
Musterlösungen Vieweg-Buch „IT-Risiko-Management mit System“

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

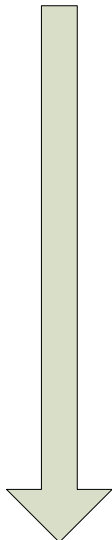
Kapitel 6: Umsetzung der Sicherheitsmassnahmen

Lösung zu Frage 4

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

Lösung zu Frage 5

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 „Endbenutzer-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 6

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 7

$$Rpz = A * B * E$$

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 angegebenen Risiko-Parametern bewertet

Lösung zu Frage 8

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 9

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.

Lösung zu Frage 10

a)

Die bereits bekannten Informationen des Falles werden vor allem in die Kapitel 1, 2 und 4 eines Sicherheitskonzepts aufgenommen.

Die Ausgangslage in Kapitel 1 soll den „allgemeinen Kontext“ des Sicherheitskonzepts und vor allem Zweck und die Ziele des neuen Teilsystems enthalten. Zum allgemeinen Kontext gehört auch das geschäftliche und organisatorische Umfeld für das neue Teilsystem (z.B. Geschäftsfunktionen, Verantwortlichkeiten, Termine, Eigentums- und Vertragsverhältnisse). Ebenfalls enthält es die Abgrenzungen für die Behandlung des Teilsystems sowie die besonderen Anforderungen und Einschränkungen.

In Kapitel 2 wird das neue Teilsystem, wie es sich in das bestehende Gesamtsystem einfügt mit seinen Funktionen beschrieben und dargestellt. Somit enthält Kapitel 2 den für die Risiken spezifischen Kontext für die neuen IT-Risiken. Unter anderem zeigt das Kapitel 2 die Schutzobjekte, für welche die Risiken und allfälligen Massnahmen ermittelt werden.

Schliesslich zeigt Kapitel 4 die an die Sicherheitsmassnahmen gerichteten Anforderungen, die sich nicht nur aus den Risiken, sondern auch aus den sonstigen Bedingungen für das IT-System ergeben, z.B. Datenschutz, Allgemeine Geschäftsbedingungen,

SSL zur Übertragungschiffrierung, SecurID-Karte zur Authentisierung des Benutzers, Online-Abfragemöglichkeit über 7 x 24 Std. für „Umsatz“ und „Kassenbestand“.

b)

Die wesentlichen IT-Gefahren für das neue Teilsystem sind:

- Missbrauch von persönlichen Daten des Käufers (Verletzung Datenschutz)
- Ausspionieren der unter das Geschäftsgeheimnis des Händlers fallenden Informationen (z.B. durch Masquerade eines Händlers oder durch Eindringen auf den PC des Händlers)
- Versagen von technischen Komponenten
- Benutzerfehler (menschliches Versagen)

c)

Aus der Fallbeschreibung kann geschlossen werden, dass insbesondere für das Systemziel „Vertraulichkeit“ allenfalls hohe Risiken anfallen können.

d)

Als kostengünstigere Händlerauthentifizierungen können Authentisierverfahren mit Passwort (ggf. auch PIN) oder Passwort mit zusätzlicher „Random-Code-Tabelle untersucht werden.

e)

Risiken für den Händler: Bei schwacher Authentisierung besteht eine höhere Wahrscheinlichkeit als bei starker Authentisierung, dass die unter „Geschäftsgeheimnis“ stehenden Informationen an die Konkurrenz abfließen. (Anm.: Mit zusätzlichen Massnahmen kann das Risiko einer schwachen Authentisierung jedoch verringert werden). => Risiko 1

Bei schwacher im Gegensatz zu starker Authentisierung wird auch die Wahrscheinlichkeit höher, dass Informationen von Kunden an Dritte abfließen. Je öfter dies vorkommt, desto höher wird der Reputationsschaden. => Risiko 2

Risiken für Interpay: Fließen Informationen an Dritte ab, dann wird der Reputationsschaden für Interpay umso grösser je öfters dies vorkommt. => Risiko 3

Anhand der Fallbeschreibung können wir diese Risiken gemäss Tabelle 1 für starke und schwache Authentisierung ordinal bewerten:

R.-Nr.	Risiko-Bezeichnung	Schwache Authentisierung		Starke Authentisierung	
		Schaden	Häufigkeit	Schaden	Häufigkeit
1	Risiko für Händler „Abfluss von Geschäfts-Informationen an Konkurrenz“	mittel	selten	mittel	sehr selten
2	Reputationsrisiko für Händler „Abfluss von Kunden-Informationen an Dritte“	mittel	selten	mittel	sehr selten
3	Reputationsrisiko für Interpay „Abfluss von Kunden- oder Geschäfts-Information an Dritte“	gross	oft	mittel	selten

Tabelle 1: Risiken bei starker und schwacher Authentisierung

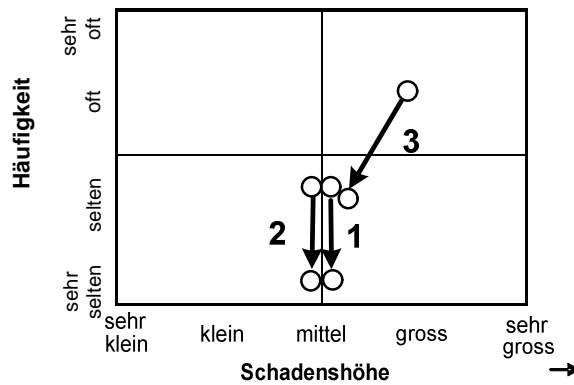


Abbildung 1: Darstellung der Risiken im „Risk Map“ bei starker und schwacher Authentisierung

f)

Aufgrund der hohen Massnahmenkosten (hohe Kosten der SecureID-Karte) und der Risiken (z.B. Datenschutzverletzung) müssen die Anforderungen der Interpay modifiziert werden. Folgende Massnahmen tragen den Anforderungen Rechnung:

M 1: Anonymisierung der für Werbeaktionen notwendigen Kundendaten.

M 2: Passwort mit erzwungener strenger Passwortpolicy (z.B. komplexes Passwort).

M 3: Anleitung des Händlers, wie er seinen PC, z.B. mittels „Personal Firewall“ und „Virenschutz“, vor Angriffen aus dem Internet schützen kann.

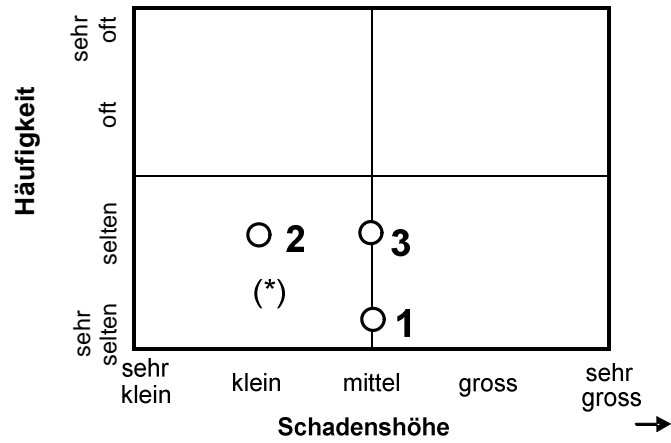
M 4: Explizite Verantwortlichkeitzuweisung im Vertrag und/oder den Allgemeinen Geschäftsbedingungen an den Händler zur Befolgung der vorgeschriebenen Massnahmen.

R.-Nr. (*)	Schutzobjekte	Bedrohungen	Massnahmen	Restrisiken	
				Schaden	Häufigkeit
1	Informationen unter Geschäftsgeheimnis des Händlers	Ausspionieren der Informationen (z.B. durch Maske oder durch Eindringen auf den PC des Händlers)	M2, M3 und M4	mittel	sehr selten
2	Kunden-Informationen	Missbrauch von persönlichen Daten eines Kunden	M1, M2, M3 und M4	klein	sehr selten
3	Dienstleistung der Interpay	„Abfluss von Kunden- oder Geschäftsinformationen an Dritte“	M1, M2, M3 und M4	mittel	selten

(*) Risiko-Nummerierung s. Tabelle 1

Tabelle 2: Restrisiken bei modifizierten Anforderungen und Massnahmen

g)



(*) Risiko-Nummerierung s. Tabelle 1

Abbildung 2: Restrisiken im Risk Map bei modifizierten Anforderungen und Massnahmen

h)

Durch die Anonymisierung werden Risiken „vermieden“