2. Bedrohungen

I.a. muss ein Teilnehmer damit rechnen, dass seine mit dem jeweiligen Dienst verbundenen Interessen bedroht werden. Solche **Bedrohungen** können sehr unterschiedliche Urheber oder Ursachen haben.

Die Spanne der **Urheber einer Bedrohung** reicht

- vom Interesseninhaber selbst über
- die anderen am Dienst unmittelbar beteiligten Teilnehmer oder
- die bei seiner Implementierung beteiligten Teilnehmer bis hin zu
- anderen im Rechensystem befugt arbeitenden Teilnehmern oder
- dort unbefugt eingedrungenen Teilnehmern und sogar zu
- den Herstellern, Vertreibern und Unterhaltern des Rechensystems.

Die Urheber können die Bedrohungen

- harmlos **versehentlich** oder
- bösartig **absichtlich**

auslösen.

Die Möglichkeiten der **Ursachen einer Bedrohung** reichen von

- unsachgemäßen Anforderungen über
- fehlerhafte Implementierungen oder
- falsche Inbetriebnahmen bis hin zu
- misslichen äußeren Einflüssen.

2.1 Risiken und Schäden; Schutz und Sicherheit

Eine **Gefahr** (von außen) und eine **Schwachstelle** des Systems zusammen ergeben ein **Risiko**.

Tritt das gefährliche Ereignis ein, so gibt es einen **Schaden**.

Maßnahmen zur Verhinderung oder Begrenzung des Schadens werden **Schutz** (*protection*) genannt.

Maßnahmen zur Vermeidung, Beseitigung und Verminderung des Risikos werden **Sicherung**,

der anschließende Zustand **Sicherheit** (*security*) genannt.

Schutz und Sicherung stehen also zueinander wie Feuerwehr und vorbeugender Brandschutz.

Das Risiko kann bewertet werden mit Hilfe der **Schadenswahrscheinlichkeit** und
der (durchschnittlichen oder maximalen) **Schadenshöhe**.

In Alltagssituationen gibt das Produkt aus Schadenswahrscheinlichkeit und durchschnittlicher Schadenshöhe einen guten Anhaltspunkt.

Ist allerdings die Schadenswahrscheinlichkeit sehr klein und die Schadenshöhe sehr groß, ist die maximale Schadenshöhe eine wichtige Zusatzinformation.

Eine Verkleinerung des Risikos kann also durch Verringerung bzw. Beseitigung der Schwachstellen im System oder durch Verringerung der Gefahr von außen erreicht werden.

Das Messen der Schadenshöhe ist manchmal problematisch.
Z.B. ist bei immateriellen Schäden (z.B. Gesundheitsschäden, Andenken) eine Bewertung in Geld oft nicht möglich bzw. nicht intersubjektivierbar.

Sicherheit (im Gegensatz zu Schutz) ist in hohem Maße dann wichtig, wenn ein System Schwachstellen mit potentiell großen Schadenshöhen hat (umgangssprachlich: von einem System hohe Risiken ausgehen) (z.B. Prozesssteuerungen bei Energieerzeugung oder chemischen Prozessen) oder

sich die Gesellschaft weitgehend von der Funktionsweise eines Systems abhängig gemacht hat (z.B. elektronischer Geldtransfer).

Es gibt Wechselwirkungen zwischen Bedrohung und Sicherheitsmaßnahmen:
Strengt man sich lieber dabei an, die Sicherheitsmaßnahmen zu vergrößern (Zäune höher…)
oder versucht man, die Bedrohungen zu verringern?

2.2 Beherrschbarkeit von IT-Systemen

Ein wichtiger Grundsatz ist, dass IT-Systeme **beherrschbar** sein müssen.

Die wird erleichtert insbesondere durch

- die **Durchschaubarkeit** der Wirkungen einer Operation für den Benutzer ("der Benutzer soll wissen, was er tut") und für die Betroffenen ("Betroffene sollen wissen, was mit ihnen passiert"),

- die **Rückverfolgbarkeit** einer Wirkung zu den auslösenden Operationen (um Verantwortlichkeiten zu modellieren),

- eine **korrekte Funktionalität**, die -mathematisch beweisbar oder technisch garantierbar- mit der Spezifikation übereinstimmt.

Damit verbunden sind Fragen nach der

• **Rückholbarkeit** eines Systems (kann man die Einführung eines Systems wieder rückgängig machen?)
und der

• **Verantwortbarkeit der Nutzung** eines Systems für den individuell verantwortlichen Benutzer.

Zu unterscheiden sind zwei komplementäre Sichten auf Sicherheit:

- **Sicherheit der Systeme**:

Weder Informationen (Daten) noch ihre Verarbeitung (Funktionen, Prozesse) dürfen unzulässig beeinträchtigt werden in ihrem Bestand oder ihrer Verfügbarkeit.

Dies ist eine Kernfrage bei der **Konstruktion** eines Systems.

- **Sicherheit der Betroffenen**:

Rechte (oder schutzwürdige Belange) der Betroffenen dürfen durch Vorhandensein oder Nutzung von IT-Systemen nicht unzulässig beeinträchtigt werden.

Dies ist eine Kernfrage (spätestens) beim **Einsatz** eines Systems.

Aber Gewährleistung der Sicherheit der Betroffenen benötigt evtl. andere Konzepte (wie Zuordbarkeit, Verantwortlichkeit), die die Konstruktion eines geänderten/erweiterten Systems verlangen.

Sicherheit der Betroffenen ist zunächst die **Sicherheit eines Einzelnen**.

Sicherheit der Betroffenen ist (z.B. bei Automatisierung von Infrastruktur) aber auch **Sicherheit der Gesellschaft**:

Daher: IT-Systeme müssen **gesellschaftlich verträglich** und **verfassungskonform** sein.

Daraus resultieren Ziele wie "informationelle Selbstbestimmung" (BVerfG 1983) oder Verfügungsrecht über eigene Rollen.

Setzt ein Unternehmen IT-Systeme ein, so bedeutet Sicherheit der Betroffenen i.a. auch **Sicherheit des Unternehmens**.

Daher: IT-Systeme dürfen keine **Eigendynamik** entwickeln, sondern müssen mit den Unternehmenszielen verträglich bleiben.