UNIVERSITÉ DE FRIBOURG SUISSE
UNIVERSITÄT FREIBURG SCHWEIZ

iimt information security brush-up workshop 11/02/2003
measuring information security –
state of the art and best practices

Rechtliche Aspekte von Informationssicherheitsmessungen

Dr. Wolfgang Straub

Überblick

- Sicherheitsmessungen als **Kontrollinstrument** von Geschäftsleitung, Verwaltungsrat und Revisoren
- Sicherheitsmessung als Instrument der **Qualitätsprüfung** von IT-Leistungen
- **Persönlichkeits- und Datenschutz**
- **Vertraglicher Regelungsbedarf** vor Sicherheitsüberprüfungen

2

Pflicht zur Sicherheitskontrolle

Zweckmässige Organisation der Informationssicherheit als **Aufgabe von Geschäftsleitung und Verwaltungsrat** (Art. 716a/717 OR):

- Periodisches **Controlling und Reporting** über Informationssicherheit im Unternehmen
- **Verantwortlichkeitsansprüche** von Aktionären und Gläubigern bei ungenügender Wahrnehmung von Leitungs- und Kontrollpflichten (754 OR)

Strafrechtliche **Überwachungspflichten**
(Art. 12 Cybercrime Convention des Europarats)

3

Qualitätsprüfung von IT-Leistungen

Sicherheit als Qualitätselement von IT-Leistungen

- Sicherheitsprüfungen bei der **Abnahme** von integrierten IT-Systemen (Art. 367 OR)
- Bewertung der Informationssicherheit für **leistungsabhängige Vergütungen** (Outsourcing, Service Level Agreements)
- Bedeutung von Sicherheitsmessungen bei der Beurteilung von **Sorgfaltpflichten** (vertragliche und ausservertragliche Haftungsarten)

4

Daten- und Persönlichkeitsschutz

Verhältnis von Datenschutz und Sicherheitsüberprüfungen:

- Sicherheitsüberprüfungen als **Kontrollmittel** zur Einhaltung des Datenschutzrechts (Art. 7 DSG) →Pflicht zur periodische Überprüfung der technischen und organisatorischen Massnahmen zum Datenschutz (Art. 8 Abs. 3 VDSG)
- Daten- und Geheimnisschutz als Grenze der Zulässigkeit von Sicherheitsüberprüfungen (insbesondere **Anforderungen** des Datenschutzrechts beim Beizug externer Personen zur Sicherheitsmessung)

5

Daten- und Persönlichkeitsschutz

Besondere Anforderungen des Datenschutzrechts zum Schutz bestimmter Datenkategorien

- Daten, welche gesetzlichen oder vertraglichen Geheimhaltungspflichten unterliegen
- Besonders schützenswerte Daten und Persönlichkeitsprofile
- Sonstige personenbezogene Daten

6

Daten- und Persönlichkeitsschutz

Geheime Daten (Art. 14 DSG)

‚Das Bearbeiten von Personendaten kann einem Dritten übertragen werden, wenn:

… keine gesetzliche oder vertragliche Geheimhaltungs-pflicht es verbietet …‘

Dem Bearbeiten grundsätzlich gleichgestellt sind Tätigkeiten im Rahmen von Sicherheitsüberprüfungen, welche Zugriff auf entsprechende Daten ermöglichen.

7

Daten- und Persönlichkeitsschutz

Geheime Daten (Art. 321 StGB)

1. Geistliche, Rechtsanwälte, Verteidiger, Notare, nach Obligationenrecht zur Verschwiegenheit verpflichtete Revisoren, Ärzte, Zahnärzte, Apotheker, Hebammen sowie ihre Hilfspersonen, die ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist, oder das sie in dessen Ausübung wahrgenommen haben, werden, auf Antrag, mit Gefängnis oder mit Busse bestraft. …
2. Der Täter ist nicht strafbar, wenn er das Geheimnis auf Grund einer Einwilligung des Berechtigten oder einer auf Gesuch des Täters erteilten schriftlichen Bewilligung der vorgesetzten Behörde oder Aufsichtsbehörde offenbart hat.

8

Daten- und Persönlichkeitsschutz

Besonders schützenswerte Daten (Art. 3 DSG)

Daten über:

1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
3. Massnahmen der sozialen Hilfe,
4. administrative oder strafrechtliche Verfolgungen und Sanktionen

9

Daten- und Persönlichkeitsschutz

Besonders schützenswerte Daten und Persönlichkeitsprofile (Art. 12 DSG)

‚Wer Personendaten bearbeitet, darf … insbesondere nicht ohne Rechtfertigungsgrund:

… besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekanntgeben.‘

10

Daten- und Persönlichkeitsschutz

Besonders schützenswerte Daten (Art. 13 DSG)

‚Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. …'

11

Daten- und Persönlichkeitsschutz

Besonders schützenswerte Daten (Strafbestimmung Art. 35 DSG)

‚Wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekanntgibt, von denen er bei der Ausübung seines Berufes, der die Kenntnis solcher Daten erfordert, erfahren hat, wird auf Antrag mit Haft oder mit Busse bestraft. …'

12

Daten- und Persönlichkeitsschutz

Sonstige Personendaten

- **Art. 2 DSG**
  - Bearbeitung nach Treu & Glauben
  - Verhältnismässigkeit
  - Zweckbestimmung
- **Art. 8 ff. VDSG**
  - Kontrollen
  - Protokollierung

13

Daten- und Persönlichkeitsschutz

Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis)

‚Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.‘

14

Vertraglicher Regelungsbedarf

Rechtliche Einordnung: generelle Anwendbarkeit von **Auftragsrecht**

Leistungsbeschreibung

- Was ist **Ziel** der Sicherheitsmessung?
- **Vertragsleistung**: Penetration Test, Audit, Assessment?
- Definition der zulässigen **Methoden und Mittel**

15

Vertraglicher Regelungsbedarf

Daten- und Geheimnisschutz

- Problematik der Strafbarkeit des **Eindringens in Informationssysteme** →Einwilligung des Inhabers/Abgrenzung notwendig
- Problematik vertraglicher oder gesetzlicher **Geheimhaltungspflichten** →Einwilligung aller möglichen Betroffenen notwendig.
- Kein unnötiger Zugang zu **besonders schützenswerten Personendaten**

16

Vertraglicher Regelungsbedarf

Daten- und Geheimnisschutz

- Umfassende **Geheimhaltungspflicht für Auftragnehmer**
- Wahrung des **Verhältnismässigkeitsprinzips** bei Sicherheitsüberprüfungen
- Kontrolle, technische Schutzvorkehren, Protokollierung und Dokumentation für **geheime und besonders schützenswerte Daten**

17

Vertraglicher Regelungsbedarf

Nebenpflichten

- Informations- und **Unterstützungspflichten**
- **Aufklärung** über Risiken →Vorsorgemassnahmen des Auftraggebers
- Beizug **Dritter** zur Vertragserfüllung
- Folgen der **vorzeitigen Vertragsbeendigung**
- **Versicherung** von Risiken
- **Ansprechspersonen**
- Schriftlichkeit von Vertragsmodifikationen

18