MUSTERLÖSUNG, H.P. KÖNIGS, SPRINGER VIEWEG „IT-RISIKOMANAGEMENT MIT SYSTEM“, 5. AUFLAGE

KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 6

Lösung zu Frage 1

Falls keine Schwachstelle vorhanden ist, kann, gemäss dem Modell (s. Abschnitt 2.4), eine Bedrohung an einem Schutzobjekt keinen Schaden hervorrufen. Das Risiko ist demzufolge gleich Null.

Lösung zu Frage 2

Ziel der **„Informationssicherheit“** ist es, sowohl die Informationen selbst als auch die Daten, Systeme, Kommunikationen, Prozeduren und Einrichtungen zu schützen, welche die Informationen enthalten, verarbeiten, speichern oder liefern. Der Schutz gilt dabei den Sicherheitszielen (System-Zielen) Vertraulichkeit, Integrität und Verfügbarkeit der Informationen Somit beschränkt sich nicht auf die Sicherheit der Informations-Technologien, welche lediglich die „Gefässe“ für die Informationen darstellen, sondern bezieht sich auf die Informationen, die auch in nichttechnologischer Form vorkommen können (z. B. Notizen auf Papier).

Die **„IT-Sicherheit“** hingegen schützt und sichert die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen soweit sie mit Informations-Technologien behandelt oder in Zusammenhang stehen.

Die **„Informationssicherheits-Risiken“** bringen die Abweichungen von den System-Zielen „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ an den Informations-Objekten und deren Folgen zum Ausdruck.

Hingegen betreffen die **„IT-Risiken“** nicht alleine die Risiken über Abweichungen bei der „Vertraulichkeit“, „Integrität“ und Verfügbarkeit“ von Informationen in der IT, sondern auch weitere Risiken, z. B. hinsichtlich Compliance oder Effektivität der IT-Prozesse. Die IT-Risiken beschränken sich damit nicht auf die Informationssicherheit der IT, sondern beziehen sich auch auf Unternehmens-Risiken hinsichtlich beispielsweise der IT-Ressourcen-Beschaffung und der IT-Nutzung.

Lösung zu Frage 3

- Informationssicherheitsrisiken können bei ihrem Eintreten ein hohes Ausmass erreichen, das allenfalls zu Bankrott eines Unternehmens führen kann. Durch ein Informationssicherheits-Risikomanagement ist es möglich, die Wahrscheinlichkeit grosser Schäden sowie die Häufigkeit ihres Eintretens durch den risikogerechten Einsatz von Massnahmen zu minimieren.

- Durch das Risikomanagement lassen sich unangemessene Massnahmenkosten vermeiden.
- Mit einem Informationssicherheits-Risikomanagement kann den Compliance-Anforderungen der Gesetzgeber, Regulierern, Vertragspartnern und weiteren Anspruchsgruppen Rechnung getragen werden.
- Ein gut durchgeführtes Risikomanagement dient der Unternehmenskultur und fördert vor allem das Bewusstsein und das Verhalten (Awareness) gegenüber möglicher Sicherheitsereignissen.
- Ein gut geführtes Risikomanagement im Rahmen eines Informationssicherheits-Management-Systems kann einen positiven Einfluss auf die die Firmen-Reputation und damit auf die Firmenergebnisse haben.

Lösung zu Frage 4

Im Rahmen von Informationssicherheit werden die primären System-Ziele resp. Informationskriterien

- Vertraulichkeit,
- Integrität und
- Verfügbarkeit behandelt.