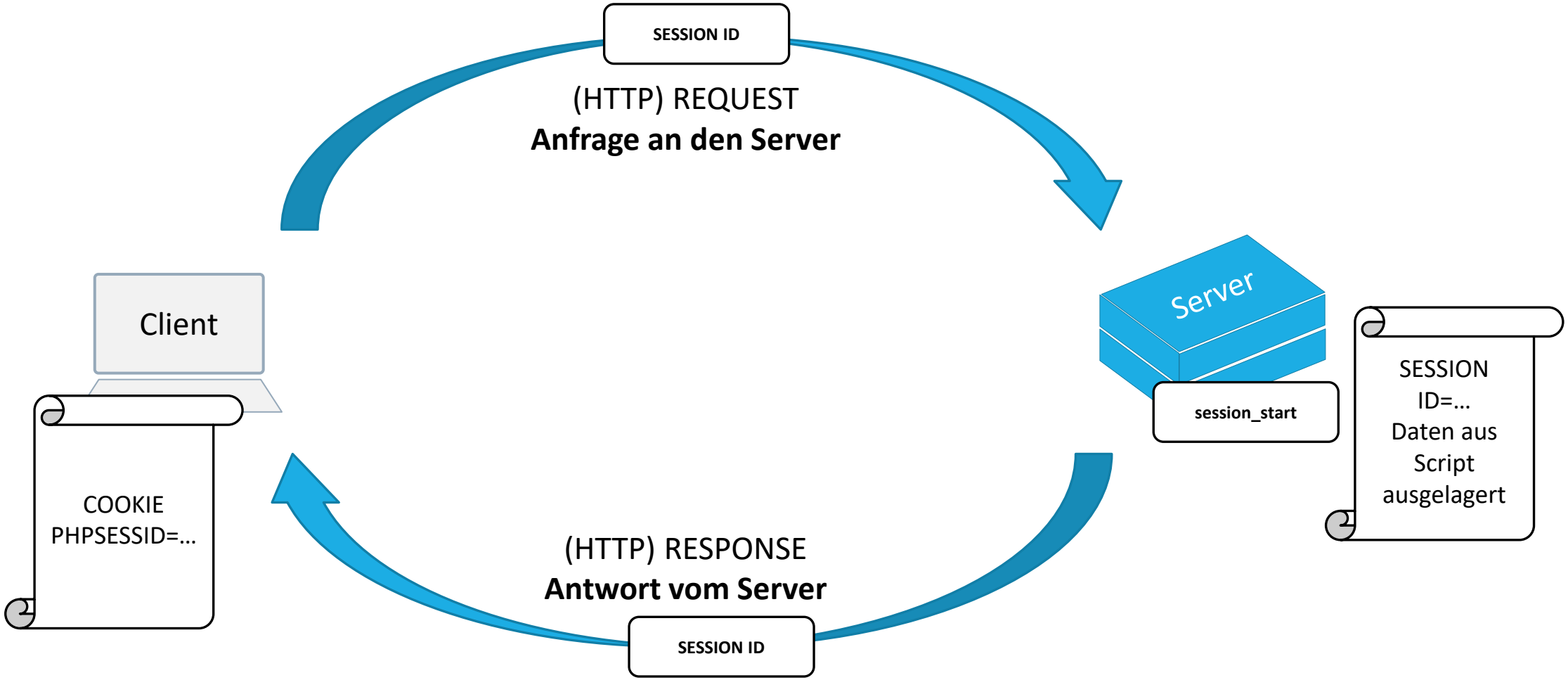
WIE SIE ALS TEMPORÄRER DATENSPEICHER DIENEN

Cookie im Server / Client Kreislauf



CLIENT: cookie	SERVER: session

Session im Server / Client Kreislauf



CLIENT: cookie	SERVER: session

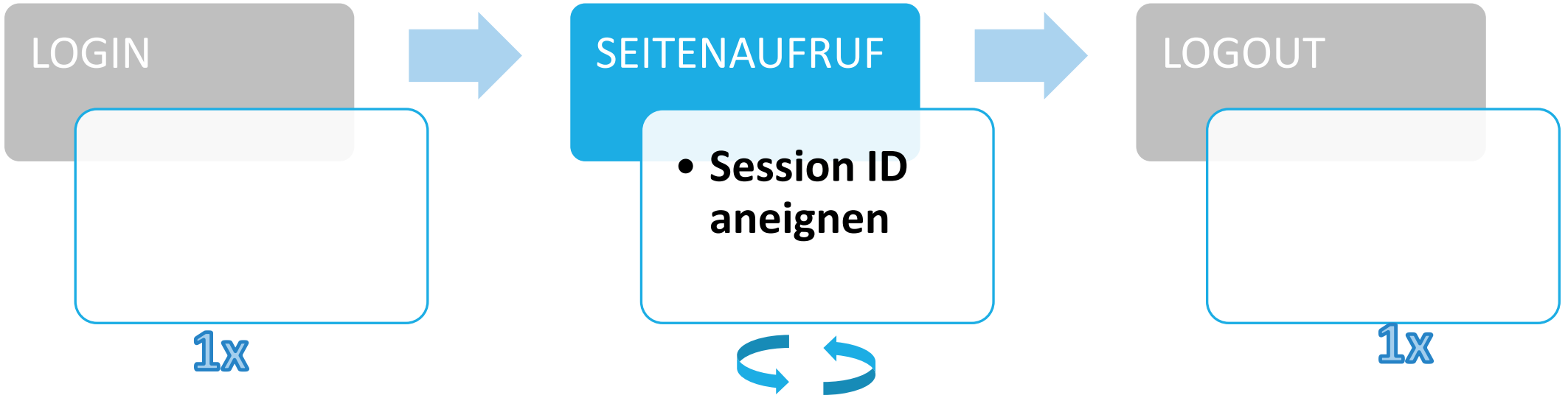
Angriffsflächen

WAS EIN HACKER VERSUCHEN WIRD…

Risiken: Session ID

DIE SESSION ID IST UNVERSCHLÜSSELT UND FREI ZUGÄNGLICH

Abfrageprozess umgehen



Session Hijacking

entführen einer Session ID – eigentlich Session ID Hijacking

Ein Hacker…

1. liest Session ID (mittels Spyware oder Sniffing)
2. legt auf seinem Computer ein Cookie mit der Session ID an
3. ruft Applikation über diesen Computer auf (Request mit Sesssion ID) und gibt sich als das Opfer aus

Session Fixation

Vorpräparieren einer Session ID – Session ID unterjubeln

Ein Hacker…

1. legt auf seinem Computer ein Cookie mit einer Session ID an
2. Verführt den ahnungslosen Benutzer, sich über ein präpariertes Formular an der Applikation anzumelden (z.b. via Phishing E-Mail)
3. Benutzer authentifiziert die schon existierende Session-ID mit seinem Login, statt eine eigene Session ID zu generieren
4. Hacker hat Zugriff

Massnahmen

Die wichtigsten Massnahmen zum Schutz eines Login-Bereichs

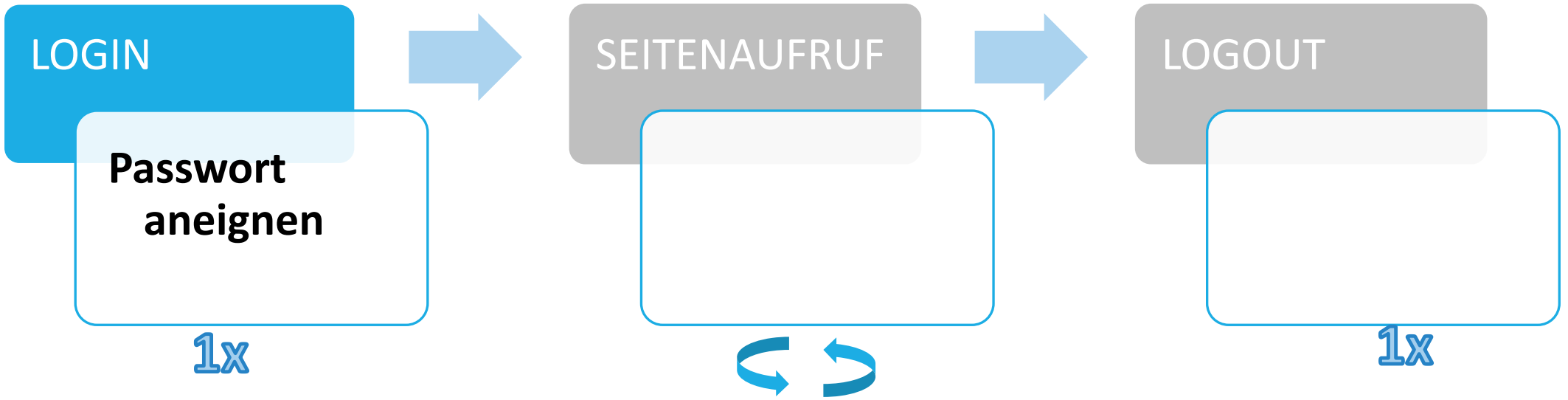
- Vom Standard abweichen – ID erraten unmöglich machen
- Angriffsfläche verkleinern – Gültigkeit der ID einschränken
- Herkunft prüfen – weitere Parameter zur Überprüfung speichern
- Mitlesen vermeiden – Sichere Verbindung erzwingen

Quelle und Details:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/WebSec/WebSec.pdf

Risiko: Authentifizierung

WAS EIN HACKER VERSUCHEN WIRD…

Authentifizierung ermöglichen



Passwort aneignen

Brute Force Attack: Ein Programm kombiniert alle gängigen Passworte und Usernames und probiert sie aus, bis es einen Zugriff erreicht hat

Rainbow / Hash Tables: Tabellen von schon bekannten Username/Passwort Kombinationen werden genutzt, wenn bei einem Datenbankzugriff die Hashes der Passworte bekannt werden

Massnahmen

Die wichtigsten Massnahmen zum Schutz des Login-Prozesses

- **Leaks unbrauchbar machen**: Passworte mit kryptologischem Algorythmus hashen
- **Erraten erschweren**: Sichere Passworte erzwingen
- *Möglichkeiten einschränken: Login-Fails limitieren mittels Zähler und Sperre*
- *Weitere Faktoren einbauen – 2FA*

