1 IT-Sicherheit von Informationssystemen

Sicherheitsanforderungen sollen sich an den Geschäftsprozessen des Unternehmens orientieren. Bei der IT-Sicherheit von Informationssystemen geht es darum, Auswirkungen möglicher Ausfälle der Systeme in Form von Unterbrechungen in der Versorgung mit (auf den entsprechenden Informationssystemen basierenden bzw. durch diese zur Verfügung gestellten) Leistungen bzw. Services zu vermeiden. Dabei ist in der Praxis eine Ausrichtung an den gängigen Normen des IT-Managements und der IT-Sicherheit außerordentlich sinnvoll, da hierdurch eine große Menge eigener Arbeit im Hinblick auf die Erarbeitung der zu beachtenden Einflussparameter und die einzusetzenden Maßnahmen erspart werden können. Konkret handelt es sich hierbei um die Normen ISO/IEC 20000 sowie ISO/IEC 27001 -02.[2]

Außer diesen internationalen Normen gibt es allerdings noch nationale Standards wie die des Instituts der Wirtschaftsprüfer, hier stellvertretend für verschiedene IDW PS 340.

Insbesondere die Interne Revision sollte diese Prüfstandards zur Grundlage ihrer Arbeit machen, da davon ausgegangen werden kann, dass auch ein externer Prüfer seine Arbeit hieran ausrichten wird.

Die Prozessschritte eines Risikomanagements lassen sich wie folgt darstellen:

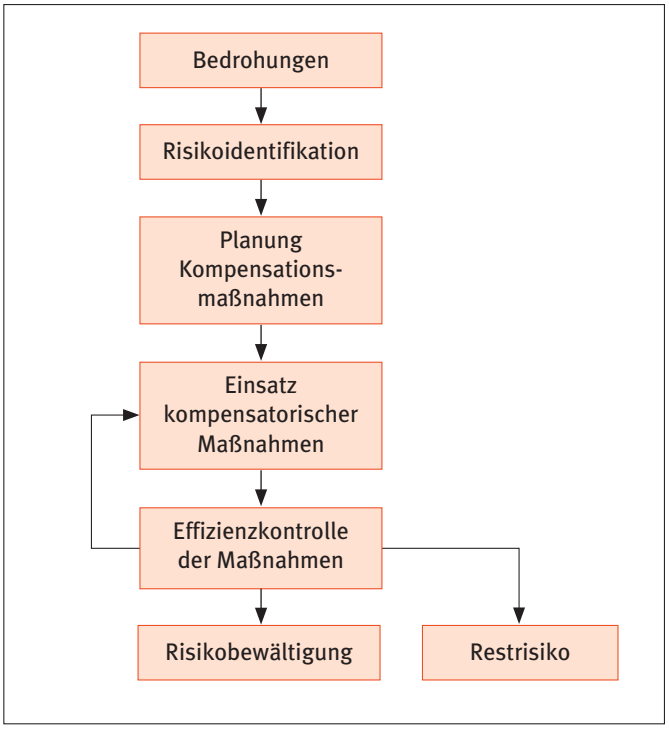

Abb. Risikomanagement: Prozessschritte

Top-Priorität hat die Verbesserung der Geschäftsprozesse. Je geringer die Ausfallhäufigkeit und je kürzer eine Unterbrechung, desto wirtschaftlicher laufen die Prozesse. So hat die IT die Geschäftsprozesse möglichst sicher und unterbrechungsfrei zu unterstützen. Dies wird besonders deutlich bei computergestützten Produktionsprozessen, bei deren Ausfall der Steuerungscomputer die Stilllegung der gesamten Produktion bedeuten würde. Kern der Problematik der IT-Sicherheit von Informationssystemen bzw. übergeordnetes Ziel ist die Gewährleistung der Versorgungssicherheit. Hierzu müssen entsprechende Maßnahmen ergriffen werden. So zielt z. B. § 109 Telekommunikationsgesetz (Technische Schutzmaßnahmen) auf die Verfügbarkeit von Telekommunikationsanlagen ab, die dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten dienen. Die Anforderungen betreffen Personal, Organisation sowie die eingesetzte Technik. Sie sind so gestaltet, dass durch die zu ihrer Erfüllung ergriffenen Schutzmaßnahmen eine dem Stand der Technik und internationalen Maßstäben entsprechende „angemessene Standardsicherheit" für die in der Vorschrift genannten Schutzziele erreicht wird. Hierauf müssen alle präventiven Tätigkeiten und sog. virtuellen Schutzmaßnahmen abzielen. Damit verbundene Überlegungen sind im Bereich der Risikovorsorge (Vermeidung von Versorgungsausfällen) anzusiedeln.

Telekommunikationsgesetz

§ 109 Technische Schutzmaßnahmen

(1) Jeder Diensteanbieter hat angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze
1. des Fernmeldegeheimnisses und personenbezogener Daten und
2. der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe
zu treffen.

(2) [1]Wer Telekommunikationsanlagen betreibt, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, hat darüber hinaus bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und gegen äußere Angriffe und Einwirkungen von

2 Vgl. *Voßbein*, Revisionstools im Bereich der IT-Sicherheit effizient einsetzen, Revisionspraxis – PRev 2/2007 S. 31 ff. sowie *Voßbein*, Prüfstandards für Datenschutzaudits – Unterstützung der Revisionsarbeit, Revisionspraxis – PRev 2/2007 S. 38 ff.