

„Pistes de réflexion“ zur Haftung von IT-Herstellern

Welche **typischen Sicherheitsrisiken** gilt es im Rahmen von IT-Projekten zu berücksichtigen? Insbesondere:

- **Vertraulichkeit** von Daten im Rahmen der Projektrealisierung und beim Betrieb eines Informationssystems
- **Angriffe** Dritter/Übergriffe von Mitarbeitern auf das Informationssystem
- Unbeabsichtigte **Veränderung oder Löschung von Daten**
- **Nichtverfügbarkeit** von Daten und Systemen wegen Mängeln

Wie können Sicherheitsrisiken **reduziert** werden? Beispiele:

- **Auswahl** eines Vertragspartners, welcher Kompetenz und längerfristige Verfügbarkeit (z.B. auch im Hinblick auf Konkursrisiken) gewährleisten kann
- Vermeidung von Unklarheiten bei der **Leistungsdefinition** (z.B. in Pflichtenheften, Service Level Agreements), Claim/Change Management Verfahren zur nachträglichen Konkretisierung und Anpassung von Leistungsinhalten
- Fortlaufende Analyse und **Information über Risiken**
- **Technische Vorkehrungen** (z.B. Systemredundanzen, Einbau spezifischer Sicherheitskomponenten, Parallelbetrieb während Transitionsphasen)
- **Organisatorische Vorkehrungen** bei Anbieter und Anwender (z.B. Implementierung und regelmässige Aktualisierung eines Sicherheitskonzepts, Konkretisierung von Mitwirkungspflichten im Rahmen eines Claim Management Verfahrens)
- **Kontrollen** während des laufenden Projekts (z.B. Integrationsabnahme, Monitoring von IT-Dienstleistungen), periodische **IT-Sicherheitsüberprüfungen** auch nach Projektabschluss
- Permanente **Wartung und Pflege** von sicherheitsrelevanten Systemen

Wer trägt die typischen IT-Sicherheitsrisiken sofern deren Verteilung vertraglich nicht geregelt ist?

- IT-Anbieter:
 - Lieferung von Systemen, die den **vertraglich zugesicherten oder vorauszusetzenden Eigenschaften entsprechen**
 - sorgfältige **Erbringung von Dienstleistungen**
 - Wahrnehmung von **Mitwirkungs- und Aufklärungspflichten**
- IT-Anwender:
 - **Aufrechterhaltung der technischen Voraussetzungen**, von welchen die Parteien bei Vertragsschluss ausgingen (z.B. Systemarchitektur, IT-Infrastruktur)
 - Einhalten von **Vorgaben des Anbieters** (z.B. Bedienung des Systems, Installation von Patches, Vorgehen bei Systemveränderungen)
 - **Schadensverhütung** insbesondere durch übliche organisatorische Massnahmen (z.B. Administration von Zugriffsberechtigungen, Datensicherung und Recovery Management)
 - Wahrnehmung von **Mitwirkungs- und Aufklärungspflichten**

Vertraglichen Mechanismen zur Risikoverteilung:

- **Explizite vertragliche Zuweisung** bestimmter Risiken, z.B. im Rahmen der Leistungsdefinition in Pflichtenheften und Service Level Agreements, Zusicherungen und Garantieverprechen
- Definition der **Einsatzbedingungen eines Informationssystems**
- Beeinflussung des **Haftungsmassstabs** durch Angaben zur vorausgesetzten Fachkompetenz
- Vertragliche **Konkretisierung von Informationspflichten** (z.B. erkannte Mängel, Erfolglosigkeit von Reparaturleistungen, Ausfall von Rechenleistungen), **Mitwirkungspflichten** (z.B. bei Fehlersuche) und **Schadensvermeidungspflichten** (z.B. Datensicherung/Disaster Recovery Planning)
- **Haftungsbeschränkungsklauseln**
- Verwirkungs- und **Verjährungsbestimmungen**

- Bindung der Geltendmachung von Ansprüchen an **verfahrensmässige Voraussetzungen** (z.B. Abnahmeverfahren, Rüge- und Abmahnungsmodalitäten, Streit-erledigung)
- Regeln über **Beweislastverteilung und Nachweis eines Verschuldens**
- **Konventionalstrafen und Schadenspauschalierung**

Ist die Tragung bestimmter Risiken durch die eine Vertragspartei ökonomisch effizienter oder gerechter?

- Who is the cheapest risk avoider?
- Who is the cheapest risk insurer?