Rechtliche Verantwortung für das ICT Risk Management

12. Berner Tagung für Informationssicherheit 2009

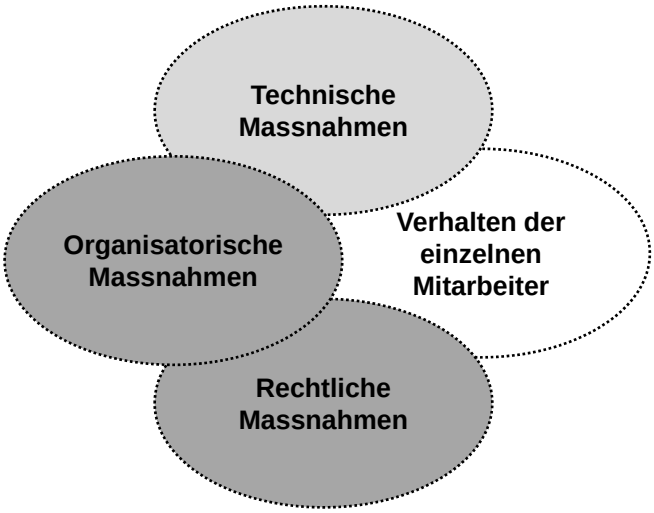
Dr. Wolfgang Straub
Deutsch Wyss & Partner

‘SQL injection’ gegen Webshop

- → Kundendaten der letzten 15 Jahre werden manipuliert
- → Vorfall wird publik
- → Umsätze brechen ein

- Existierte ein adäquates Risk Management?
- Wer ist für Schäden verantwortlich?

Sicherheit und Risk Management



Pflichten des Unternehmens

- **Vertraulichkeitspflichten**
  - → **Schutz von Personendaten** (DSG)
  - → **Berufsgeheimnisse**, z.B. im medizinischen oder juristischen Bereich (siehe auch Art. 321 und 11 StGB)
  - → **Sektorielle Bestimmungen** (z.B. im Telco-Bereich)
  - → **Vertragliche Verpflichtungen** gegenüber Zulieferern und Kunden
- **Informations- und Nachweispflichten**
  - → **Steuerrechtliche** Nachweispflichten
  - → **Aufbewahrungsvorschriften** (z.B. GeBüV)

Verantwortlichkeit der Organe

Gegen wen sind Verantwortlichkeitsklagen möglich?

- Gründer
- Verwaltungsrat
- Geschäftsleitung
- Revisoren

Ergänzung durch arbeits- und auftragsrechtliche Ansprüche

Verantwortlichkeit der Organe

Anwendungsbereich in der IT

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

Verantwortlichkeit der Organe

Verwaltungsrat

- **Nicht delegierbare Pflichten** (Oberleitung/ Oberaufsicht) → Bestimmung strategischer Ziele der IT
- **Sorgfalt bei Auswahl, Instruktion und Überwachung** von Delegationsempfängern (intern und extern)
- Internes **Kontrollsystem** und **Risk Management**
- Massnahmen zur **Compliance** (→ Swiss Code of Best Practice for Corporate Governance)

Verantwortlichkeit der Organe

Geschäftsleitung

- Schaffung eines **Informationssicherheits-Konzepts**, Umsetzung und Kontrolle, Bereitstellen der notwendigen Ressourcen
- Korrekte **Weiterdelegation**, Auswahl, Instruktion und Überwachung der Ausführung

Verantwortlichkeit der Organe

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
- Bedeutung von **Standards** & Best Practices (z.B. ISO/IEC 17799, Weisungen über die Informatiksicherheit in der Bundesverwaltung, EBK RS 99/2 «Outsourcing»)?
- Bedeutung von **Zertifizierungen**?

Verantwortlichkeit vermeiden

US Federal Trade Commission

Verpflichtung zur Realisierung eines vollständigen Informationssicherheitsprogramms

- Definition der **Verantwortlichkeiten** innerhalb des Unternehmens
- **Risikoanalyse**
- Implementierung von **Sicherheitsmassnahmen**
- **Maintenance** der Sicherheitselemente
- Periodische **Überprüfung** (Audits)

Verantwortlichkeit vermeiden

Organisatorische Massnahmen

- IT-Ziele und eine IT-Strategie definieren
- Sicherheitsanalyse durchführen (lassen)
- Sicherheitskonzept/Weisungen verabschieden
- Vertragspartner integrieren
- Periodische Überprüfung (→ Audits)
- Dokumentieren der eigenen Sorgfalt (Entscheide und Massnahmen)

Verantwortlichkeit vermeiden

Rechtliche Massnahmen

- **Verantwortlichkeiten definieren**
- Formell korrekte **Delegation** (→Organisationsreglement)
- **Plausibilitätskontrolle** von Expertenvorschlägen
- Sorgfältige Auswahl, Instruktion und **Überwachung der Delegationsempfänger**
- IT und Sicherheit regelmässig **traktandieren**
- **Interessenkonflikte** offenlegen
- Abschluss einer **D&O-Versicherung** mit ausreichender Deckung

Verantwortlichkeit vermeiden

Risk Management für Verträge

- Regeln zu Risikosphären und Beweislastverteilung (z.B. Verantwortlichkeitsmatrix mit Auffangregeln)
- Informationsmechanismen, Kontrollrechte
- Erfolgsabhängige Zahlungsvoraussetzungen
- Auflösungsmodalitäten
- Rückstellungen für Restrisiken
- …

Ergebnisse

- Die Verantwortung für Informationssicherheit lässt sich nie vollständig delegieren - auch nicht durch Outsourcing!
- Nicht alle Risiken lassen sich eliminieren (Zielkonflikte).
  → Auch das nachvollziehbare Akzeptieren gewisser Risiken führt zur Entlastung.

Fragen, Kritik, Anregungen?

Wolfgang Straub
Deutsch Wyss & Partner
Effingerstrasse 17/Postfach 5860
CH-3001 Bern

+41 31 381 44 25

wolfgang.straub@advobern.ch
www.advobern.ch