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

KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 14

Lösung zu Frage 1

Die Schutz-Phasen im Lebenszyklus (Lifecycle) von Informationen, in den die Informationen generell unterschiedlichen Bedrohungen unterliegen, sind:

- Entstehung,
- Bearbeitung,
- Übertragung (Übermittlung),
- Speicherung (Archivierung) und
- Entsorgung (Löschung).

Lösung zu Frage 2

Die Kriterien, nach denen Informationen meist eingestuft werden, sind:

- Mass des Schadens (Impact) der Informationen wenn ihre Vertraulichkeit verletzt wird;
- Mass des Schadens (Impact), wenn die Integrität (Richtigkeit) der Informationen verletzt wird.
- Mass des Schadens (Impact), wenn die Informationen zur erforderlichen Zeit in der erforderlichen Weise nicht verfügbar sind.

Lösung zu Frage 3

Vertrauliche Informationen werden bei der elektronischen Übertragung (Übermittlung) durch Chiffrierung (Kryptographie) gegen unberechtigte Kenntnisnahme geschützt.

Lösung zu Frage 4

Die Lieferobjekte, die im Projektablauf abgenommen sein müssen, bevor jeweils die nächste Projektphase begonnen werden darf, sind von der Projektmanagement-Methode abhängig. Die Projektmanagement-Methode gemäss dem folgenden „Wasserfall“-Lifecycle, lässt sich leicht auf andere Methoden übertragen, z.B. auf das V-Modell oder den Applications-Managements-Lifecycle gemäss ASL®. In einem pragmatischen Modellansatz sind im „Wasserfall“-Lifecycle nachfolgend die Lieferobjekte bezüglich Informationssicherheit eingetragen:

1) Anforderungs-Analyse

Abnahme „First Cut“

Das mit „First Cut“ bezeichnete Risiko-Assessment liefert Anhaltspunkte darüber, ob höhere Risiken vorhanden sind oder ob die Risiken weitgehend durch bestehende Grundschutzmassnahmen oder anderweitig vorhandene Massnahmen abgedeckt sind. Werden für die zukünftige Betriebsphase grössere Risiken sichtbar, dann wird bereits zu diesem Zeitpunkt ein detailliertes Risiko-Assessment mit einer möglichst gründlichen „Risiko-Identifikation“ und dem „Aufzeigen der Impacts“ vorgenommen.

2) Anforderungsdefinition und Entwurf

Abnahme Sicherheitskonzept „Grobfassung“ Sicherheitskonzept,

Das in allen sechs Kapiteln grob ausgearbeitetes Sicherheitskonzept muss vor allem die voraussichtlichen IT-Sicherheits-Risiken aufzeigen. Ebenso sind in diesem grob ausgearbeiteten Sicherheitskonzept die für ein akzeptables Restrisiko notwendigen Massnahmen mit dem Realisierungsvorgehen vorzuschlagen.

3) Entwicklung oder Beschaffung

4) Integration und Test

Abnahme Sicherheitskonzept „Betriebsfassung“

Dieses detaillierte Sicherheitskonzept dokumentiert die Risiken, Massnahmen, Restrisiken und Umsetzungs-Aktivitäten für den späteren einwandfreien Systembetrieb.

5) Einführung und Ausbreitung

6) Systembetrieb

7) Systemoptimierung

8) Systemabbau – Archivierung und Entsorgung

Bei der Methode „Hermes“ sind drei wichtige für die Informationssicherheit und den Datenschutz notwendige Lieferobjekte genehmigen zu lassen:

- Schutzbedarfsanalyse in der „Initialisierungsphase“;
- Falls die Schutzbedarfsanalyse einen höheren Schutzbedarf anzeigt, ist ein „Konzept für Informationssicherheit und Datenschutz“ (ISDS-Konzept) erforderlich, welches auch ein Notfallkonzept enthält. Das ISDS ist in der „Konzeptphase“ zu erstellen;
- Das ISDS-Konzept ist in den weiteren Phasen „Realisierung“ und „Einführung“ entsprechend umzusetzen und der Stand der Umsetzung im ISDN-Konzept nachzuführen.
- Die Risikobeurteilung („Projektrisiken“ und „Geschäfts- und Betriebsrisiken“) wird im Phasenbericht jeder Projekt-Phase festgehalten und dient der Entscheidung für die Freigabe der nächsten Phase.

Lösung zu Frage 5

Der Application Security Lifecycle gemäss ISO/IEC 27034 für Softwareentwicklung enthält die folgenden Phasen:

- Am Anfang des Lifecycles die „Vorbereitungsphase“ und sodann die Phase, in der das Softwareprodukt erstellt oder beschafft wird, mit der Unterscheidung „Entwicklung“, „Outsourcing“ oder „Beschaffung“. Diese Phasen werden auch als Bereitstellungsphasen bezeichnet.
- Die nachfolgende Benutzungsphase ist unterteilt in „Benutzung“, „Archivierung“ und „Vernichtung“.

Die im Standard definierten Sicherheitsmassnahmen (ASC= Application Security Controls) sind auf diesen Lifecycle ausgerichtet und in diesen eingefügt.

Lösung zu Frage 6

Die Methode „V-Modell XT für einen Entwicklungsprozess“ für ein Autragnehmer-Projekt weist folgende der Sicherheit und dem Datenschutz dienliche Produkte auf:

- Sicherheitsanalyse in der Phase „Systemspezifikation“
- Datenschutzkonzept, Sicherheitsanalyse und Informationssicherheitskonzept in der Phase "Systementwurf"
- Sicherheitsanalyse, Informationssicherheitskonzept in der Phase „Abschluss Feinentwurf“

Die Produkte werden durch den Auftragnehmer abgenommen, unter Mithilfe von durch ihn beauftragte Stellen, z.B. Beauftragten für IT-Sicherheit und bei personenbezogenen Daten, zusätzlich durch einen Datenschutzbeauftragten.

Lösung zu Frage 7

Im HERMES-Modell beginnt die agile Entwicklung in der Phase „Konzept“.