3 Maßnahmen

3.0 Sicherheitsstrategien und Mechanismen

Üblicherweise unterscheidet man zwischen der **Strategie** (*policy*) und dem **Mechanismus** (*mechanism*).

Die Strategie spezifiziert, welche Maßnahmen (z.B.Zugriffe) berechtigt sind (sozusagen der SOLL-Zustand);

der Mechanismus bestimmt, welche Maßnahmen ausführbar sind (der IST-Zustand).

Im Idealfall ist ein Mechanismus eine präzise Implementation der gewählten Strategie:

- Ein Mechanismus heißt **präzise** (*precise*) bzgl. einer Strategie, wenn die Menge der ausführbaren Maßnahmen und die Menge der berechtigten Maßnahmen gleich ist.

- Ein Mechanismus heißt **sicher** (*secure*) bzgl. einer Strategie, wenn die Menge der ausführbaren Maßnahmen eine Teilmenge der erlaubten Maßnahmen ist
  ("es kann nur ausgeführt werden, was auch erlaubt ist").

3.1 Sicherheit im Spannungsfeld zwischen Ermöglichen und Begrenzen

Sicherheit steht stets im Spannungsfeld zwischen **Ermöglichen** (Gewährleisten) und **Begrenzen**:

Sie soll die eigentlichen Aufgaben ermöglichen (sicherstellen), anderes aber verwehren;
Unangenehmes verhindern, oder zumindest doch erkennen, dass Unangenehmes (z.B. Fälschungen, Dateneinbruch) stattgefunden hat.

Traditionelle Maßnahmen zur Begrenzung sind:

A) Unangenehmes verhindern:

- Verschlüsselung von Daten (*data encryption*):
  Die Daten sind zugreifbar, aber sie können nicht interpretiert werden.

- Kontrolle des Datenzugriffs (*access control*):
  Die Daten sind nur zugreifbar, wenn der Zugriffskontrolle die zugehörigen Rechte vorgewiesen werden.

- Kontrolle des Informationsflusses (*flow control*).
  Darf eine bestimmte Information dorthin fließen?

- Kontrolle der Folgerungen (*inference control*), d.h.
  der Information, die aus mehreren Datenbank-Antworten erschlossen werden kann.

B) Unangenehmes erkennen:

- Protokollierung zur Beweismittelsicherung, welche Operationen z.B. stattgefunden haben.
- kryptographische Methoden wie MAC (*message authentication code*) zur Erkennung von Veränderung (Fälschungen) von Dokumenten oder digitale Signaturen zur Erkennung von Fälschungen des Absenders.

Zur Wahrung der Funktionalität müssen aber auch die dualen Funktionen ermöglicht werden:

- Entschlüsselung von Daten,
- Gewährleistung des Zugriffs,
- Gewährleistung des Informationsflusses,
- Gewährleistung der Folgerungsmöglichkeiten.

Konsequenz aus dem Spannungsfeld zwischen Ermöglichen und Begrenzen ist:

Es müssen **erwünschte und unerwünschte Eigenschaften** (möglichst vollständig) **spezifizier**t werd**en**.

Was ist erwünscht? D.h., was soll ermöglicht werden?

Was ist unerwünscht? D.h., was soll begrenzt werden?

Wer ist vom (sicheren) System betroffen?

Wem dient die Sicherheit? Wer hat die Vorteile?

Wie werden die Risiken verteilt? Wer hat die Nachteile?

Soweit ein IT-System Teil der gesellschaftlichen Infrastruktur wird, soll primär nicht die Sicherheit der Technik erhöht, sondern die Verletzlichkeit der Gesellschaft verringert werden.

3.2 Duale Sicherheitsfunktionen

Die Dualität setzt sich technisch fort. Je nachdem, wer sich sicherfühlen will, braucht man Funktionen der einen oder anderen Seite:

Identifikation ↔ Anonymität
Authentisierung ↔ Pseudonymität
Rechte ↔ Pflichten
Beweissicherung ↔ Unbeobachtbarkeit

Für jede dieser Sicherheitsfunktionen gibt es in unserer Gesellschaft etablierte Anwendungen:

a) **Identifikation ↔ Anonymität**:

Barzahlung beim Einkauf, vorbezahlte Telefon-(Chip-)karte ermöglichen Anonymität,
Tafelgeschäfte bei der Bank (als Spezialfall der Barzahlung) leben von Anonymität;

Bezahlung per Überweisung / Kreditkarte / ec-Karte verlangen Identifikation.
Eine (auch vorbezahlte) Handy-Chipkarte kann der Identifizierung dienen.
Eigentum: Eigentümer will sich sicherfühlen (Identifikation), Dieb will sich sicherfühlen (Anonymität).

Beim Telefonieren ist i.a. Identifikation erwünscht, aber auch da gibt es Ausnahmen: Seelsorge, Zeugnistelefon etc. bedingen Anonymität.

Geldscheine sind identifizierbar (aber kaum einer kümmert sich drum, es sei denn es stammt aus Lösegeld, Banküberfällen etc.), Geldmünzen sind anonym.

b) **Authentisierung ↔ Pseudonymität**

Authentisierung wird verlangt durch Vorzeigen eines Personalausweises / Passes z.B. bei Grenzübertritt oder bei Bankgeschäften (z.B. Kontoeröffnung);
durch Eingabe einer Personlichen Identifikationnummer (PIN) beim Geldabheben von Geldautomaten.

Pseudonymität (eine Person hat mehrere Namen) kommt öfter vor bei Autoren von Büchern oder Zeitungartikeln, im technischen Bereich z.B. alias unter UNIX.
Aber auch: Eine Person mit mehreren Kreditkarten oder Geldkarten.

c) **Rechte ↔ Pflichten**

Durch Rechte geregelt sind große Teile unseres Lebens angefangen durch das Grundgesetz: Grundrechte, Bürgerrechte (Wahlrecht), Recht auf Forschungsfreiheit, Recht auf Unversehrtheit der Wohnung, Versammlungsfreiheit.

Umgekehrt Pflichten:
Bürgerpflichten (Schulpflicht, Wehrpflicht, Pflicht zur Übernahme eines Ehrenamtes (Schöffe, Wahlvorstand…), Pflicht zur Hilfeleistung in Notfällen, (Ärztliche) Schweigepflicht, Pflicht zur Schadensbegrenzung, Haftpflicht

d) **Beweissicherung ↔ Unbeobachtbarkeit**

Beweissicherung z.B. durch Protokollierung / Aktenvermerke ist verbreitet insbesondere im gesamten Verwaltungsbereich.
Am bekanntesten ist vielleicht die Anzeige / Unfallprotokollierung durch die Polizei.
(Problem der Fälschungssicherheit). Weiterhin durch Zeugen.

Zur Unbeobachtbarkeit sind in unserer Gesellschaft eine Reihe von Geheimnissen kodifiziert: z.B. Briefgeheimnis, Fernmeldegeheimnis, geheime Wahlen.

3.3 Idee der Informationsflusskontrolle

Zum Entwurfszeitpunkt muss also ein Rahmen festgelegt werden:
Welche Person (oder welche Position in einem Unternehmen) hat welche Aufgaben (Verpflichtungen)?

Ein solcher Rahmen folgt i.a. zwei Entwurfsprinzipien:

dem Prinzip der **Aufgabentrennung** (*separation of duties*) zwischen Benutzern und

dem Prinzip der **kleinstmöglichen Berechtigungen** (*least privilege*) von Benutzern.

Für jede Aufgabe muss festgelegt werden:

Welche Informationsflüsse müssen gewährleistet werden, damit die Aufgabe erfüllt werden kann?
(z.B. Versandabteilung eines Versandhauses muss Aufträge kennen)

Welche Informationsflüsse dürfen nicht stattfinden, damit die Aufgabe erfüllt werden kann?
(z.B. Klausuraufgaben dürfen Studierenden nicht vor der Klausur bekannt sein)

Gegen welche Informationsflüsse ist die Aufgabe immun (d.h. Welche Informationsflüsse sind egal für die Aufgabenerfüllung)?

Eine Definition des Informationsflusses ist schwierig, sie muss den Begriff der Information formalisieren und das jeweils relevante "Vorwissen" des Empfängers berücksichtigen.

Informationsflusskontrolle in allgemeiner Form ist unentscheidbar.
Denn nutzen Sender und Empfänger eine universelle Programmiersprache, so müsste man insbesondere erkennen können, ob eine bestimmte Anweisung (die einen Informationsfluss bewirken kann) überhaupt ausgeführt wird.
Dies ist äquivalent zum Halteproblem.

Als Ausweg bietet sich die **mittelbare Kontrolle des Informationsflusses durch die Kontrolle des Zugriffs** an:

Durch Zugriffsrechte kann man Informationsflüsse ermöglichen (die zur Erfüllung der Aufgabe dienen), durch fehlende Zugriffsrechte oder Zugriffsverbote kann man Informationsflüsse verhindern (die zur Erfüllung der Aufgabe nicht stattfinden sollen).

Allerdings wird durch Zugriffsrechte nicht geregelt, dass Informationsflüsse wirklich stattfinden (nur die Möglichkeit dazu wird geschaffen).

Außerdem ist das "Raster" der Zugriffskontrolle recht grob: In der Regel schafft man es nur, durch Zugriffskontrolle die gewünschten Informationsflüsse angenähert zu modellieren.