# Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 7. Übung im SoSe 2015:

Mehrseitige IT-Sicherheit &
IT-Risikomanagement

# 7.1 Notfall-Vorsorge-Konzept & Notfallplan

**Aufgabe**:

- Lesen Sie auf den Web-Seiten des BSI, abrufbar unter www.bsi.de, die Ausführungen in den BSI-Grundschutzkatalogen bzw. den BSI-Standards zum Notfallmanagement durch.
  A) Welche Bestandteile sollte ein **Notfall-Vorsorge-Konzept** bei einem Unternehmen, das lediglich mittleren Schutzbedarf und nur eine geringe Komplexität aufweist, Ihrer Ansicht nach auf alle Fälle beinhalten? Begründen Sie Ihre Antwort!
  B) Welche Bestandteile sollte dagegen ein **Notfallplan** aufweisen? Begründen Sie Ihre Antwort!

# 7.1 Notfall-Vorsorge-Konzept & Notfallplan (1)

A) 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

# 7.1 Notfall-Vorsorge-Konzept & Notfallplan (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

# 7.1 Notfall-Vorsorge-Konzept & Notfallplan (3)

B) 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)

# 7.2 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%).

# 7.2 Verfügbarkeitsberechnung

**A)**

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

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

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

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

**B)**

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

$V_{gesamt\_neu} = V_{server}*V_{client}*V_{netzcluster} = 99{,}744\%*99{,}487\%*99{,}994\%$
$= 99{,}226\%$

# 7.3 Risikoanalyse I

**Aufgabe**:

- Gegeben seien folgende Werte einer Sicherheitsanalyse eines IT-Systems hinsichtlich der Gefährdungen der Vertraulichkeit (C), Integrität (I) und Verfügbarkeit (A):

| | | | Schaden | | |
|---|---|---|---|---|---|
| **Bedrohung** | **Verwundbarkeit** | **Auftreten** | **C** | **I** | **A** |
| Datenverlust | fehlende Clusterung | 3 | 1 | 1 | 3 |
| Datenverlust | Ermüdung Backupmedien | 2 | 1 | 4 | 4 |
| unbefugter Zugriff | fehlende Schutzzonen | 3 | 5 | 1 | 5 |
| unbefugter Zugriff | schlechte Passwörter | 4 | 4 | 3 | 2 |
| unbefugter Zugriff | fehlende Systemhärtung | 3 | 4 | 4 | 4 |
| unbefugter Zugriff | fehlende Timeoutfunktion | 2 | 3 | 3 | 3 |
| unbefugter Zugriff | Missbrauch Adminrechte | 1 | 2 | 5 | 5 |
| Vireninfektion | fehlende Schutzzonen | 3 | 3 | 4 | 4 |
| Vireninfektion | schlechter Virenscanner | 2 | 3 | 3 | 3 |
| DoS-Attacke | fehlende Schutzzonen | 4 | 1 | 1 | 5 |
| DoS-Attacke | fehlende Timeoutfunktion | 2 | 1 | 1 | 4 |

Die Angaben lägen dabei zwischen 1 (sehr gering) und 5 (sehr hoch).

A) Erstellen Sie auf der Grundlage obiger Werte das zugehörige **Risikoportfolio**! Betrachten Sie hierzu lediglich die Vertraulichkeitswerte, da der verantwortlichen Stelle die Vertraulichkeit besonders wichtig sei. Beim Risikoportfolio gilt:

° Felder, die ein Risiko bis max. den Wert 4 aufweisen, gelten dabei als akzeptabel.

° Felder, die ein Risiko ab dem Wert 15 aufweisen, gelten dabei als inakzeptabel.

° Felder, die ein Risiko zwischen diesen Werten aufweisen, bedürfen einer Prüfung.

Für welche Risiken empfehlen Sie auf Grundlage des Risikoportfolios welche Gegenmaßnahmen?

# 7.3 Risikoanalyse II

**Aufgabe:**

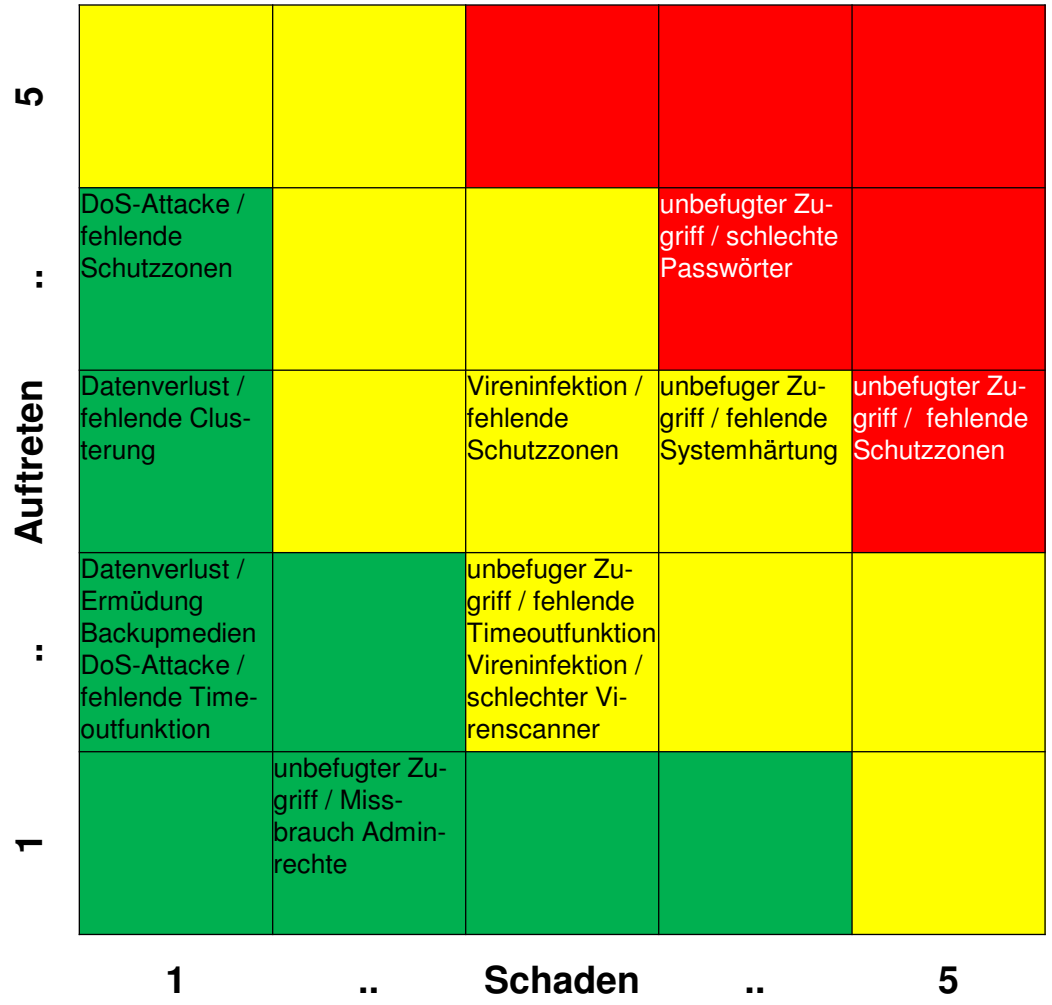
- B) Erstellen Sie auf der Grundlage obiger Werte die zugehörige **Risikomatrix** in Form einer Risikotabelle! Betrachten Sie hierzu lediglich die Verfügbarkeitswerte, da der verantwortlichen Stelle die Verfügbarkeit besonders wichtig sei.
  Für die zu verwendende Risikotabelle verwenden Sie folgendes Schema:

| Rg. | Gefährdung | Auftreten | Schaden | Risiko |
|---|---|---|---|---|

Das Risiko ergibt sich aus dem Produkt von Auftreten und Schaden. Die Liste ist entsprechend dem sich rechnerisch ergebenden Rang aufzuführen.

# 7.3 Risikoanalyse (1)

A) **Risikoportfolio** zu Vertraulichkeitsrisiken



# 7.3 Risikoanalyse (2)

Zwingend zu ergreifende Gegenmaßnahmen (inakzeptable Risiken):

- Die Passwortgüte ist zu erhöhen, indem Passwörter künftig mind. 8 Stellen unter Einhaltung der Komplexitätsregeln aufweisen müssen und jeden Monat zu wechseln sind. Diese Passwortregel ist technisch zu implementieren.
- Es ist eine sinnvolle Netzwerksegmentierung mit funktionstüchtiger Netzwerksegregation einzuführen. Hierzu ist eine zweistufige Firewall zu verwenden.

Ergänzende Gegenmaßnahmen (zu prüfende Risiken):

- Die Server sollen auf gehärteten Systemen betrieben werden, indem alle nicht notwendigen Dienste entfernt werden.
- Auf jedem Server soll ein Virenschutz implementiert sein (durch die bereits erfolgte Schutzzoneneinführung greift das bereits voll).

# 7.3 Risikoanalyse (3)

B) **Risikotabelle** zu Verfügbarkeitsrisiken:

| Rg. | Gefährdung | Auftreten | Schaden | Risiko |
|---|---|---|---|---|
| 1. | DoS-Attacke durch fehlende Schutzzonen | 4 | 5 | 20 |
| 2. | unbefugter Zugriff durch fehlende Schutzzonen | 3 | 5 | 15 |
| 3. | unbefugter Zugriff durch fehlende Systemhärtung | 3 | 4 | 12 |
| 3. | Vireninfektion durch fehlende Schutzzonen | 3 | 4 | 12 |
| 5. | Datenverlust durch fehlende Clusterung | 3 | 3 | 9 |
| 6. | Datenverlust durch Ermüdung Backupmedien | 2 | 4 | 8 |
| 6. | unbefugter Zugriff durch schlechte Passwörter | 4 | 2 | 8 |
| 6. | DoS-Attacke durch fehlende Timeoutfunktion | 2 | 4 | 8 |
| 9. | unbefugter Zugriff durch fehlende Timeoutfunktion | 2 | 3 | 6 |
| 9. | Vireninfektion durch schlechter Virenscanner | 2 | 3 | 6 |
| 11. | unbefugter Zugriff durch Missbrauch Adminrechte | 1 | 5 | 5 |

# 7.4 Fehlerbaum

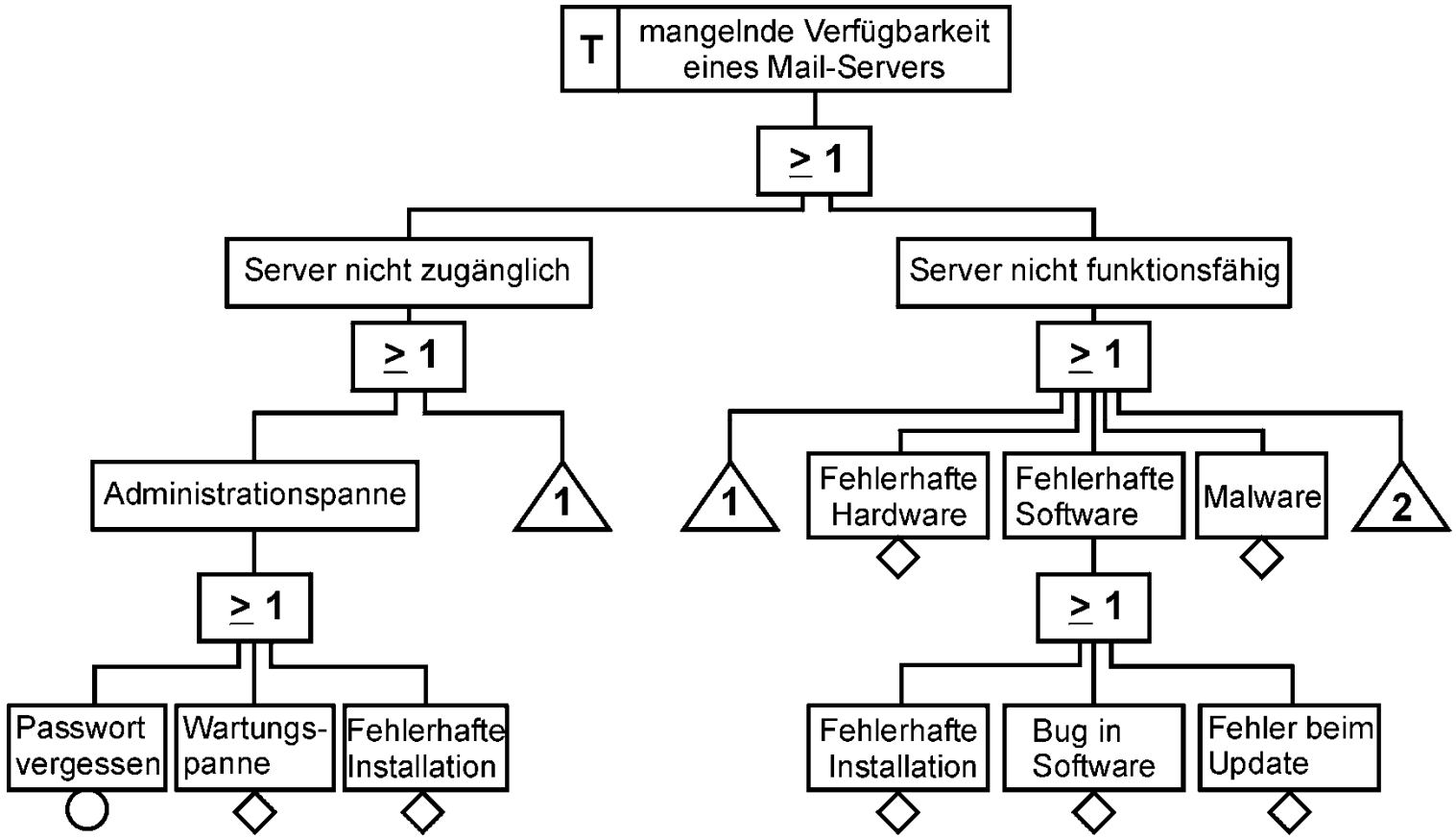
**Aufgabe**:

- A) Erstellen Sie eine **Fehlerbaum** (Fault Tree Analysis) zu dem Fehlerereignis "mangelnde Verfügbarkeit eines Mail-Servers".
- B) Welche Gründe (= Basisereignisse) sind der **Safety** (unbeabsichtigte Ereignisse) zuzuordnen und welche der **Security** (beabsichtigte Angriffe)?

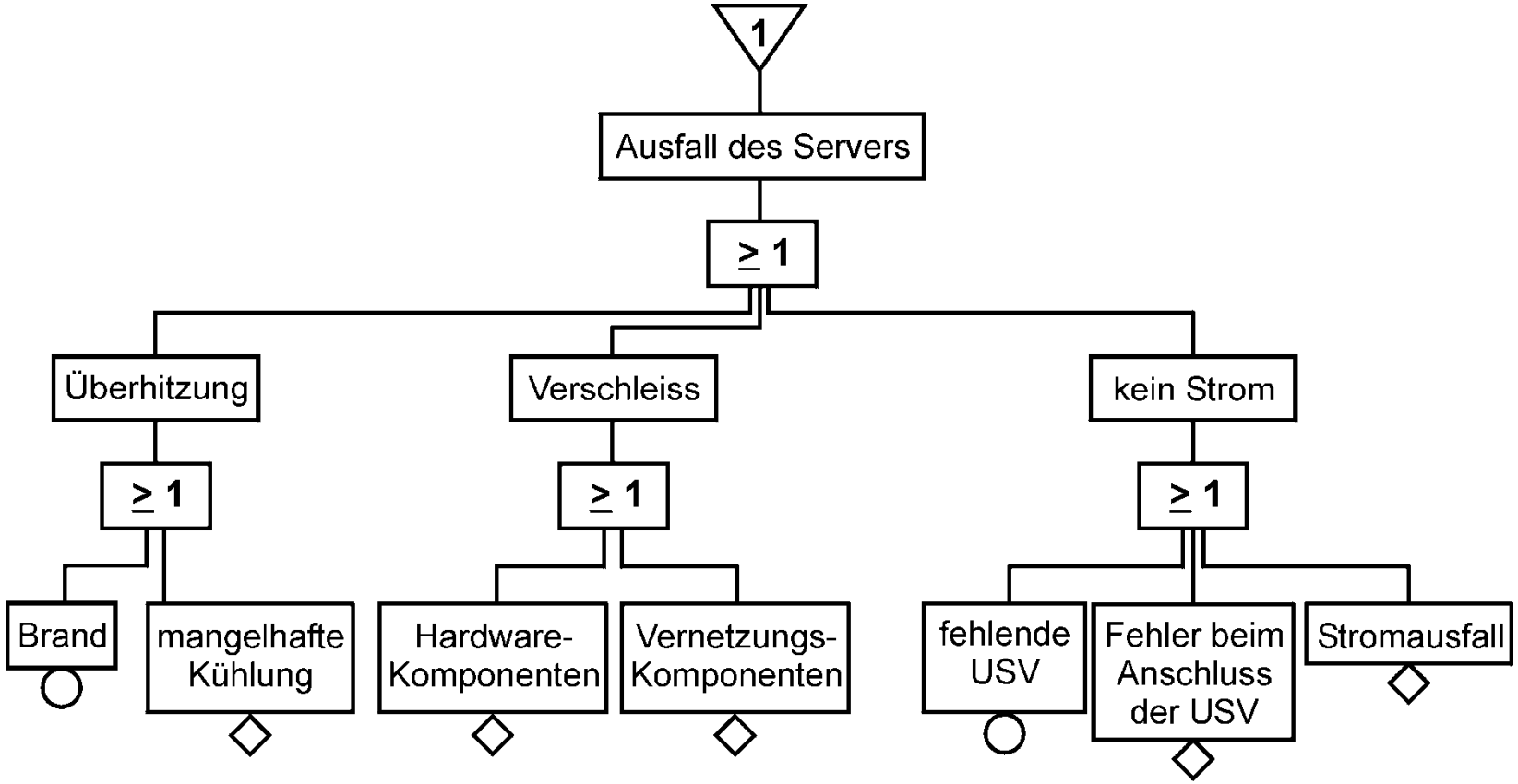
Lösungshinweis zu 7.4 & 7.5:

- Recherchieren Sie im Web zu diesen beiden Analyse-Methoden, wie entsprechende Darstellungen von Fehlerbaum bzw. Angriffsbaum aussehen.

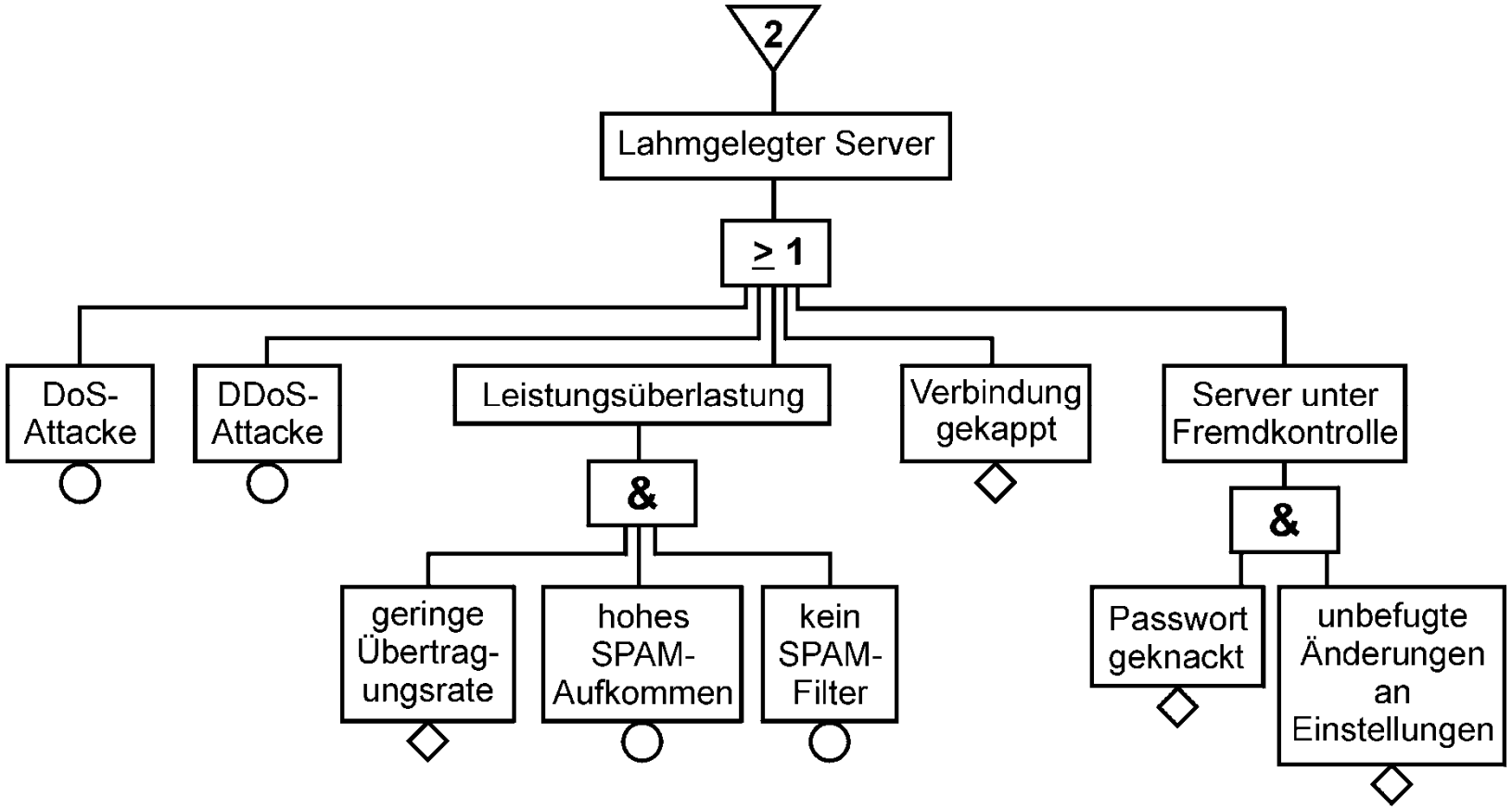
# 7.4 Fehlerbaum (1)



# 7.4 Fehlerbaum (2)



# 7.4 Fehlerbaum (3)



# 7.4 Fehlerbaum (4)

**Gründe aus Safety-Sicht**:

- Ausfall des Servers aufgrund
  - Überhitzung
  - Verschleiss
  - kein Strom
- Administrationspanne aufgrund
  - vergessenes Passwort
  - Wartungspanne
  - fehlerhafte Installation
- fehlerhafte Hardware
- fehlerhafte Software
  - fehlerhafte Installation
  - Bug in Software
  - Fehler beim Update

**Gründe aus Security-Sicht**:

- lahmgelegter Server aufgrund
  - DoS-Attacke
  - DDoS-Attacke
  - Leitungsüberlastung
  - gekappten Verbindungen
  - Server unter Fremd-kontrolle
- Malware

# 7.5 Angriffsbaum

**Aufgabe**:

- Erstellen Sie einen **Angriffsbaum** (Attack Tree Analysis) für das Angriffsziel "Beeinträchtigung der Verfügbarkeit eines Mail-Servers".

Lösungshinweis zu 7.4 & 7.5:

- Recherchieren Sie im Web zu diesen beiden Analyse-Methoden, wie entsprechende Darstellungen von Fehlerbaum bzw. Angriffsbaum aussehen.

# 7.5 Angriffsbaum