Winkelmann Domenico & Winkler Olivier

# Datenschutz

Datenschutz ist ein Begriff, der in der zweiten Hälfte des 20. Jahrhunderts aufgetaucht ist und wird teilweise unterschiedlich definiert & interpretiert. Je nachdem wird «Datenschutz» als Schutz von missbräuchlichen Daten, Schutz des Rechts von informationellen Selbstbestimmungen, Persönlichkeitsrechtsschutz & Schutz der Privatsphäre verwendet. Aus Sicht der ITC beinhaltet der Datenschutz organisatorische und technische Massnahmen gegen den Missbrauch von Daten innerhalb einer Organisation. Ursprünglich wurde aber mit Datenschutz der Schutz der Daten selbst verwendet (z.B. Datensicherung vor Verlust).

# Die wichtigsten juristische Punkte

- ***Schutzobjekt: natürliche Personen***
  Während das aktuell gültige Datenschutzgesetz von 1992 den Schutz von Daten von sowohl natürlichen als auch juristischen Personen regelt, beschränkt sich das neue Datenschutzgesetz auf Daten von natürlichen Personen.
- ***Sanktionen***
  Im Gegensatz zum bestehenden Datenschutzgesetz definiert der Entwurf des neuen Gesetzestextes klare Sanktionen. So können Individuen, die das neue Datenschutzgesetz Schweiz vorsätzlich verletzen, mit einer Busse von bis zu CHF 250’000 bestraft werden.
- ***Besonders schützenswerte Personendaten***
  Das neue Datenschutzgesetz erweitert die bestehende Auflistung von Daten, die unter die Kategorie der schützenswerten Personendaten fallen. Neu aufgelistet sind genetische und biometrische Daten (z.B. Fingerabdruck), die eine natürliche Person eindeutig identifizieren.
- ***Technikgestaltung und datenschutzfreundliche Voreinstellung***
  Datenverarbeiter erhalten strengere Sorgfaltspflichten, die genauer definiert sind. So müssen Verantwortliche für Daten und Datenverarbeitung bereits bei der Planung der Datenverarbeitung das Risiko einer Verletzung der Persönlichkeit angemessen verringern («privacy by design»). Zudem sind sie verpflichtet, mit geeigneten Voreinstellungen sicherzustellen, dass standardmässig nur für den jeweiligen Verwendungszweck erforderliche Personendaten bearbeitet werden («privacy by default»).
- ***Datenschutz-Folgenabschätzung***
  Datenverantwortliche oder Datenverarbeiter müssen nach dem neuen Datenschutzgesetz eine Datenschutz-Folgenabschätzung vornehmen, wenn die vorgesehene Datenverarbeitung zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt. Dabei müssen sie sowohl Risiken als auch geeignete Massnahmen umschreiben.
- ***Meldung von Verletzungen des Datenschutzes***
  *Datenverantwortliche müssen dem Eidgenössischen Datenschutz und Öffentlichkeitsbeauftragten (EDÖB) eine Datenschutzverletzung so rasch als möglich melden, wenn ein hohes Risiko für die Persönlichkeit oder Grundrechte der betroffenen Person besteht. Sofern erforderlich, müssen sie die betroffenen Personen zudem informieren.*

*Quelle: https://www.pwc.ch/de/dienstleistungen/consulting/risiken/datenschutz.html*

# Sichere Authentifikation

**OAUTH Authentication**

Bei dieser Methode wird dem Client ein «Access Token» von dem Server zugestellt. Somit können Daten/Services geschützt werden, indem nur authentifizierte User darauf zugreifen können. Im Scope bei der Anfrage können diverse Berechtigungen beim Authorization Server angefragt werden. Das Token ist hat jedoch eine zeitlich begrenzte Gültigkeit.

**SSO**

Unter «SSO» aka Einmalanmeldung wird in der IT ein einfaches Authentifizierungsverfahren verstanden. Dies besteht ausfolgenden Punkten:

- Ein Benutzer meldet sich einmalig an seinem Arbeitsplatz an. Er erhält dadurch Zugriff auf alle Rechner und Dienste (inklusive der Cloud), für die er lokal autorisiert ist, solange er sich am selben Arbeitsplatz aufhält. Sobald sich der Benutzer von seinem Arbeitsplatz abmeldet, entfallen alle Zugriffsrechte. Dies passiert entweder nach einem vorher festgelegten Zeitraum oder wenn der Benutzer manuell ein Single-Sign-Out bzw. -Off ausführt
- SSO wird für assoziierte aber voneinander unabhängige Anwendungen verwendet, da sich der Benutzer nur einmal anmelden muss und somit nicht bei jeder einzelnen Anwendung anmelden.
- Zudem ist SSO sehr benutzerfreundlich und kommt daher bei vielen privaten Anwendungen als auch im professionellen Bereich zum Einsatz.

**Zwei-Faktor-Authentifizierung**

Zwei-Faktor-Authentifizierung dient als Identitätsnachweis eines Nutzers mittels einer Kombination von zwei unterschiedlichen & unabhängigen Komponenten. Typische Beispiele für diese Methode sind Bankkarten plus PIN beim Geldautomaten, Fingerabdruck plus Zugangscode in Gebäuden oder Passphrase und TAN beim E-Banking. Zwei-Faktor-Authentifizierung ist ein Spezialfall der Multi-Faktor-Authentisierung.

**Multi-Faktor- Authentifizierung (Google Authenticator)**

Mit dem Google-Authenticator ist es möglich eine Zwei-Stufen-Authentifizierung zu ermöglichen. Mit dem Authenticator können Konten über ein Einmalkennwort einmalig verbunden werden und danach muss bei jeder Anmeldung zusätzlich der Code aus dem Authenticator angegeben werden.

**Touch- & FaceID**

Es gibt auch Authentifizierungen, die mit einmaligen Merkmalen des menschlichen Körpers funktionieren. Zum Beispiel sind Iris-Scanner bei Zutrittskontrollen zu Sicherheitsanalgen sehr verbreitet. Finger- & Gesichtserkennung sind ebenfalls verbreitete Methoden. Bei Touch- und FaceID werden die Daten für die Authentifizierung an einem speziell abgesicherten Bereich im Prozessor verschlüsselt gespeichert.

# Sicherheitsmechanismen in verwendeter Anwendung

**Backups**

Im Ticketverkauf werden die Systeme ständig abgeglichen und mehrere Backups auf diversen Plattformen erstellt. Dieses Verfahren passiert alle 10 Minuten und je nach Verwendung der Anwendung. Dabei werden vor allem Daten gespeichert, die häufig ändern wie z.B. Userdaten & Abfahrtszeiten (inkl. Verspätungen).

**Firewall & Antivirusprogramm**

Die Firewalls & Server für den Ticketverkauf werden von T-Systems verwaltet. Diese Infrastruktur wird stets auf dem neusten Stand gebracht und wird kontinuierlich überwacht. Die Server verfügen über einen Virusschutz und sind zudem mit Berechtigungen etc. geschützt. Die Server sind in einem sicheren Raum, Programme oder Scripte können nicht einfach so auf den Servern ausgeführt werden etc.

**Passwörter & Benutzeridentifikation**

Für die Software beim Ticketverkauf gibt es Administratoren, die diese anpassen können. Dies wird über einen Adminbereich gerelegt, bei dem nur bestimmte Personen Zugriff haben. Benutzer werden mit ihrem Benutzernamen und Passwort identifiziert oder zum Teil ein speziell für die Applikation angepasster Funktionsuser. Den Serverraum können nur bestimmte Personen mit den korrekten Berechtigungen diesen betreten und auf den Servern arbeiten.

# Allfällige Massnahmen

Die oben aufgelistete Sicherheitsmechanismen sind bereits in der vorhandenen Konfiguration in unserer Anwendung aktiv.

# Möglichkeiten von Verschlüsselungen

**Symmetrische Verschlüsselung**

Wird mit selbem Schlüssel verschlüsselt/entschlüsselt

**Asymmetrische Verschlüsselung**

Gibt zwei Schlüssel, der eine ist öffentlich zugänglich und der andere private Schlüssel wird geheim gehalten. Der öffentliche Schlüssel wird zur Verschlüsselung und der private zur Entschlüsselung verwendet.

**Nutzen der Verschlüsselung**

- gemeinsam genutzten Computer (Daten eines Benutzers sind für die Mitbenutzer unlesbar)
- unberechtigt Zugang zu einem Computer resp. den Daten ist nicht möglich
- Informationen auf mobilen Geräten wie Notebooks und USB-Speichermedien
- eMail werden über unsichere Pfade verteilt
- Nutzung von unsicheren WLAN in öffentlichen Bereichen -> Verschlüsselt kommunizieren
- **Vertraulichkeit**: Die Nachricht ist nur für denjenigen lesbar, für den sie bestimmt ist.
- **Authentizität**: Die Echtheit des Absenders wird gewahrt. Der Absender ist die Person (oder das System), welche als Absender angegeben wird.
- **Integrität**: Die Information wird auf dem Weg zwischen Absender und Empfänger nicht verändert
-

# Allfällige Massnahmen für verwendete Anwendung

Bei unserem online Ticketverkauf wäre eine asymmetrische Verschlüsselung notwendig.