# Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 5. Übung im SoSe 2013:

Mehrseitige IT-Sicherheit & Risikomanagement

# 5.1 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%).

# 5.1 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)**

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

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

# 5.2 Risikoportfolio Vertraulichkeit

**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).

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:

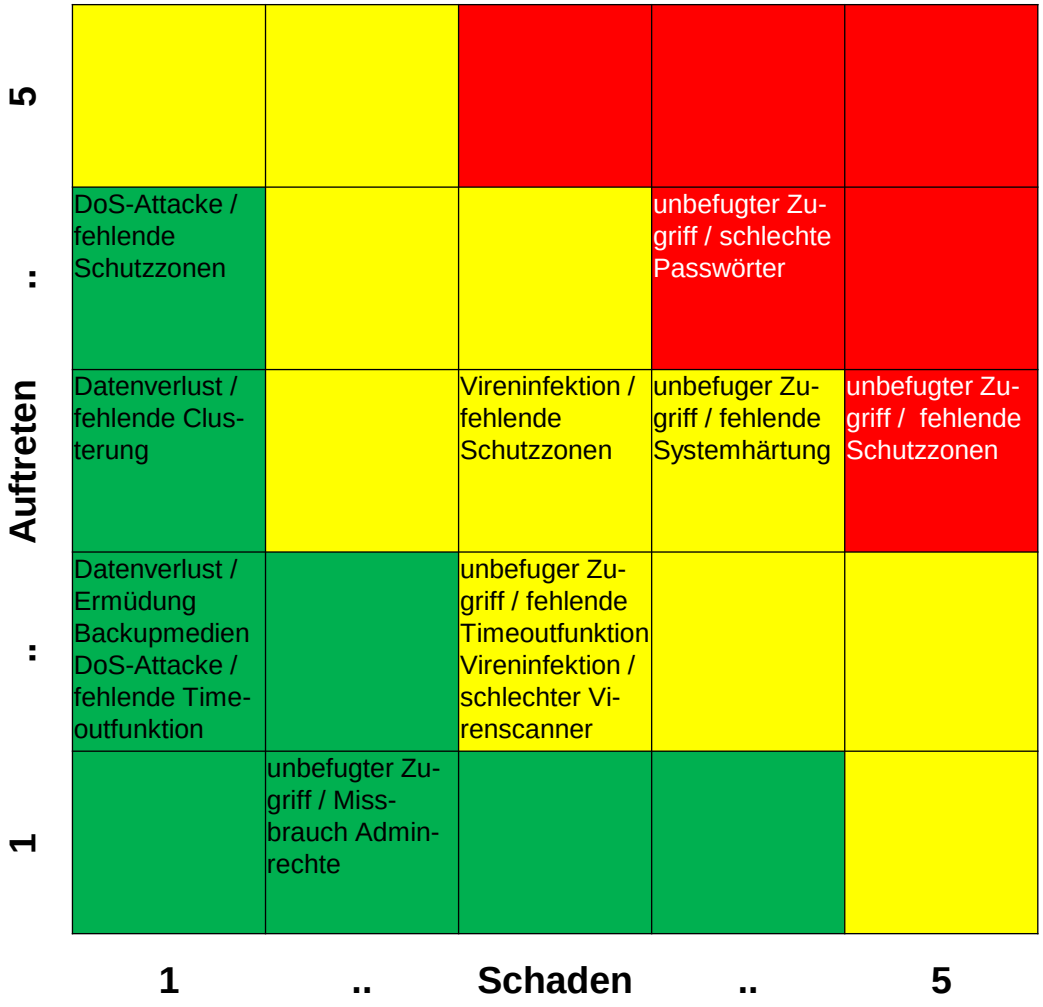
° Felder, die ein Risiko bis max. den Wert 4 aufweisen, gelten dabei als akzeptabel.

° 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?

# 5.2 Risikoportfolio Vertraulichkeit (1)



# 5.2 Risikoportfolio Vertraulichkeit (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):

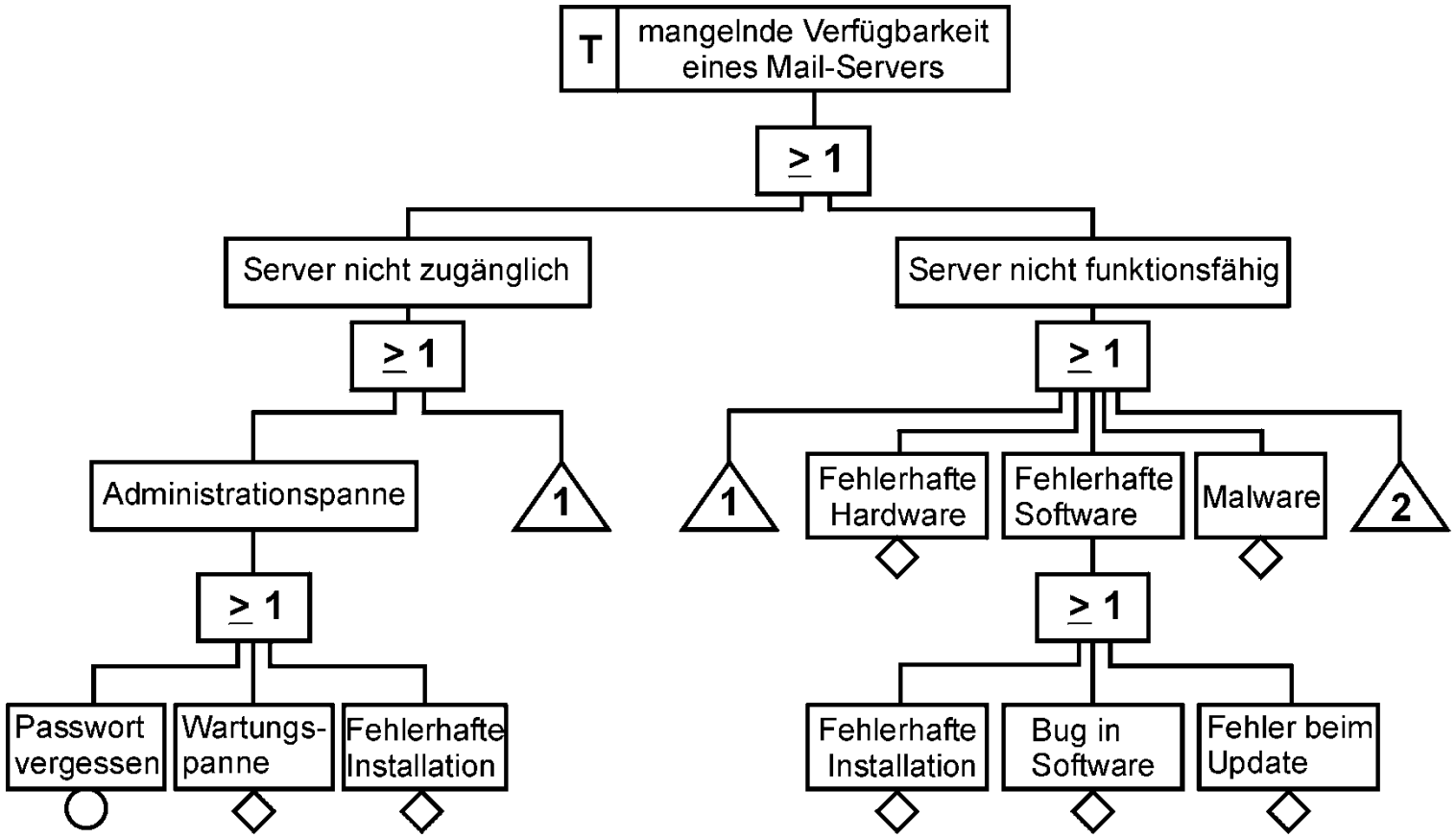
- Die Server sollen auf gehärteten Systemen betrieben werden, indem alle nicht notwendigen Dienste entfernt werden.
- Auf jedem Server soll ein Virenschutz implementiert sein (durch die bereits erfolgte Schutzzoneneinführung greift das bereits voll).

# 5.3 Fehlerbaum

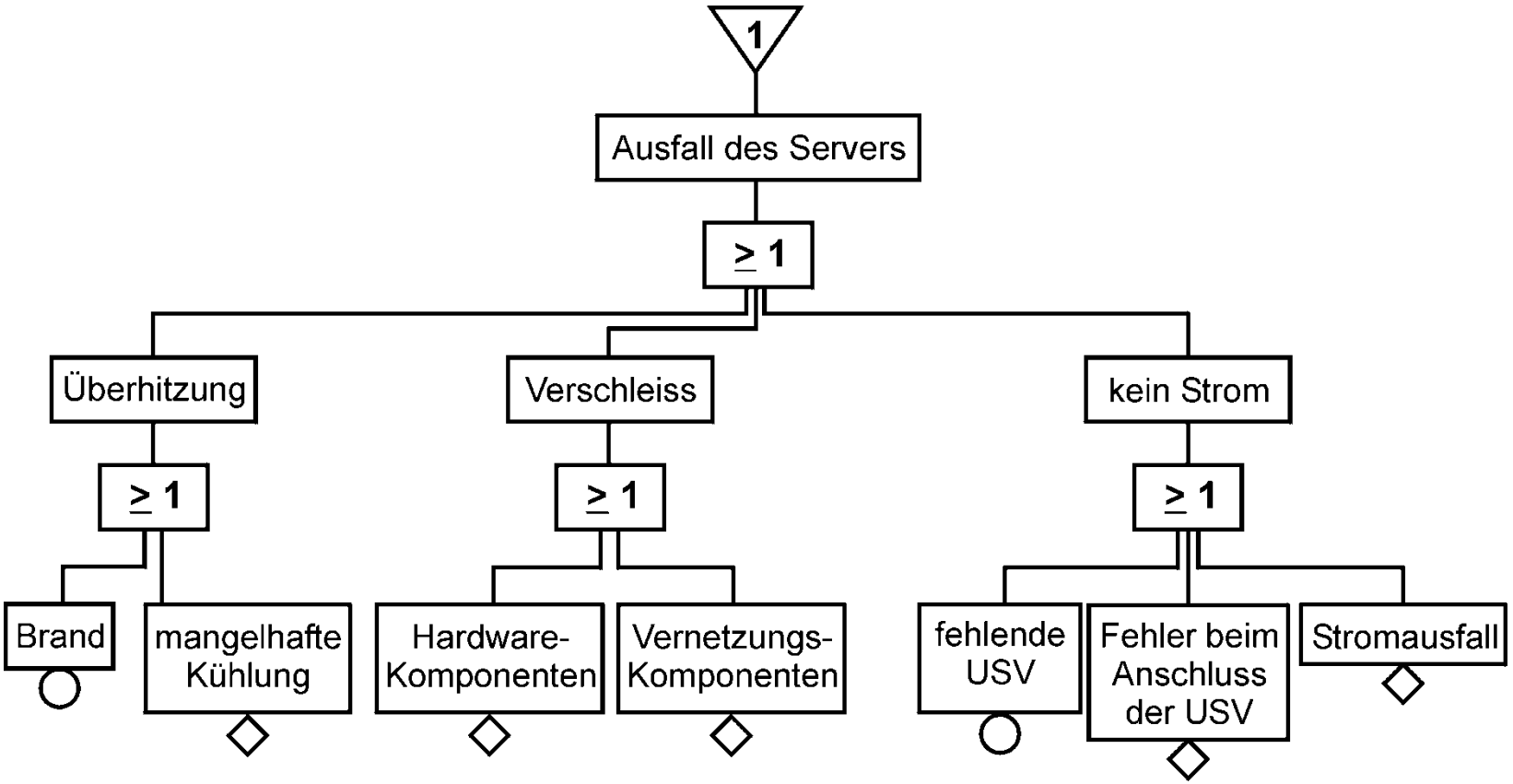
**Aufgabe**:

- Erstellen Sie eine **Fehlerbaum** (Fault Tree Analysis) zu dem Fehlerereignis "mangelnde Verfügbarkeit eines Mail-Servers".

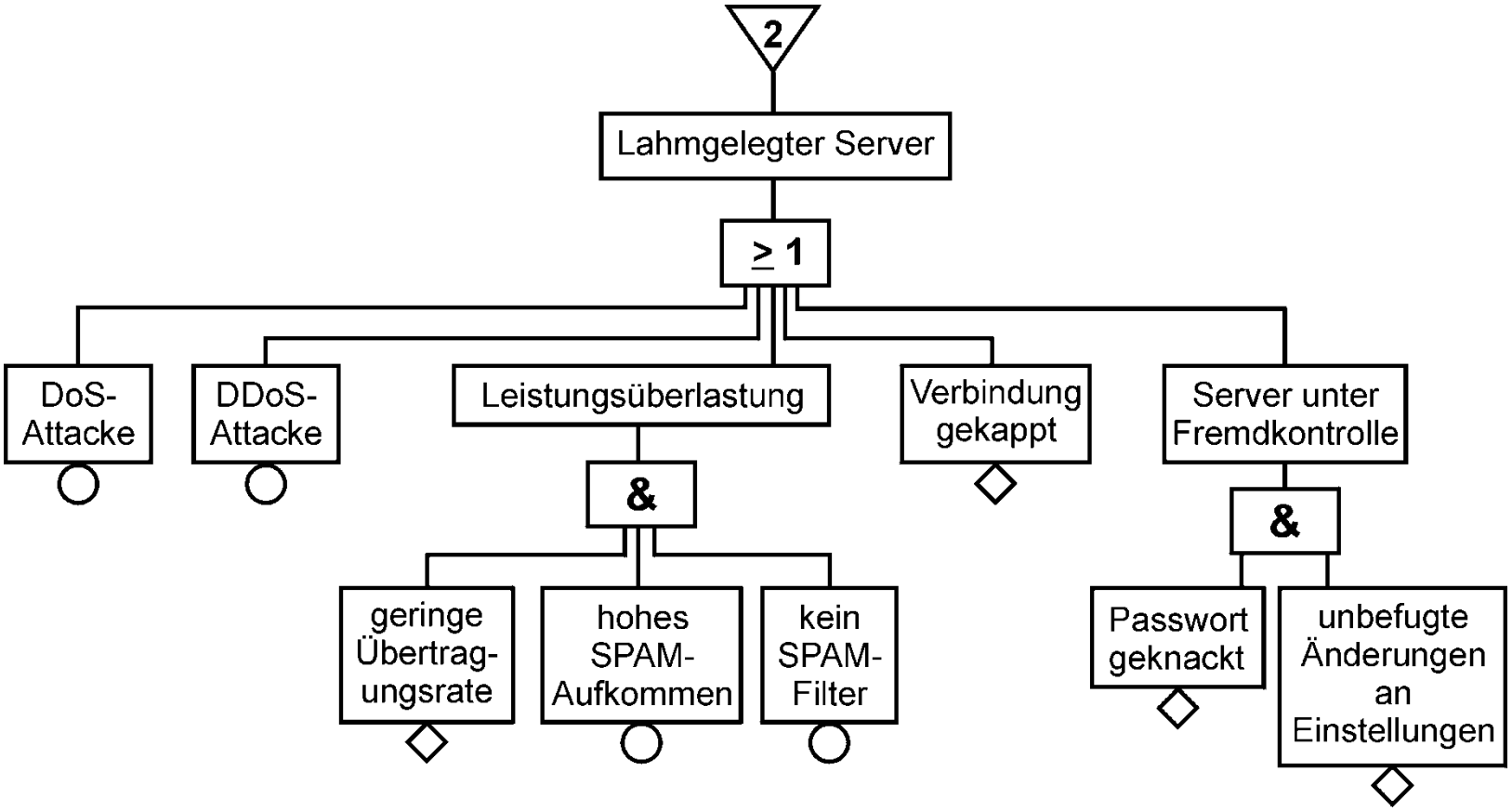
# 5.3 Fehlerbaum (1)



# 5.3 Fehlerbaum (2)



# 5.3 Fehlerbaum (3)

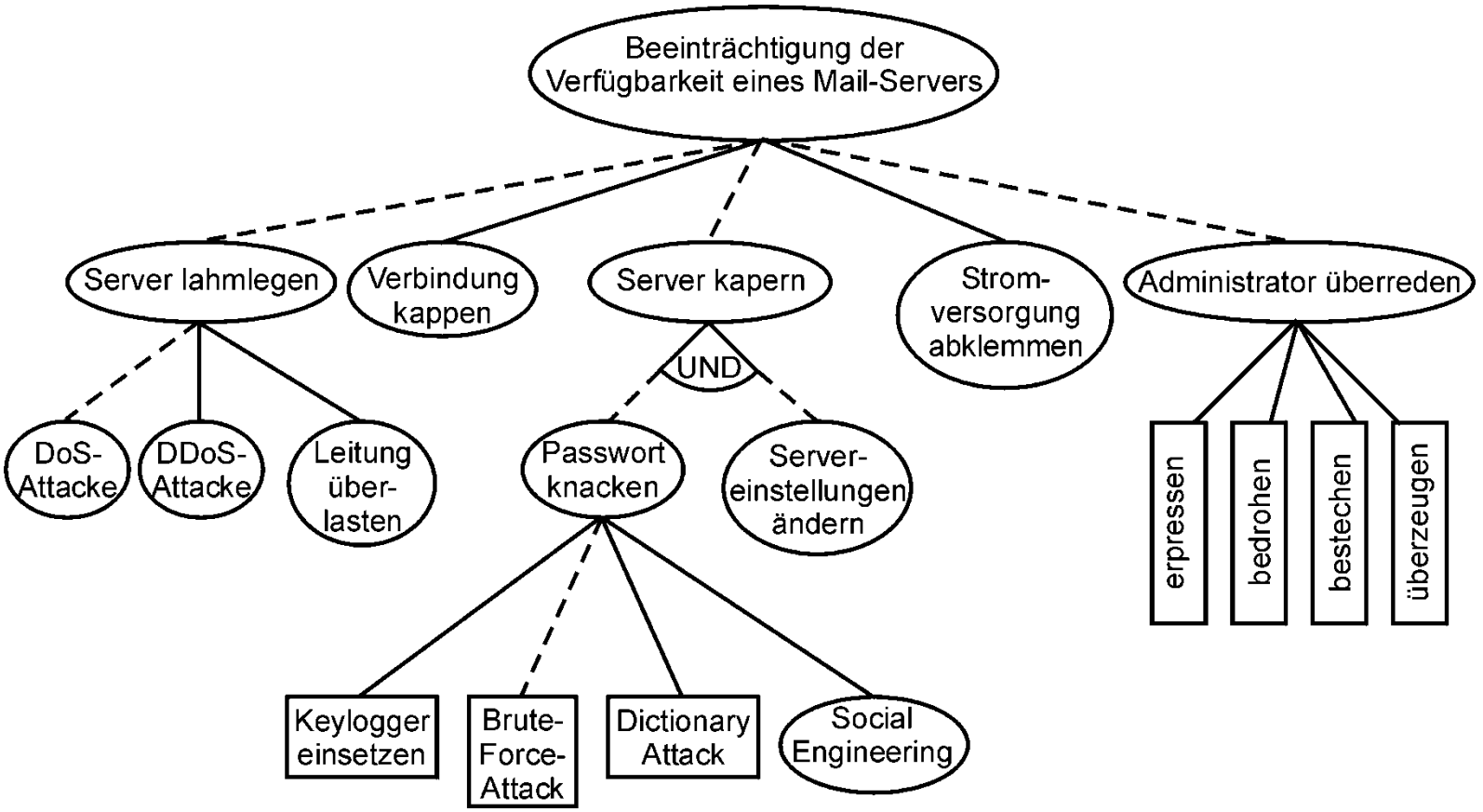


# 5.4 Angriffsbaum

**Aufgabe**:

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

# 5.4 Angriffsbaum



# 5.5 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!

# 5.5 Sicherheitskonzept

**Abwehr gängigster Schwachstellen durch folgende Controls**:

- Sensibilisierung und Schulung der Mitarbeiter
- Authentisierung bei Zugang und Zugriff anhand Wissen/Besitz/Merkmal
- Aktueller 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
- Einrichtung eines Vulnerability Managements
- regelmäßige Kontrollen (z.B. durch Penetrationstests)

→ **Hilfsmittel**: Sicherheitsleitlinie (information security policy), mit dem die Ziele im einzelnen als Control Objectives vorgegeben werden. Die Einzelmaßnahmen werden dann in entsprechenden Policies (zu Awareness, Access Management, Virenschutz, Netzwerksicherheit, Testverfahren, Dokumentationsmanagement, Vulnerability Management & Wirksamkeitskontrollen) geregelt.