Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 5. Übung im SoSe 2010:

Konzepte zur IT-Sicherheit

5.1 Sicherheitskonzept

Aufgabe:

- Welche Aspekte sollten in einem **Sicherheitskonzept**, das den laufenden Betrieb der IT-Infrastruktur gewährleisten soll, auf jeden Fall geregelt werden, um die gängigsten Schwachstellen abzudecken? Begründen Sie Ihre Antwort.

5.1 Sicherheitskonzept

Abwehr gängigster Schwachstellen durch folgende Controls:

- Sensibilisierung und Schulung der Mitarbeiter
- Authentisierung bei Zugang und Zugriff anhand Wissen/Besitz/Merkmal
- Schutz vor Viren, Würmer, Trojanische Pferde etc.
- Protokollierung (→ Überwachung der Technik & Datenströme; z.B. Netzwerkmonitoring, Intrusion Detection System)
- Änderung von Produktivsystemen erst nach Erfolg bei Testsystemen
- Dokumentation von Änderungen an Systemeinstellungen
- regelmäßige Kontrollen (z.B. durch Penetrationstests)
- Einrichtung eines Vulnerability Managements

→ **Hilfsmittel**: Sicherheitsleitlinie (security policy)

5.2 Empfohlene Gegen-maßnahmen für Safety

Aufgabe:

- Nennen Sie fünf potentielle Gefährdungen der **Safety** eines IT-Systems! Was würden Sie als IT-Leiter tun, um die von Ihnen aufgelisteten Gefährdungen zu vermeiden?

5.2 Empfohlene Gegen-maßnahmen für Safety

- Brand
  → Notfallvorsorgekonzept (z.B. Datenspiegelung, redundante Technik, Ausfallrechenzentrum in räumlich ausreichender Entfernung)
- Stromausfall
  → Unterbrechungsfreie Stromversorgung
- Hardware-Defekt
  → regelmäßige Erneuerung korrosionsgefährdeter Hardware-Komponenten
- Software-Defekt
  → Einrichtung eines Testsystems getrennt vom Produktivsystem mit identischer Konfiguration
- Bedienungsfehler
  → Bereitstellung einer ausreichenden Dokumentation und Mitarbeiterschulung

5.3 Notfall-Vorsorge-Konzept

Aufgabe:

- Welche Bestandteile sollte ein **Notfall-Vorsorge-Konzept** bei einem mittelständischen Unternehmen Ihrer Ansicht nach auf alle Fälle beinhalten? Sehen Sie sich hierzu die entsprechenden Ausführungen in den BSI-Grundschutzkatalogen auf www.bsi.de an und wählen Sie begründet aus.

5.3 Notfall-Vorsorge-Konzept (1)

Ein Notfallvorsorgekonzept beschreibt, wie das Eintreten eines Notfalls vorzugsweise verhindert werden kann/soll → **präventiver Schutz**

→ Komplettes Notfallmanagement ist auf den BSI-Seiten beschrieben im **BSI-Standard 100-4** (abrufbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/31045/standard_1004.pdf)

→ Darin **Kapitel 5.5 Notfallvorsorgekonzept** auswerten

→ **Bestandteile** (Inhalt des Notfallvorsorgekonzepts):
- ° Verantwortlichkeiten, Geltungsbereich, Inhaltsangabe
- ° Abgrenzungen, Ziele, Zuständigkeiten, Ablauforganisation
- ° betrachtete Notfallszenarien, Wiederanlauf-Anforderungen, Priorisierungen
- ° Alarmierungsverfahren, Beschreibung vorbeugender Maßnahmen
- ° Einbinden des Notfallmanagements in Unternehmenskultur
- ° Aufrechterhaltung & Kontrolle

5.3 Notfall-Vorsorge-Konzept (2)

Ein mittelständisches Unternehmen wird sich auf Kernfragen konzentrieren

→ In Grundschutzkatalogen nach Notfallmanagement suchen

→ **Baustein 1.3 zum Notfallmanagement** wählen (abrufbar unter: https://www.bsi.bund.de/cln_183/sid_AB2A5EAB735FF0FE0D1D3C525AB43C3D/ContentBSI/grundschutz/kataloge/baust/b01/b01003.html)

→ Im Baustein 1.3 lediglich Maßnahmen der Kategorie A (Einstieg in Grundschutz) auswählen (M 6.111 zur Leitlinie, M 6.112 zur Organisationsstruktur, **M 6.114 Notfallkonzept** & M 6.118 Aufrechterhaltung des Notfallmanagements)

Bestandteile eines Notfallvorsorgekonzepts nach M 6.114:

- Übersicht zu Verfügbarkeitsanforderungen (maximal tolerierbare Ausfallzeiten, Wiederanlaufparameter, Prioritäten für Wiederanlauf)
- Vorgehen zur Durchführung einer Business Impact Analyse (BIA) & einer Risikoanalyse
- Auflistung der Maßnahmen zur Risikobehandlung

5.4 Notfallplan

Aufgabe:

- Welche Bestandteile sollte dagegen ein **Notfallplan** aufweisen?

5.4 Notfallplan

Ein Notfallplan beschreibt, was bei Eintritt eines Notfalls zu tun ist!

→ **reaktiver Schutz**

→ Notwendige **Bestandteile** eines Notfallplans:

- Zielsetzung des Notfallplans und ggf. geltende Abgrenzungen (hinsichtlich des Scope)
- Festlegung der Verantwortlichkeiten (wer macht was?)
- Aufstellung des Alarmierungsplans (wer ist wann anzurufen?)
- Ablaufpläne für entsprechende Notfallszenarien (im Sinne von Checklisten)
- Dokumentationen zur eingesetzten IT-Infrastruktur und den Maßnahmen zur Notfall-Vorsorge
- Bereitstellung aller wesentlichen Unterlagen und Nachweise (z.B. zu durchgeführten Notfall-Übungen)

5.5 Verfügbarkeitsberechnung

Aufgabe:

- Die **Verfügbarkeit** eines IT-Systems kann als das Produkt der Verfügbarkeiten ihrer jeweiligen Komponenten verstanden werden, sofern diese Komponenten seriell miteinander verbunden sind. Diese werden unter Berücksichtigung etwaiger Ausfallzeiten in % gegenüber der vereinbarten Servicezeit berechnet:

$$\text{Verfügbarkeit einer IT-Komponente} = \frac{(\text{vereinbarte Servicezeit} - \text{Ausfallzeit})}{\text{vereinbarte Servicezeit}} \text{ [in \%]}$$

- Wenn hingegen Komponenten eines IT-Systems parallel betrieben werden, erhöht sich die Verfügbarkeit für diesen technisch redundanten Cluster in Abhängigkeit zur Anzahl der technisch redundant ausgelegten IT-Komponenten auf:

$$\text{Redundanz-Verfügbarkeit} = 1 - (1 - \text{Verfügbarkeit}_{\text{normal}})^{\text{Anzahl}}$$

- A) Das zu betrachtende IT-System bestehe aus einem Server, der während der Betriebszeit zu 8 Stunden pro Jahr ausfällt, einem Client, der dabei zu 16 Stunden pro Jahr ausfällt, und einer Vernetzungskomponente, die während des Betriebs zu 24 Stunden pro Jahr ausfällt. Als Servicezeit sei ein 12-Stunden-Betrieb von Montag bis Freitag vereinbart worden. Wie hoch ist die Verfügbarkeit jeder einzelnen Komponente und des gesamten IT-Systems?
- B) Wie wirkt sich es sich auf die Verfügbarkeit des gesamten IT-Systems aus, wenn die Vernetzungskomponente mit einer identisch konfigurierten weiteren geclustert wird? Die Prozentangaben sind dabei auf drei Nachkommastellen anzugeben (also 12,345%).

5.5 Verfügbarkeitsberechnung

Teil A)

$V_{server} = (12*5*52 – 8)/(12*5*52) = 3112/3120 = 99,744\%$

$V_{client} = (12*5*52 – 16)/(12*5*52) = 3104/3120 = 99,487\%$

$V_{netz} = (12*5*52 – 24)/(12*5*52) = 3096/3120 = 99,231\%$

$V_{gesamt} = V_{server}*V_{client}*V_{netz} = 99,744\%*99,487\%*99,231\% = 98,469\%$

Teil B)

$V_{netzcluster} = 1 – (1 – V_{netz})^2 = 1 – (1 – 0,99231)^2 = 99,994\%$

$V_{gesamt\_neu} = V_{server}*V_{client}*V_{netzcluster} = 99,744\%*99,487\%*99,994\%$

$= 99,226\%$