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

KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 10

Lösung zu Frage 1

Neben den Risiken sind in einem IT-Sicherheitskonzept beispielsweise folgende Anforderungen zu berücksichtigen:

- Leistungsvorgaben (z.B. definiert mittels SLA)
- Qualitätsanforderungen
- Architektur-Vorgaben
- Innerbetriebliche Standards
- Gesetzliche und regulative Vorgaben (Informationenschutz, Bankgeheimnis, Urheberrecht, Basel II usw.)

Lösung zu Frage 2

Die Erstellung eines IT-Sicherheitskonzepts ist dann nützlich, wenn es bei Prozessen oder IT-Systemen darum geht, mit geeigneten Massnahmen die Risiken auf tragbare Restrisiken zu reduzieren und wenn die Art und Weise der Bewältigung der Risiken aufgezeigt und dokumentiert werden muss.

Das Sicherheitskonzept kann sich auf die Sicherheitsaspekte des ganzen Lebenszyklus eines Systems (z.B. Beschaffung, Entwicklung, Einführung, Betrieb und Entsorgung) oder auch nur auf einzelne Phasen (z.B. Entwicklung oder Betrieb) beziehen. Solche phasenspezifischen Sicherheitskonzepte sind dann sinnvoll, wenn einzelne Lebenszyklusphasen (z.B. Entwicklung, Migration und Einführung) in sich stark risikobehaftet sind.

Lösung zu Frage 3

Die sechs Kapitel eines IT-Sicherheitskonzepts sind:

Kapitel 1: Ausgangslage

Kapitel 2: Systembeschreibung und Schutzobjekte

Kapitel 3: Risikoanalyse

Kapitel 4: Anforderungen an Sicherheitsmassnahmen

Kapitel 5: Sicherheitsmassnahmenbeschreibung

Kapitel 6: Umsetzung der Sicherheitsmassnahmen

Lösung zu Frage 4

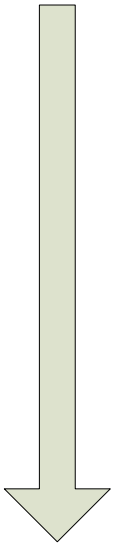
Ausserhalb des Prozesses der Erstellung eines Sicherheitskonzepts bedarf es eines weiteren wichtigen Prozesses, nämlich des Prozesses der Vorlage, der Abnahme und Akzeptanz sowie der Umsetzungskontrolle; dieser Prozess sollte vorzugsweise durch eine entsprechende „Policy" gesteuert und durch von der Erstellung unabhängigen Funktionsträger durchgeführt werden. Mit einem solchen zusätzlichen Prozess erfüllt ein Sicherheitskonzept die an einen Risikomanagement-Prozess gestellte wichtige Anforderung der „stetigen Kontrolle und Anpassung an die Risikolage".

Lösung zu Frage 5

In Situationen, in denen die Schutzobjekte nicht in einer bewertbaren Form vorliegen, muss auf die Impact-Analyse (Schadensausmass-Analyse) verzichtet werden. In solchen Fällen ist es oft sinnvoll, anstelle einer Risikoanalyse eine bewertende Schwachstellenanalyse durchzuführen.

Lösung zu Frage 6

Die Schutzobjekte bei CRAMM werden im sog. Asset-Model gemäss folgender Hierarchie verknüpft:

Hierarchie der Schutzobjekte-Kategorien	
Informationen-/Informationsobjekt und für die Informations-Lieferung zuständiger „Endbenützer-Service".	
Software-Objekte	
Physische Objekte, welche die Informationsobjekte jeweils unterstützen (z.B. Hardware, Netzwerkkomponenten und Betriebssysteme. Anm.: Die Betriebssysteme und ihre Komponenten werden zu den physischen Objekten gezählt)	
Räume	

Lösung zu Frage 7

Die Fehlermöglichkeits- und Einflussanalyse (FMEA) ist eine Bottom-up-Methode; sie zeigt, wo Einzelkomponenten zu Ausfällen und Auswirkungen auf den höheren Ebenen eines ganzen Systems oder Teilsystems führen können. Damit kann sie als „Schwachstellenanalyse“ insbesondere zum Aufzeigen von „Single point of failures“ dienen. Nach dem „What-if“-Prinzip (Was ist, wenn…?) können auch Massnahmen verifiziert werden, die den Störungs-Einfluss einer kritischen Komponente auf das Gesamtsystem mildern.

Lösung zu Frage 8

Rpz = A ∗ B ∗ E

Rpz: Risikoprioritätenzahl

A: Auftretenswahrscheinlichkeit

(1= sehr gering; 10= sehr hoch)

B: Bedeutung

(1=geringfügige Auswirkungen; 10=äusserst schwerwiegend Folgen)

E: Entdeckungswahrscheinlichkeit

(1= sehr hoch; 10 = sehr gering)

Die Zuordnung der Risikoprioritätenzahl zu einzelnen Komponenten oder Konfigurationen ermöglicht die quantitative Bewertung der Gesamtzuverlässigkeit einer gewählten Systemvariante.

Für jedes System resp. Merkmal werden im Wesentlichen die potenziellen Fehler, die potenziellen Folgen der Fehler, die potenziellen Fehlerursachen sowie die empfohlenen Massnahmen mit Verantwortlichkeitszuordnung registriert. Der derzeitige und der mit Massnahmen verbesserte Zustand werden anhand der oben angegeben Risiko-Parametern bewertet

Lösung zu Frage 9

Die Fehlerbaum-Analyse ist eine Top-Down-Methode. Bei dieser Methode werden von einem bestimmten Fehlerereignis dem sog. Top-Ereignis (Top Event) „deduktiv“ die ursächlichen Ereignisse gesucht, die für das Top-Ereignis verantwortlich sind. Die möglichen Ereignisse werden dabei logisch zu einer Baumstruktur verknüpft. Der Baum zeigt auf, welche untergeordneten Ereignisse in welcher logischen Verknüpfung ein jeweils übergeordnetes Fehler-Ereignis verursachen.

Als quantitative Aussage liefert die Fehlerbaumanalyse insbesondere die Eintrittswahrscheinlichkeit des Top-Ereignisses. Diese Wahrscheinlichkeit ergibt sich rechnerisch aus den logischen Verknüpfungen des Baumes und den Wahrscheinlichkeiten der ursächlichen (Basis)-Ereignisse.

Lösung zu Frage 10

Die Ereignisbaumanalyse ist eine Bottom-up-Methode; sie liefert die Folgen (Schäden) und deren Wahrscheinlichkeiten aufgrund eines auslösenden Ereignisses. Das auslösende Ereignis kann beispielsweise der Ausfall einer Systemkomponente im System sein.