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

KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 8

Lösung zu Frage 1

Die allgemeine Risiko- und Sicherheitspolitik gibt die für das Unternehmen gültigen Sicherheits- und Risiko-Ziele sowie die dazu wichtigsten Grundsätze wieder. Die Ziele und Grundsätze beziehen sich auf die Unternehmens-Mission und Unternehmens-Ziele und bringen wichtige Werte und Haltungen (ggf. auch ethische Grundsätze) zu Risiken und zur Sicherheit des Unternehmens zum Ausdruck. Eine solche Politik ist anderen Risiko- und Sicherheits-Policies übergeordnet und langfristig angelegt und stellt damit ein Führungs-Instrument des „Normativen Managements“ dar. Folgerichtig wird auch der Verwaltungsrat (resp. der Vorstand) in massgeblicher Weise den Inhalt bestimmen und die Politik genehmigen.

Lösung zu Frage 2

Die Informationssicherheit und des Informationssicherheits-Risikomanagements hängen zu einem grossen Teil vom Verhalten der Mitarbeiter und den Benutzern der IT-Systeme ab. Auch bedürfen die Beschaffung, der Aufbau, der Betrieb, und nicht zu vergessen, die Entsorgung der IT-Systeme, klarer, auf die Organisation (Unternehmen) abgestimmter Sicherheits-Vorschriften. Die an Personen (z.B. Nutzer von Informationssystemen oder Funktionsträger) oder Organisationseinheiten gerichteten Vorschriften definieren Massnahmen und Verhaltensweisen genereller Natur und bewirken somit einen „Grundschutz“ im Unternehmen.

Die Informationssicherheits-Weisungen kommunizieren dabei meist die Vorschrift oder Vorgabe, was einzuhalten oder umzusetzen ist. Hingegen die Ausführungsbestimmungen oder Anleitungen kommunizieren meist die Mittel oder die detaillierten Aktivitäten wie einzelne Vorschriften einzuhalten oder umzusetzen sind.

Lösung zu Frage 3

Die Informationssicherheits-Architektur in einem Unternehmen ist ein Baukasten-System mit abgestimmten, standardisierten Bausteinen unterschiedlicher Sicherheitsdienste mit abgestuften Stärken und den Anforderungen entsprechenden Schnittstellen. Die IT-Sicherheits-Architektur resultiert aus der für das Unternehmen typischen System-Situation.

Sie beinhaltet u.a. die auf die allgemeinen Systemanforderungen abgestimmten Sicherheits-Dienste und –Mechanismen und ist somit der Bauplan für die standardisierte IT-Sicherheits-Infrastruktur im Unternehmen. Die Informationssicherheits-Architektur in einem Unternehmen wird sukzessive mit einzelnen Sicherheitskomponenten und –systemen überall dort aufgebaut, wo sich aufgrund mehrerer gleichartiger Sicherheitsanforderungen eine innerbetriebliche Standardisierung aufdrängt. Durch die Standardisierung der Sicherheitskomponenten und -systeme ergibt sich zum einen ein Rationalisierungseffekt und zum anderen aufgrund der Übersichtlichkeit die Vermeidung unbekannter Schwachstellen und damit eine höhere Sicherheit.

Lösung zu Frage 4

Das Sicherheitskonzept definiert die Massnahmen zur Bewältigung der für den betreffenden Anwendungsfall (Situationen, Risikoobjekte, Systeme etc.) massgeblichen Risiken. Die Weisungen hingegen definieren Massnahmen und Verhaltensweisen genereller Natur und bewirken somit einen „Grundschutz“ im Unternehmen, mit dem die generellen und allenfalls typischen Risiken bewältigt werden können.

In bestimmten Anwendungsfällen können einzelne Forderungen von Policies, Weisungen und Ausführungsbestimmungen jedoch kontraproduktiv sein (z.B. aufgrund spezieller Kundenanforderungen oder bestimmter Systemvorgaben), wodurch spezifische Lösungen, die nicht den allgemeinen Regelungen der Policies, Weisungen und Ausführungsbestimmungen entsprechen, notwendig werden. Aufgrund der vorhandenen spezifischen Risiken sind oft auch andere Massnahmen angezeigt, die unter geringerem Aufwand den Zweck besser erfüllen können. Somit ist es im Ausnahmefall oft sinnvoll, die durch Weisungen vorgeschriebenen Massnahmen mittels alternativen aus einem Sicherheitskonzept resultierenden Massnahmen zu übersteuern.

Die in solchen Fällen praktizierbare Übersteuerung von Polcies, Weisungen und Ausführungsbestimmungen in einzelnen Punkten durch ein spezifisches Sicherheitskonzept setzt jedoch voraus, dass das Sicherheitskonzept mit seinen besonderen Massnahmen risikobasiert ausgearbeitet ist und einer sicherheitstechnischen Prüfungs- und Genehmigungsprozedur unterliegt.

Lösung zu Frage 5

Die Grundschutzmassnahmen dienen vor allem der Behebung von „Schwachstellen“, die für die gegenwärtige Bedrohungslage allgemein bekannt sind, somit können sie zu einer Verbesserung der Sicherheitslage im Unternehmen beitragen. Bis zu einem bestimmten Grad können die Grundschutzmassnahmen auch auf die Gegebenheiten im Unternehmen angepasst werden, wobei weniger die aktuell vorhandenen Risiken als die Gegebenheiten der IT-Systeme und der IT-Infrastruktur den Einsatz bestimmter Massnahmen bestimmen.

Da der Grundschutz kein detailliertes auf das Risikoobjekt bezogenes Risiko-Assessment erforderlich macht, wird der Grundschutz in vielen Unternehmen für die Absicherung gegen häufig vorkommende Bedrohungen und Schwachstellen mit nicht allzu hohen zu erwartenden Impacts eingesetzt. Zur Bestimmung der Massnahmen gegen die Risiken mit hohem Impact wird hingegen ein detailliertes umfassendes Risiko-Assessment durchgeführt, wofür auch Massnahmen aus den Grundschutzkatalogen entnommen werden können.

- Beliebt sind die Grundschutzkataloge in vielen Unternehmen, da sie detaillierte Hinweise für die Gestaltung und Umsetzung der Massnahmen geben, was bei den sehr generisch gehaltenen ISO-Standards (z.B. ISO/IEC 27002) nicht gegeben ist.
- Wichtig für Grundschutzmassnahmen ist auch, dass sie bei mehreren gleichartigen Risikoobjekten (z.B. Server einer Server-Farm) in gleichartiger Weise eingesetzt werden (z.B. Härtung von Server-Plattformen), wodurch eine rationelle Massnahmenumsetzung möglich ist.

Weitere Argumente, Grundschutzmassnahmen im Unternehmen einzusetzen sind:

- Übersichtlichkeit
- Vergleichbarkeit mit anderen Unternehmen
- Überprüfbarkeit
- Gütesiegel bei Dienstleistungsangeboten (z.B. bei Offerings)
- Argumentationshilfe in der Kostendebatte

Als Fazit kann festgehalten werden, dass sich für den Einsatz in einem Unternehmen der Grundschutz und eine risikobasierte Vorgehensweise (z.B. mit ISO/IEC 27001) vorteilhaft ergänzen können.

Lösung zu Frage 6

Um die Notwendigkeit einer umfassenden Risikoanalyse festzustellen, werden die Risiken, identifiziert und mittels einer einfachen Impact-Analyse (Auswirkungs-Analyse) deren „Impacts“ (mögliche Schadenshöhen) ermittelt.

Übersteigen die Impacts einen tolerierbaren Wert, dann ist eine umfassende Risikoanalyse unter Einschluss der Bedrohungen und Schwachstellen notwendig.