

Risiken und Haftungsfragen für Sicherheits- und Führungskräfte

mag. iur. Maria Winkler

Geschäftsführerin der IT & Law Consulting GmbH

SSI-Fachtagung vom 28.10.2010
„Unternehmenssicherheit - Neue Herausforderungen“

Themen

- Verantwortung für Informationssicherheit
- Gesetzliche Grundlagen der Informationssicherheit
- Sichere Verträge und ihre Grenzen
- Was wird mit einer Zertifizierung erreicht?

Verantwortung der Unternehmensführung

- Der VR ist verantwortlich für die **Oberleitung der Gesellschaft** und für die Erteilung der nötigen Weisungen.
- Er muss die **Einhaltung von Gesetzen und Weisungen** überprüfen und ist verantwortlich für die Ausgestaltung des **Rechnungswesens und der Finanzkontrolle**.
- Er kann diese Pflichten nicht delegieren und haftet für deren Verletzung (Art. 754 OR).

Risikomanagement

- Der VR ist daher zuständig für die Regelung von Verantwortlichkeiten, den Erlass von **Weisungen** und deren Kontrolle, die Bereitstellung der erforderlichen Infrastruktur sowie der personellen und finanziellen **Ressourcen**.
- Der VR muss zudem gemäss Art. 663b Ziff. 12 OR im Anhang der Jahresrechnung Angaben über die Durchführung einer **Risikobeurteilung** machen.

Identifikation der relevanten Bereiche

- Es sind die für das eigene Unternehmen aufgrund des **eigenen Tätigkeitsbereichs** geltenden **gesetzlichen Anforderungen** zu erheben und die Massnahmen für die Umsetzung einzuleiten.
- Zudem müssen die wesentlichen **Risiken** erhoben werden – dabei sind die Bedingungen im technischen, wirtschaftlichen, sozialen und politischen Umfeld darzulegen, da diese sich sehr rasch ändern.

Informationssicherheit

- Informationen stellen für Unternehmen, unabhängig von ihrem konkreten Tätigkeitsgebiet, einen wichtigen unternehmerischen Wert dar.
- Verschiedene gesetzliche Grundlagen verpflichten die Unternehmen, ihre Organe und Mitarbeitenden, die Informationen, welche im Unternehmen bearbeitet werden, zu schützen.
- Dazu zählen z.B. Normen über die kaufmännische Buchführung (**Records Management**), der **Datenschutz**, das Verbot der Verletzung von **Geschäfts- und Betriebsgeheimnissen**, die Pflicht zur Führung eines **Internen Kontrollsystems (IKS)**, etc.

Records Management

- Buchführungspflichtige Unternehmen müssen alle **geschäftsrelevanten Unterlagen** mindestens 10 Jahre ab Ende des Geschäftsjahres archivieren (Art. 957 ff. OR).
- Die elektronische Archivierung der Geschäftsunterlagen ist zulässig (Ausnahme: Bilanz und Erfolgsrechnung), wenn u.a. die **Integrität** und **Verfügbarkeit** während der gesamten Archivierungsfrist sichergestellt werden.
- Zudem enthalten Spezialgesetze oft Normen, welche indirekt die Erstellung und Archivierung bestimmter Unterlagen verlangen (z.B. Produkthaftpflichtgesetz).

Datenschutz

- Bei der Bearbeitung von Personendaten sind die Vorgaben des Datenschutzgesetzes zu beachten (z.B. Personaldaten, Kundendaten, etc.).
- Das Datenschutzgesetz verlangt unter anderem, dass Personendaten angemessen vor dem Zugriff unberechtigter Dritter oder zufälligem Verlust oder Zerstörung geschützt werden (**Datensicherheit**).

Geheimhaltungspflichten

- Wer ein **Geschäfts- oder Fabrikationsgeheimnis**, das er aufgrund einer gesetzlichen oder vertraglichen Pflicht bewahren soll, verrät oder für sich oder andere ausnutzt, ist **strafbar** (Art. 162 StGB).
- Verträge mit Lieferanten oder Kunden verbieten häufig die Weitergabe von Geschäfts- oder Fabrikationsgeheimnissen an Dritte – dies muss durch ausreichende Sicherheitsmassnahmen gewährleistet werden.

Internes Kontrollsystem IKS

- Die **Implementierung eines funktionierenden IKS** gehört zu den Aufgaben des Verwaltungsrats (Art. 716a Ziff. 3 OR, Art. 728a OR und Art. 728b OR).
- Ein funktionierendes IKS ist daher als Bestandteil guter Corporate Governance zu sehen.

Sorgfaltspflichten

- Bei der Umsetzung der verschiedenen gesetzlichen Vorschriften stellt der Gesetzgeber auf die erforderliche **Sorgfalt** ab.
- Diese wird meist anhand des „**aktuellen Standes der Technik**“, des aktuellen Standes der Wissenschaft etc. ermittelt.

Erfüllung der Sorgfaltspflichten

- Im Rahmen der Informationssicherheit müssen unter anderem die folgenden Massnahmen ergriffen werden, um die gesetzlich geforderten Sorgfaltspflichten zu erfüllen:
 - Sorgfältige Auswahl und Instruktion der Mitarbeitenden
 - Erlass von Weisungen und Kontrolle von deren Einhaltung
 - Bereitstellung der erforderlichen Ressourcen
 - Evaluation der anwendbaren gesetzlichen Bestimmungen
 - Sorgfältige Auswahl von Lieferanten
 - Sorgfältige Erstellung von Verträgen

Beispiel Cloud Computing

- Es handelt sich (aus rechtlicher Sicht) um einen **Outsourcingvertrag**, welcher die folgenden besonderen Merkmale aufweist:
 - Die Daten werden an verschiedenen geographischen Orten bearbeitet.
 - Daten werden in der Regel (auch) im Ausland bearbeitet.
 - Es besteht eine grosse Abhängigkeit vom Anbieter sowie vom Netz.

Compliance

- Im Rahmen von Cloud Computing wird ein Teil der eigenen Geschäftstätigkeit zu einem externen Unternehmen ausgelagert.
- Zahlreiche gesetzliche Vorschriften halten fest, dass das Outsourcing zwar erlaubt ist, der Auftraggeber aber für das **Funktionieren** und die **Gesetzeskonformität** der ausgelagerten Tätigkeit **verantwortlich** bleibt (z.B. Art. 10a DSGVO).
- Zudem dürfen keine gesetzlichen oder vertraglichen **Geheimhaltungspflichten** bestehen, welche das Outsourcing verbieten.

Umsetzung

- Wegen der grossen Abhängigkeit vom Anbieter muss bei der **Evaluation** sehr sorgfältig vorgegangen werden.
- Zudem ist zu überprüfen, ob die angebotene Dienstleistung die **gesetzlichen Anforderungen** erfüllt (z.B. Buchführungsvorschriften) bzw. welche Auflagen zur Herstellung der Gesetzeskonformität gemacht werden müssen.
- Bestehen **Geheimhaltungspflichten**, dann ist ein Outsourcing in die Cloud unter Umständen unzulässig (z.B. Banken).

Vertrag

- Der Anbieter muss ausdrücklich verpflichtet werden, die Daten nur für den **vereinbarten Zweck** zu bearbeiten, die Weitergabe an Dritte sollte ausdrücklich untersagt werden!
- Es sollte zudem vertraglich geregelt werden, **in welchen Ländern** die Datenbearbeitung erfolgt, da eine Weiterleitung von Personendaten ins Ausland nur zulässig ist, wenn im Empfängerland eine angemessene Gesetzgebung herrscht (Art. 6 DSG).
- Zudem sollten **Informationspflichten** und **Kontrollrechte** vereinbart werden.

Zusammenfassung

- Im Rahmen des Cloud Computings erzeugt die Kombination verschiedener Elemente besondere Risiken, welche durch das Unternehmen erkannt und wenn möglich reduziert werden müssen.
- Es muss grundsätzlich geklärt werden, ob das Outsourcing in die Cloud für den beabsichtigten Bereich zulässig ist und welche gesetzlichen Vorgaben einzuhalten sind.
- Die sorgfältige Auswahl des Anbieters und die sorgfältige Ausarbeitung von Verträgen sind dabei zentrale Elemente der Risikoreduktion!

Sichere Verträge

- Die sorgfältige Ausarbeitung von Verträgen gehört zur gesetzlich verlangten Sorgfaltspflicht.
- Die **Definition des Vertragsgegenstandes** sowie durchdachte Regelungen über **Vertragsänderungen** und die **Vertragsbeendigung** helfen, die unternehmerischen Risiken so weit als möglich zu reduzieren.
- Zudem sollten die eigenen **Mitwirkungspflichten** vertraglich festgehalten werden.

Konfliktregelungen

- Auch gut durchdachte Verträge verhindern nicht, dass der Vertragspartner die Leistung nicht oder nicht korrekt erbringt!
- Die Rechte und Pflichten bei **mangelhafter Leistung** sowie bei **Verzug** sollten klar bestimmt sein.
- Zudem müssen die **Haftungsbestimmungen** den Risiken des Unternehmens entsprechen.
- Es ist zu beachten, dass die Haftung für Absicht und grobe Fahrlässigkeit nicht ausgeschlossen werden kann.

Zertifikate

- Der Gesetzgeber fördert im Bereich des Datenschutzes die **Selbstregulierung** – durch den Erwerb eines Zertifikats kann man sich von der Meldepflicht für Datensammlungen befreien (Art. 11 DSG).
- Die Anforderungen an die Zertifizierung sind in der **Verordnung über die Datenschutzzertifizierung** geregelt (VDSZ), welche wiederum auf ISO 27001 abstellt.

Managementsystem

- Sowohl die VDSZ als auch ISO 27001 verlangen ein **systematisches Vorgehen** beim Schutz von Informationen.
- Verlangt werden unter anderem die Regelung der Verantwortlichkeiten, der Erlass einer Politik, die Dokumentation der Prozesse, die Schulung der Mitarbeitenden, die Durchführung interner Audits, etc.
- Dadurch soll sichergestellt werden, dass Datenschutz bzw. Informationssicherheit gemanagt werden.

Folgen der Zertifizierung

- Eine Zertifizierung z.B. nach ISO 27001 und/oder der Erwerb eines Datenschutzzertifikats kann dem Unternehmen, dem Unternehmer, der GL, dem VR, etc. den Nachweis der Einhaltung der erforderlichen Sorgfalt beim Schutz der geschäftlichen Informationen erleichtern!
- Dies **kann** das Abwenden der persönlichen Haftung erleichtern, ist aber keine Garantie für eine Haftungsbefreiung!

Schlussbemerkung

- Die Sicherstellung der Einhaltung der gesetzlichen Vorschriften, die Regelung der Kompetenzen und Verantwortung sowie die Definition von Vorgaben über den Umgang mit geschäftlichen Informationen ist **Chefsache**.
- Dabei muss die **Verfügbarkeit** von Informationen und Dokumenten sowie die **Integrität** von Geschäftsdokumenten sichergestellt werden.
- Neben den Buchführungsvorschriften muss auch den Anforderungen von Spezialgesetzen, des Datenschutzes sowie von Geheimhaltungspflichten genügend Beachtung geschenkt werden.

Vielen Dank!

mag. iur. Maria Winkler
IT & Law Consulting GmbH
Grafenaustrasse 5
6300 Zug
maria.winkler@itandlaw.ch
www.itandlaw.ch
+41 41 711 74 08

SSI-Fachtagung vom 28.10.2010
„Unternehmenssicherheit - Neue Herausforderungen“