

6. Berner Tagung für Informationssicherheit 2003

# **Delegieren von IT-Sicherheitsaufgaben Rechtliche Aspekte**

Dr. Wolfgang Straub, LL.M.

Advokaturbüro Deutsch & Wyss, Bern

Lehrbeauftragter am Departement Informatik der  
Universität Fribourg

# Übersicht

- Ist die Verantwortung für Informationssicherheit delegierbar?
- Welche Regeln gelten für Outsourcing- und MSS-Verträge?
- Praktische Hinweise zur Vertragsredaktion
- Datenschutzproblematik
- Wer haftet für Sicherheitsverletzungen?

# Verantwortlichkeit von Geschäftsleitung von Verwaltungsrat

- Pflicht zur sorgfältigen Oberleitung und Organisation → **zweckmässige Organisation** der Informationssicherheit (Art. 716a/717 OR)
- **Controlling und Reporting**
- **Verantwortlichkeitsansprüche** von Aktionären und Gläubigern bei ungenügender Erfüllung von Leitungs- und Kontrollpflichten (754 OR)

# Dauerdienstleistungsverträge

- **Arbeitserfolg**
- Bestimmte **Dauer**
- Eventuell **Rahmencharakter**
- Kombination mit **Elementen anderer Vertragstypen** (Werkvertrag, Auftrag, Lizenzen etc.)

# Generelle Hinweise zur Vertragsredaktion

- **Konsistenzprüfung**
- **Koordinationsproblematik**
- Konkretisierung von **Mitwirkungspflichten**
- **Dokumentation** von Änderungen
- **Controlling**
- **Eskalationsverfahren**
- **Preisbestimmung**
- **Auflösungsmodalitäten**

# Service Level Agreement

- Definition der **Voraussetzungen**, unter welchen die Leistung zu erbringen ist
- Bestimmung der **Messkriterien/Methoden**
- **Gewichtung** der Kriterien/Bestimmung von Key Service Levels
- Relevanter **Zeitraum**
- Was gilt während **Transitionsperioden**?

# Nebenpflichten

- Konsultation vor sicherheitsrelevanten **Veränderungen** (z.B. Einspielen von Softwareupdates)
- Information über **Leistungseinschränkungen**
- Beratungspflichten bei **Einzelaufträgen**
- **Disaster Recovery**
- Unterstützung beim **Backsourcing**

# Datenschutz

- **Datenherrschaft** muss beim Kunden bleiben
- Angemessene **Schutzvorkehrungen** für besonders schützenswerte Daten und Persönlichkeitsprofile
- Besondere vertragliche oder gesetzliche **Geheimhaltungspflichten**, Sonderregelung für Banken (Art. 47 BankenG)
- Besondere Regeln für **grenzüberschreitende Datenverarbeitung** (Art. 6 DSGVO)
- **Geheimhaltungsrevers**

# Haftung

- Verschiedene **Haftungsebenen**
- **Sorgfaltsmassstab**
- **Haftungsausschlüsse** heben qualifizierte Zusicherungen nicht auf!
- **Mitverschulden** des Geschädigten
- **Konventionalstrafen**
- Eventuell Regeln zur **Beweislastverteilung**
- **Dokumentation**
- **Versicherungsdeckung**