security zone newsletter
PLATTFORM FÜR INFORMATIONSSICHERHEIT

Risk Management und IT-Sicherheit

Risiken sind seit eh und je dauernde Begleiter des Menschen. Im privaten wie im beruflichen Umfeld gehen wir tagtäglich, bewusst oder unbewusst, eine Vielzahl von Risiken ein und müssen damit leben. Die Art dieser Risiken haben sich vor allem für Unternehmungen in den letzten Jahren verändert. Dies zum einen mit der steigenden Durchdringung des Lebens, speziell des Geschäftslebens, mit Computing und zum anderen (z.T. auch dadurch damit verbunden) mit der fortschreitenden Globalisierung

Ursula Sury

Ursula Sury ist selbständige Rechtsanwältin in Luzern (CH) und leitet die Studienrichtung Management + Law an der Hochschule Luzern – Wirtschaft. Sie ist zudem Dozentin für Informatikrecht an verschiedenen Nachdiplomstudien, welche am Institut für Wirtschaftsinformatik der Hochschule durchgeführt werden. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig.

Gefahren und Risiken

Gefahren, d.h. allgemeine Bedrohungen für die Unternehmung, ergeben sich aus dem Managementprozess, aus dem Geschäftsprozess oder aus dem Unterstützungsprozess einer Unternehmung. Aber auch von Akteuren aus dem unternehmerischen Umfeld, wie beispielsweise von Mitarbeitenden, Kunden, der Konkurrenz, Lieferanten oder von staatlicher Seite können Gefahren entstehen (vgl. dazu Rüegg-Stürm Johannes, das neue St.Galler-Management-Modell, Bern 2003).

Ursache für die Gefahren können durch Handlungen oder Unterlassungen von Unternehmen oder Dritten heute gesetzt werden, sich aber erst in Zukunft auswirken. Die Auswirkung von Gefahren ist rechtlich gesprochen grundsätzlich der Eintritt von Schaden, welcher sich in Geld messen oder mind. ungefähr bestimmen lässt. Sobald Gefahren nach Häufigkeit d.h. Eintrittserwartung und Auswirkung konkret geschätzt und systematisiert werden, spricht man von Risiken.

Risikotragung

"Qui ne risque rien, ne gagne rien!" heisst ein altes Sprichwort. Nebst der Tatsache, dass nur wer tot ist, keine Risiko mehr trägt, gehört das bewusste Eingehen und auch Einkalkulieren von Risiken zum unternehmerischen Handeln schlechthin. Folglich müssen sich Unternehmensverantwortliche auch überlegen, wie mit Risiken umzugehen ist, damit ein möglicher Risikoeintritt nicht die Existenz des ganzen Unternehmens gefährdet.

Riskmanagement: Prävention

Wer Riskmanagement betreibt, analysiert im obgenannten Sinn die möglichen Gefahren, die aus dem unternehmerischen Handeln (strategisch oder operativ) oder aus dem Umfeld entstehen

können, und bewertet diese nach Schadensgrösse, Schadensart und Eintrittswahrscheinlichkeit. Als nächstes wird überlegt, welche Risiken sinnvollerweise zu vermeiden sind, welche zu vermindern sind und welche man gegebenenfalls an eine Drittperson überwälzen kann.
Um Risiken zu vermeiden oder zu vermindern können verschiedenste Massnahmen getroffen werden, welche auch eine Vielzahl rechtlicher Instrumente beinhalten. Auch bei der Frage der Überwälzung sind rechtliche Überlegungen notwendig, so ob sie wirksam auf einen Haftpflichtigen überwälzt werden kann oder ob sich eine Versicherung findet, welche den Schaden eingetretener Risiken übernimmt.

Riskmanagement: Reaktion
Zum Riskmanagement zählt aber auch die Planung, wie mit einer eingetretener Krise korrekt umgegangen werden soll, damit der Schaden möglichst klein gehalten werden und aus dem eingetretenen Schaden für die Unternehmung viel gelernt werden kann. Es braucht folglich eine Überwachung sämtlicher möglicher Risikoherde und die Installation einer Krisenorganisation, die unverzüglich die Krise bewältigt. Die Überwachung impliziert dabei einerseits die Identifikation der Krise aber auch die Beurteilung resp. Bewertung, damit anschliessend die adäquaten Bewältigungsmassnahmen getroffen und umgesetzt werden können.

IT-Sicherheit und Riskmanagement
Das Einhalten von IT-Sicherheit im Unternehmen ist somit ein wesentlicher Beitrag zum Riskmanagement. Wie schon früher ausgeführt, impliziert IT-Sicherheit, damit sie effektiv und effizient umgesetzt werden kann, eine Vielzahl von rechtlichen Aspekten (vgl. dazu Sury Ursula, „Rechtliche Aspekte der IT-Sicherheit", Informatikspektrum vom 20.06.2002). So beispielsweise bei der korrekten Gestaltung sämtlicher IT-relevanten Verträge wie mit Software- und Hardwarelieferanten, im Bereich Providing, Housing, Hosting, Webdesign, mit Freelancern und Mitarbeitenden, mit Geschäfts- und Einzelkunden im B2B- und B2C-Bereich etc.

Rechtssicherheit und Riskmanagement
Das Sicherstellen von Rechtssicherheit, d.h. der Ausschluss von Prozess- und Schadenrisiken wegen schlecht gestalteten oder ungeklärten Rechtssituationen oder Rechtsbeziehungen, zählt in der Informationsgesellschaft in steigendem Mass zum Bedürfnis von Unternehmungen und somit zu einem wesentlichen Teil des Riskmanagement. Klagen wegen Urheberrechtsverletzungen, Datenschutzverletzungen, Markenverletzungen, unzulässigem Gebrauch von Domainnamen, Versenden unzulässiger Inhalte übers Internet (Computerkriminalität), unzulängliche Archivierung elektronischer Dokumente etc. sind heute ernst zu nehmende Bedrohungen. Sehr viele dieser Bedrohungen lassen sich durch rechtzeitige Abklärung und korrekte Gestaltung von Beziehungen oder unternehmerischen Prozesse (beispielsweise Daten archivierung) mit Weisungen und Policys vermeiden. In diesem Sinne sind die Spezialisten von Leagel Compliance und Rechtsanwältinnen und Rechtsanwälte nicht nur, wie traditionell gehandhabt, erst nach Schadeneintritt beizuziehen, sondern sinnvollerweise schon bei der Umsetzung eines sinnvollen Riskmanagement-Prozesses.

Versicherungen im IT-Umfeld
Eine mögliche Strategie, eingetretene Risiken zu überwälzen, ist der Abschluss von Versicherungen. Bei den Schäden im besprochenen Kontext (Dienstleistungsbereich) handelt es sich in aller Regel um Vermögensschäden, die astronomische Höhen erreichen können. Analysiert man die gängigen Standardprodukte der Versicherungsgesellschaften, so stellt man fest, dass Versicherungen für reine Vermögensschäden, entstehen diese aus dem Betrieb innerhalb der eigenen Unternehmung oder aus Nicht- und Schlechterfüllung von vertraglichen Verpflichtungen gegenüber Dritten, kaum versicherbar sind. Wohl finden sich Produkte für den Abschluss von Versicherungen für Schäden an Hardware, will man diese aber auf die Übernahme von Schäden, die sich aus Datenverlusten ergeben, ausdehnen, stösst man auf Unverständnis. Selbst wenn sich die grundsätzliche Bereitschaft zur Übernahme gewisser, sehr eingeschränkter Vermögensschäden ergibt, sind die **Anforderungen betreffend Sorgfalt** an den Versicherungsnehmer so gross, dass die Wahrscheinlichkeit eines Schadeneintritts wieder gegen null tendiert.
Auch im Bereich des Underwriting bemühen sich die Versicherungen immer mehr, die Unternehmen in Risk Management Verhalten zu zwingen, werden diese doch auf Herz und Nieren geprüft, bevor man mit ihnen

gewisse Versicherungen überhaupt abschliesst.

Corporate Governance

Im Rahmen der weltweiten Diskussion von Corporate Governance und der damit verbundenen (Rück-) Besinnung auf die Verantwortlichkeit der Verwaltungsräte drängt sich auch die Frage der Verantwortung für die IT-Sicherheit auf. Das strategische Führungsorgan einer jeden Unternehmung ist insbesondere dafür verantwortlich, dass die Unternehmung zweckmässig organisiert ist und die Gesetze eingehalten werden. Diese Aufgaben müssen, wie andere auch, mit aller Sorgfalt erfüllt werden, damit die Interessen der Gesellschaft in guten Treuen gewahrt werden (vgl. beispielsweise CH OR, Artikel 716a, 717). Werden diese Pflichten absichtlich oder fahrlässig nicht eingehalten, haften die Mitglieder des Verwaltungsrates persönlich und solidarisch für den entstandenen Schaden (vgl. dazu CH OR, Artikel 754, 759).

Dass die Implementation IT-Sicherheit wesentliche organisatorische Fragen beinhaltet, liegt auf der Hand. Auch die Einhaltung von Gesetzen kann zu grossen Teilen, beispielsweise im Bereich Datenschutz, nur mittels der Instrumente der ITSicherheit erreicht werden. Aber auch bei der Implementation verschiedener neuer technischer Errungenschaften, wie Intrusion Detection, RFID, Trust Computing etc. ist die rechtliche Dimension rechtzeitig einzubeziehen, um Gesetzesverletzungen vorzubeugen. In diesem Sinne kann durchaus gesagt werden, dass das organisatorische und strategische Sicherstellen von Informatiksicherheit heute zu den Pflichten eines Verwaltungsrates gehören (vgl. dazu auch Sury Ursula „Verantwortung und Haftung für menschliche Fehler im IT-Bereich", Zeitschrift Schweizer Informatik Nr. 6/2000).

Zusammenfassung

Zusammenfassend kann festgehalten werden, dass:

- IT-Sicherheit ein wesentlicher Aspekt von Risk Management ist
- Schäden im IT-Bereich schlecht abgewälzt werden können
- die Verantwortlichkeit für IT-Sicherheit Führungssache ist