Prof. Dr. Reinhard Voßbein[1]

Management von Risiken der IT-Sicherheit/IT-Security

Inhalt

Die Beherrschung von Risiken gehört zu den strategischen Aufgaben eines Unternehmens und sichert den mittel- und langfristigen Geschäftserfolg. Ein zentraler interner Erfolgsfaktor ist die organisatorisch und technisch sichere Abwicklung der Geschäfte. Sie bezieht sich auf die mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens. Ein typisches Beispiel hierfür ist die *Business Continuity*. Hier werden insbesondere die Kernprozesse des Unternehmens durch entsprechende technische und organisatorische Maßnahmen so abgesichert, dass eine Beeinträchtigung der Funktionalität nach menschlichem Ermessen ausgeschlossen werden kann. Es sollte jedoch ein auf die Aufrechterhaltung von Geschäftsprozessen abzielendes *Business-Continuity-Management* eingerichtet werden, statt nur auf ein ereignisabhängiges *Disaster Recovery* zu vertrauen.

Risikomanagement ist längst nicht mehr ein Merkmal besonders guter Unternehmensführung, sondern ist vielmehr eine Forderung, die von verschiedenen Gesetzen (KonTraG, Basel II, und anderen, vor allem Handels- und Steuergesetzen) mit Blick auf die Ordnungsmäßigkeit der Unternehmensführung und die Haftung der Geschäftsführung aufgestellt wird. Die Interne Revision ist in der Pflicht, die Umsetzung von Ordnungsmäßigkeitskriterien sicherzustellen.

1 Unter Mitarbeit von Dipl.-Ing., Dipl.-Wirt.-Inf. Dr. Thomas Collenberg