Deutsch Wyss
& Partner

IT-Risikomanagement
9. November 2006

IT-Haftungsrisiken
und rechtliche Vorsorgemöglichkeiten

Wolfgang Straub

Überblick

- **Haftungs- und Gewährleistungskonstellationen**
- **D&O-Ansprüche**
- **Risikoanalyse und Risikoverteilung in IT-Verträgen**

Haftungskonstellationen

Was bei Ausfall/Fehlfunktion von IT-Systemen alles schief laufen kann…

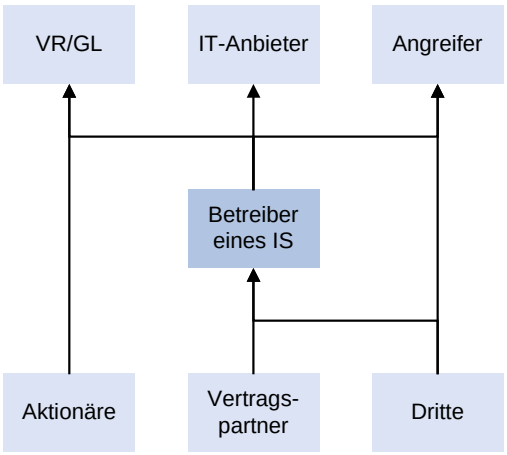
- → Datenverlust/-verfälschung
- → Verletzung von Datenschutz- und Aufbewahrungsvorschriften
- → Fehlsteuerung von Prozessen
- → Produktionsausfall
- → Zugriffsmöglichkeiten Unbefugter
- → Imageverluste
- → Drittschäden

Haftungskonstellationen

Ursachen von Schädigungen durch IT

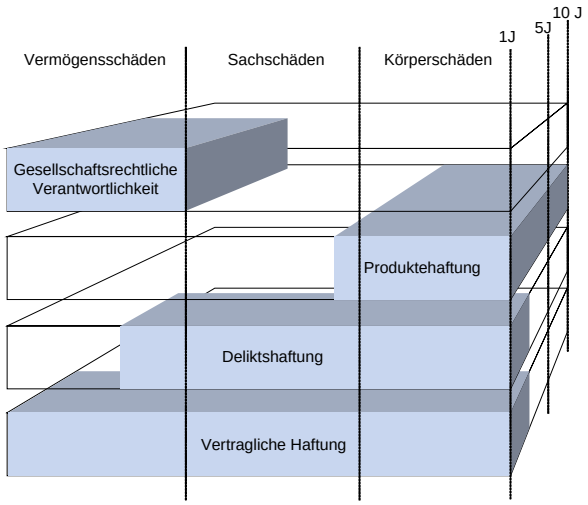
- Konzeptions-, Implementierungs- und Bedienungsfehler
- Einflüsse der IT-Infrastruktur/Interdependenzprobleme
- Mangelhafte Leistungen von Vertragspartnern
- Angriffe Dritter

Haftungskonstellationen



4 I 25

Haftungskonstellationen



5 I 25

Beispiel

Fehlerhafte Zinsabrechnung wegen Softwarefehler

→ Wiederherstellung/Auseinandersetzung mit Kunden

- Keine Produktehaftung für Datenschäden
- Vertragliche Ansprüche gegen Softwarehersteller?
- Arbeitsvertragliche Ansprüche gegen IT-Verantwortliche?
- Verantwortlichkeitsansprüche gegen GL/VR?

Haftungskonstellationen

Warum IT-Verträge selten perfekt erfüllt werden

- Unklarheiten in Leistungsdefinitionen
- Statistische Fehlerinhärenz von Software
- Interdependenz- und Schnittstellenprobleme
- Projektänderungen

Haftungskonstellationen

Warum Gerichtsverfahren selten sind

- Notwendigkeit der weiteren Zusammenarbeit
- Prozessrisiken
  - Nebenpflichten / Abmahnungsobliegenheiten
  - Schadensvermeidung / Schadensminderung
  - Dokumentation / Reproduzierbarkeit
- Unzulänglichkeit von Gerichtsverfahren (Dauer, technisches Verständnis etc.)

Haftungskonstellationen

Fragen in Haftungs- und Gewährleistungsfällen

- Welche vertraglichen/gesetzlichen Haftungs- und Gewährleistungsregeln sind anwendbar?
- Vertragliche Haftungsbegrenzungen?
- Verwirkung von Ansprüchen (z.B. Verjährung)?
- Eigene Mitverantwortung an Schadensentstehung → Schadensvermeidungspflichten
- Beweisbarkeit und Beweislastverteilung?
- Durchsetzbarkeit (z.B. Solvenz)?

Haftungskonstellationen

D&O-Ansprüche

Wer untersteht der Haftung? (Art. 754ff. OR)

- **Verwaltungsrat**
- **Geschäftsleitung**
  - erste Führungsebene (Direktoren)
  - ausnahmsweise untergeordnete Mitarbeiter
  - faktische Organe
- **Revisoren/Revisionsgesellschaften**

D&O-Ansprüche

Wofür wird gehaftet?

- Unsorgfältige Handlungen
- Unterlassungen trotz Pflicht zum Handeln

D&O-Ansprüche

Verwaltungsrat

- **Nicht delegierbare Pflichten** (Oberleitung/ Oberaufsicht) → Bestimmung strategischer Ziele der IT
- **Delegation** durch VR-Beschluss → periodische Überprüfung des Delegationsumfangs
- **Sorgfalt bei Auswahl, Instruktion und Überwachung** von Delegationsempfängern (intern und extern)
- Internes **Kontrollsystem** und **Riskmanagement** (Swiss Code of Best Practice for Corporate Governance 19)
- Massnahmen zur **Compliance** (Swiss Code 20)

D&O-Ansprüche

Geschäftsleitung

- Korrekte **Weiterdelegation** (Auswahl, Instruktion und Überwachung)
- **Sorgfaltspflichten** → Schaffung eines Informationssicherheits-Konzept, Umsetzung und Kontrolle, Bereitstellen der notwendigen Ressourcen

D&O-Ansprüche

Sorgfaltsmassstab

- Objektivierte Betrachtungsweise (was konnte von einem typischen VR/GL-Mitglied erwartet werden?)
- Abhängig von Unternehmensgrösse
- Abhängig vom Schadenspotenzial/Bedeutung der IT für das betreffende Unternehmen
- Messbarkeit und Dokumentation
- Bedeutung von Standards (z.B. ISO/IEC 17799, COBIT, Grundschutzhandbuch, ITIL)?
- Bedeutung von Zertifizierungen?

D&O-Ansprüche

Anwendungsbereich in der IT

- Unsorgfältig geplante oder realisierte IT-Projekte (inkl. vertragliches Riskmanagement)
- Vernachlässigung von Informationssicherheit, Disaster Recovery Planning etc.
- Schadenersatzansprüche Dritter aufgrund unsorgfältiger Leistungen (insbesondere schwerwiegende Organisationsfehler)
- Bilanzierungsfehler wegen unsachgemässer Bewertung wesentlicher Risiken

D&O-Ansprüche

Haftung aus Arbeitsrecht

- Organe sind oft arbeitsvertraglich angestellt oder stehen in einem Auftragsverhältnis → vertragliche Ansprüche der Gesellschaft
- Art. 321e OR: Berücksichtigung des Berufsrisikos, der erforderlichen Fachkenntnisse und der individuellen Eigenschaften des Arbeitnehmers, die der Arbeitgeber kennen musste
- IT als schadensgeneigte Tätigkeit?

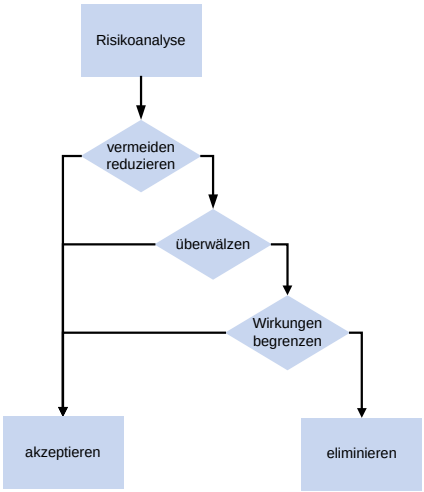
Beispiel

Brand eines Netzteils im RZ

→ Beschädigung von Hardware →Datenverlust → Produktionsausfall → Ansprüche von Kunden

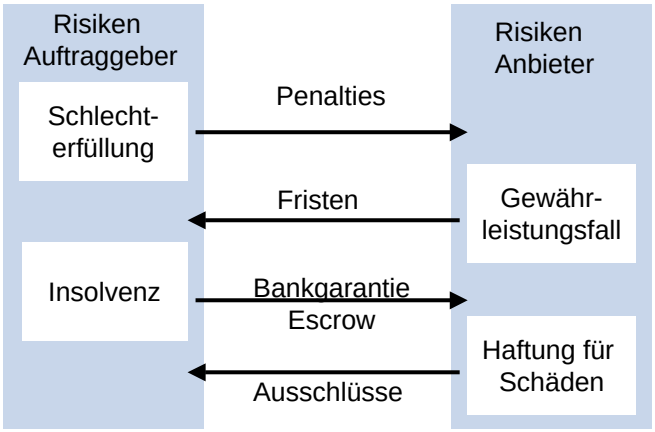
- Produktehaftung des Geräteherstellers?
- Vertragliche Ansprüche gegen Hardwarelieferant
- Schadensverhütungsmöglichkeit durch Früherkennung
- Schadensminderung durch Datensicherung/BCM
- Arbeitsvertragliche Ansprüche gegen IT-Verantwortliche?
- Verantwortlichkeitsansprüche gegen GL/VR?

Risikovorsorge

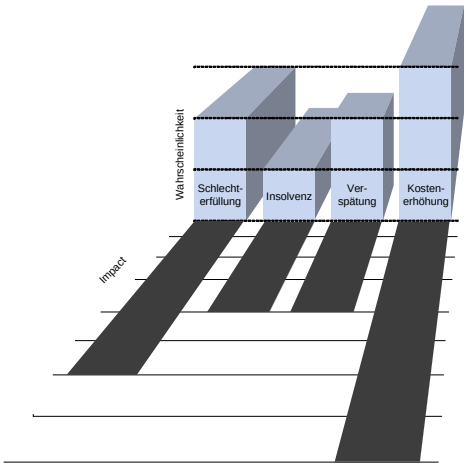


Risikovorsorge

Vertragliche Risiken



Risikovorsorge



Risikovorsorge

Beispiel einer Risikomatrix

Trend	Beschreibung Risiko	Proba-bility	Impact	Risiko faktor	Massnahmen
⇨	Verspätung	3	4	12	Hard Milestones mit Konventionalstrafen, periodische Fortschrittskontrolle
⇧	Kostenerhöhung	3	3	9	Kostendach mit Frühwarnung, CHF als Vertragswährung, periodische Kosteninformation
⇨	Scheitern Abnahme XY	3	3	9	Vorabnahme, Vertragsauflösungsmöglichkeit bei definitivem Scheitern
⇩	Insolvenz	3	3	9	Konzerngarantie, Escrow von Sourcecode und Dokumenten
NEU	Koordination Teilprojekte A und B	3	3	9	Gemeinsames Claim Management Verfahren, Integrationsabnahme
⇧	Management der Abhängigkeiten und Abgrenzungen mit anderen Projekten	3	2	6	Koordinationsmeetings, Verfahren zur Definition von Schnittstellen

Probability: Wahrscheinlichkeit dass ein Risiko eintritt (1: tief, 2: eher tief, 3: eher hoch, 4: hoch)
Impact: Auswirkung falls das Risiko eintritt (1: tief, 2: eher tief, 3: eher hoch, 4: hoch)
Risikofaktor: Multiplikation aus Probability und Impact

Risikovorsorge

Vertragsverhandlungen

- Regeln zu Risikosphären und Beweislastverteilung (z.B. Verantwortlichkeitsmatrix mit Auffangregeln)
- Informationsmechanismen, Kontrollrechte
- Verfahrens- statt spezifikationsorientiertes Vertragsdesign
- Claim Management Verfahren
- Erfolgsabhängige Zahlungsvoraussetzungen
- Auflösungsmodalitäten

Risikovorsorge

Vertragsvollzug

- Verfahrensregeln einhalten (z.B. Change Management)
- Nebenpflichten beachten (z.B. Mitwirkung)
- Erkennbare Vertragsverletzungen abmahnen
- Schäden verhüten (z.B. Datensicherung, Business Continuity Management)
- Konflikte frühzeitig bereinigen
- Eigene Sorgfalt dokumentieren

Risikovorsorge

Verwaltungsrat und Geschäftsleitung

- Verfügbarkeit von IT-Infrastruktur und -Prozessen als Ziel der strategischen Geschäftsplanung behandeln
- Zweckmässigen Organisation schaffen
- Formell korrekte Delegation der Ausführung
- IT-Sicherheitskonzept
- Nötige Mittel bereitstellen
- Periodische Berichterstattung
- Periodische Kontrolle (IT Security Audits)
- Angemessene Reserven für Restrisiken bilden