Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 7. Übung im SoSe 2014:
IT-Risikomanagement

7.1 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:

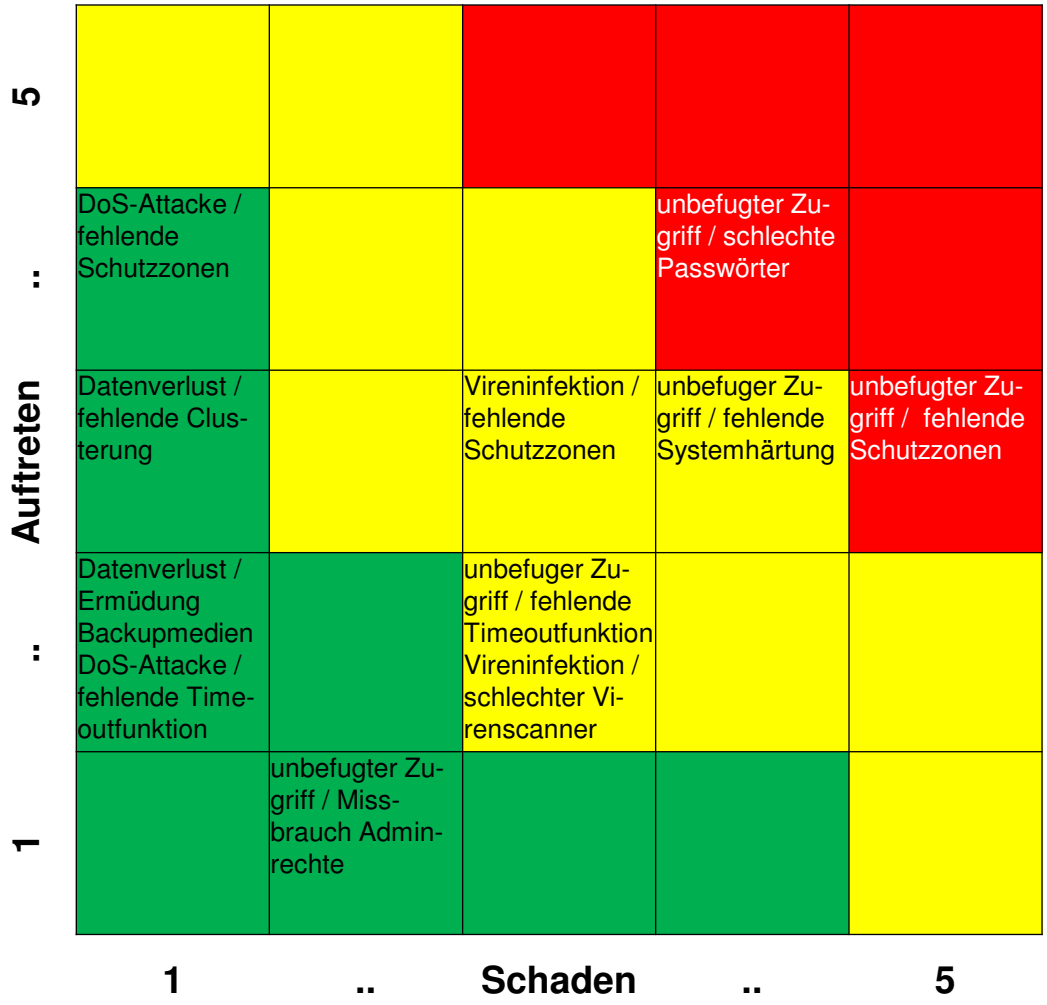
° Felder, die ein Risiko bis max. den Wert 4 aufweisen, gelten dabei als akzeptabel.

° 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?

7.1 Risikoportfolio Vertraulichkeit (1)



7.1 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).

7.2 Tabelle Verfügbarkeitsrisiken

Aufgabe:

- Erstellen Sie anhand der Werte aus 7.1 die zugehörige **Risiko-matrix** 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.

7.2 Tabelle Verfügbarkeitsrisiken

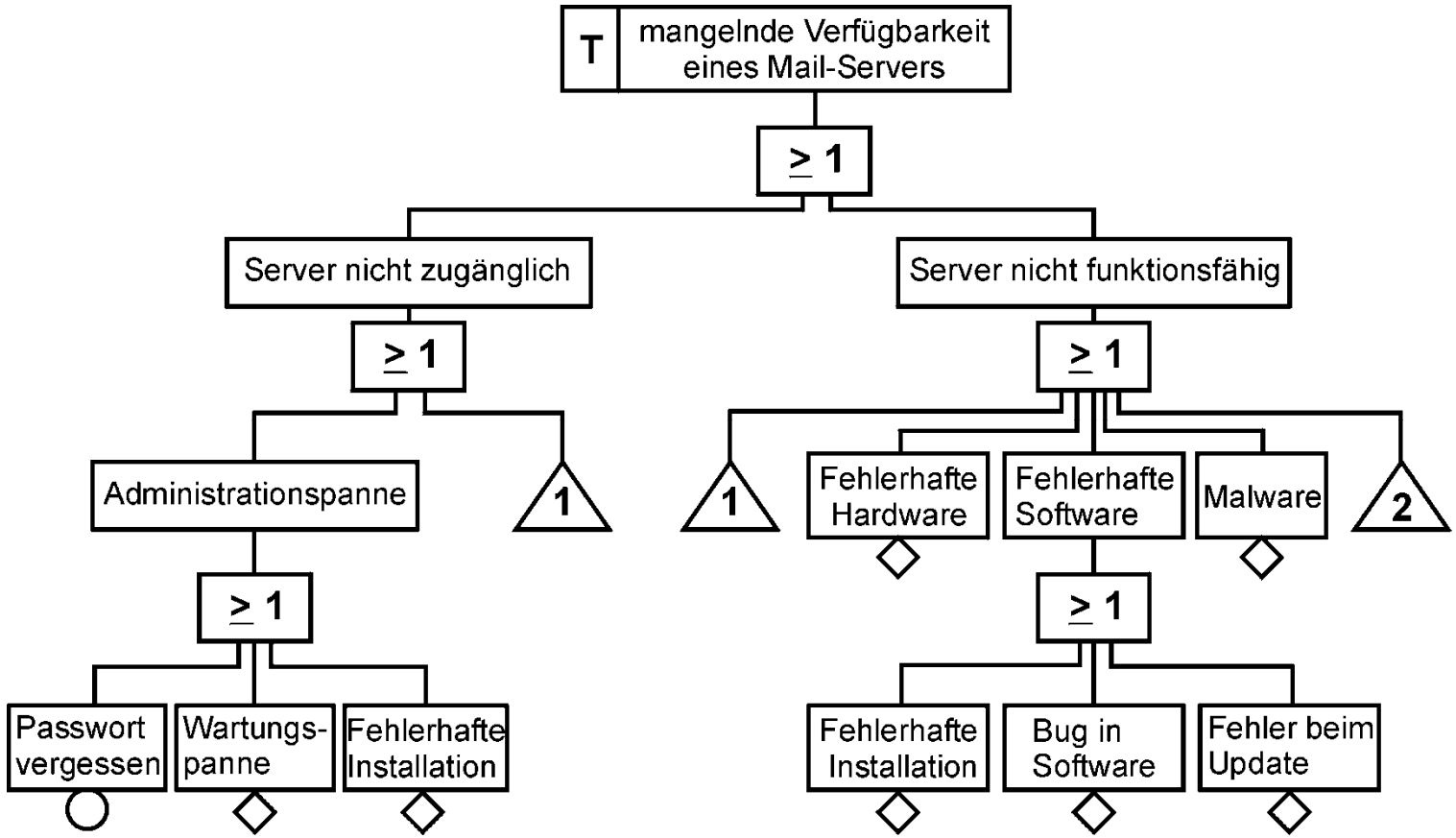
Rg.	Gefährdung	Auftreten	Schaden	Risiko
1.	DoS-Attacke durch fehlende Schutzzonen	4	5	20
2.	unbefugter Zugriff durch fehlende Schutzzonen	3	5	15
3.	unbefugter Zugriff durch fehlende Systemhärtung	3	4	12
3.	Vireninfektion durch fehlende Schutzzonen	3	4	12
5.	Datenverlust durch fehlende Clusterung	3	3	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

7.3 Fehlerbaum

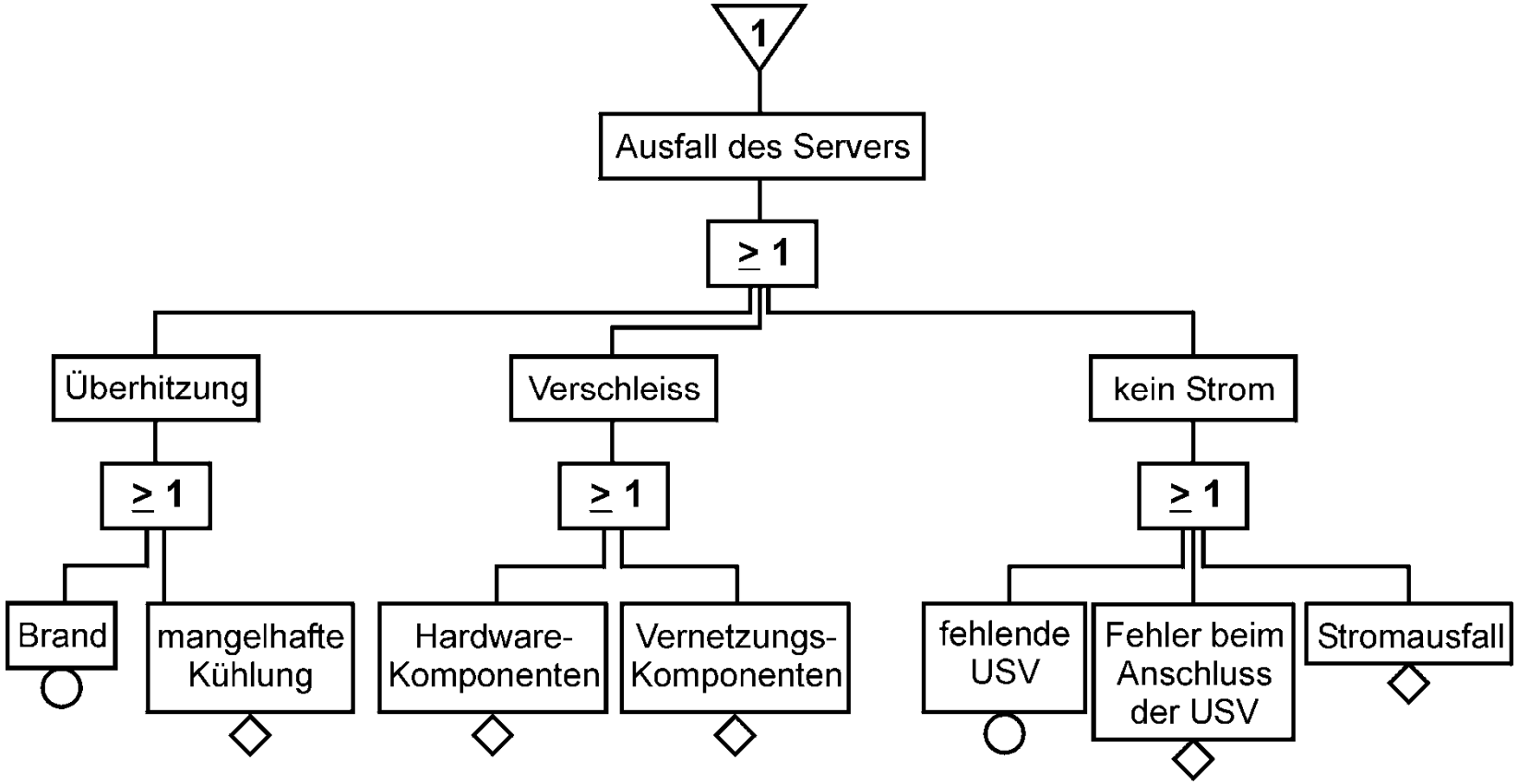
Aufgabe:

- 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)?

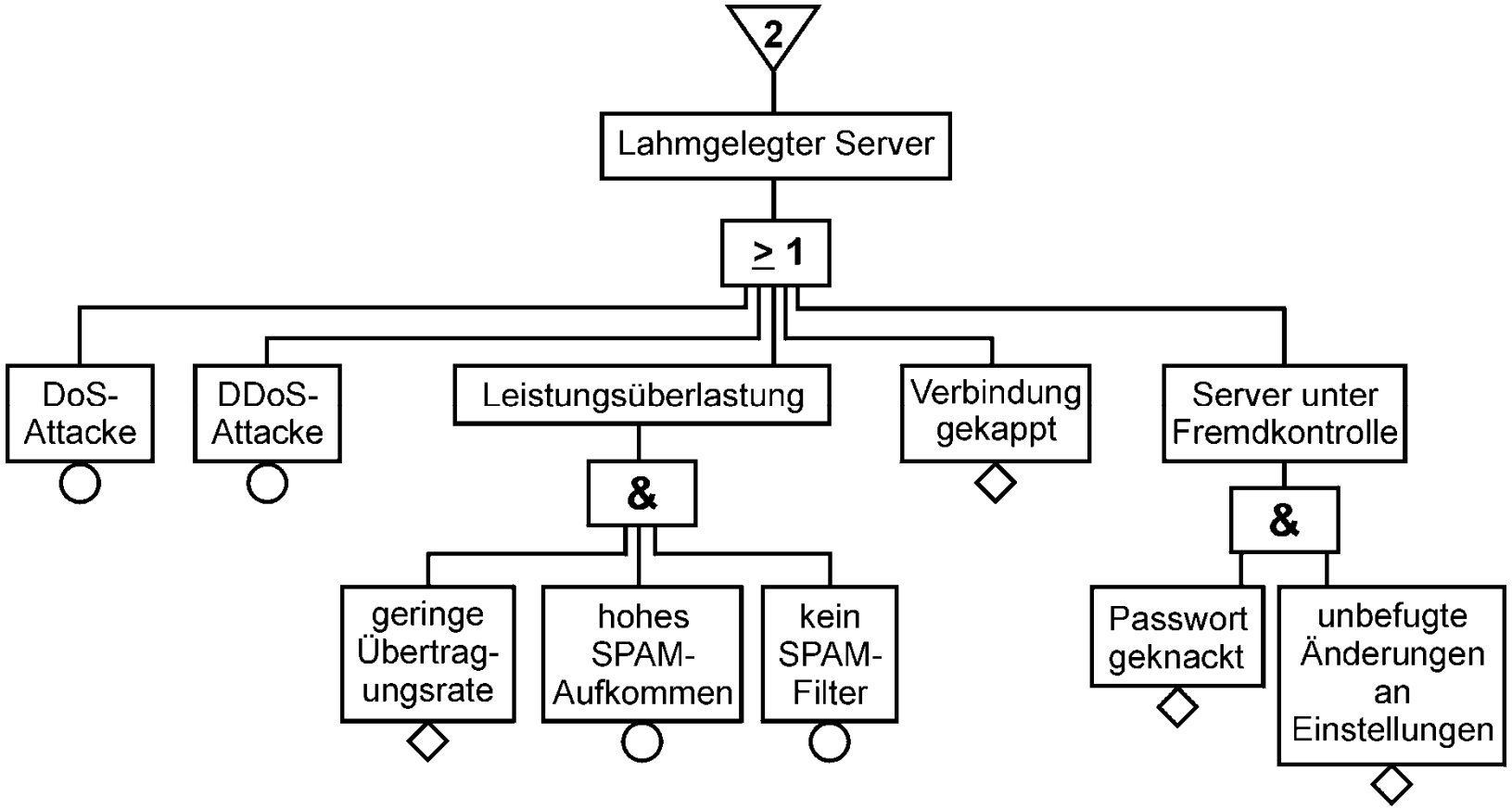
7.3 Fehlerbaum (1)



7.3 Fehlerbaum (2)



7.3 Fehlerbaum (3)



7.3 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:

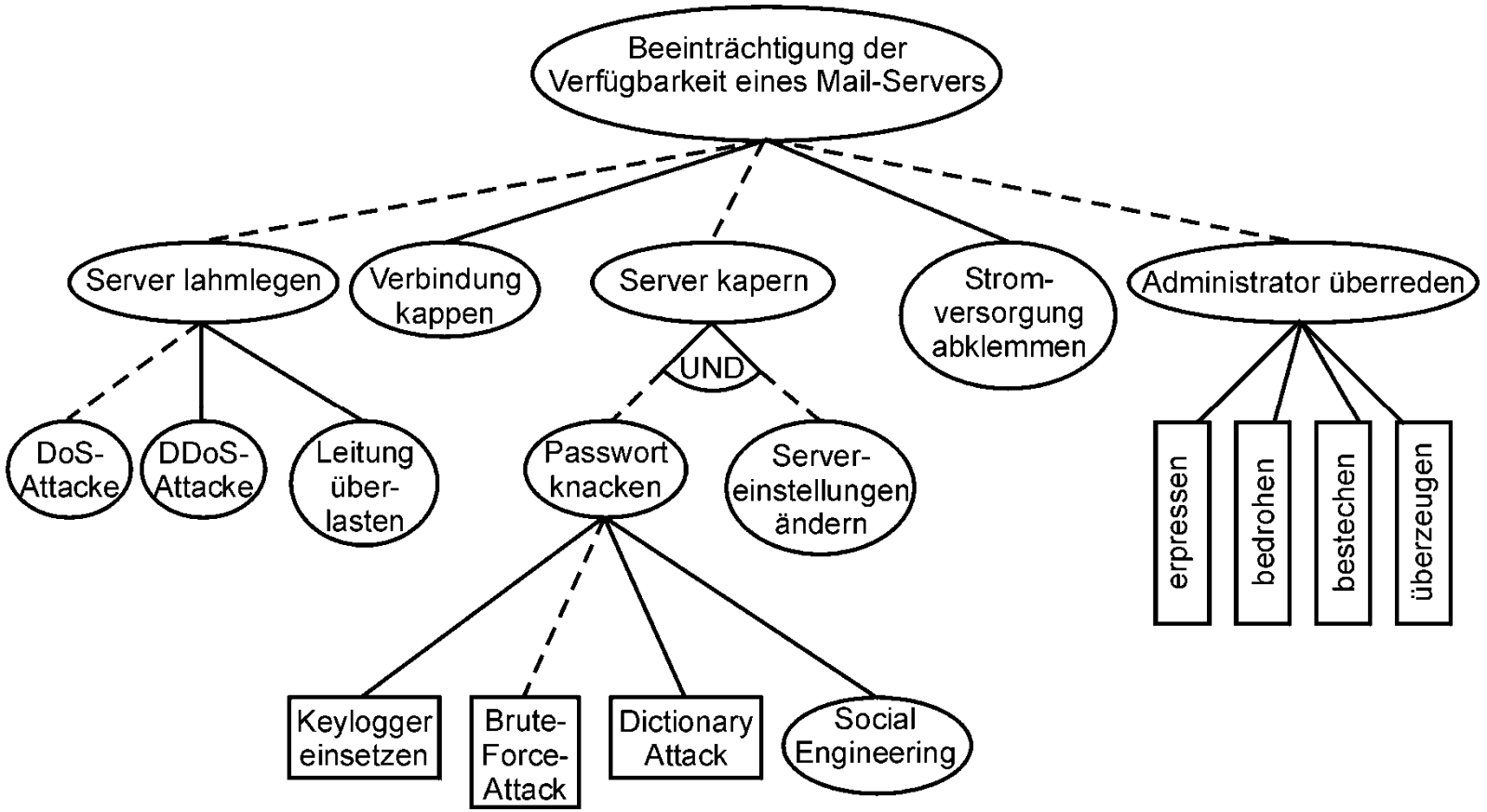
- lahmgelegter Server aufgrund
  - DoS-Attacke
  - DDoS-Attacke
  - Leitungsüberlastung
  - gekappten Verbindungen
  - Server unter Fremd-kontrolle
- Malware

7.4 Angriffsbaum

Aufgabe:

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

7.4 Angriffsbaum



7.5 Fehlerbaum vs. Angriffsbaum

Aufgabe:

- A) Welche **Unterschiede** stellen Sie bei diesen beiden Analyse-Methoden fest?
- B) Welche **Schwachstellen** lassen sich anhand dieser beiden Analyse-Methoden ermitteln? Welche Konsequenzen würden Sie als verantwortlicher IT-Leiter daraus ziehen?

7.5 Fehlerbaum vs. Angriffsbaum (1)

- Bei der Fehlerbaumanalyse ist der Ausgangspunkt der festgestellte Fehler (hier: mangelnde Verfügbarkeit eines Mail-Servers), während bei der Angriffsbaumanalyse die Sicht des potentiellen Angreifers hinsichtlich seines Angriffsziels (hier: Beeinträchtigung der Verfügbarkeit eines Mail-Servers) maßgeblich ist
- Ziel der Fehlerbaumanalyse ist das Herausfinden von Single-Point-of-Failure, während bei der Angriffsbaumanalyse untersucht wird, welche Wege für einen Angreifer hinreichend lukrativ sind
- Bei Fehlerbaumanalyse sind Aspekte der Safety als auch der Security maßgeblich (also eine umfassende Analyse gegeben), bei der Angriffsbaumanalyse lediglich der Security [Grund: Safety durch Notfall-Vorsorge bereits abgedeckt]
- Die Gefährdung durch Bedrohung lässt sich bei der Angriffsbaumanalyse präziser ablesen, da ein intelligent handelnder Angreifer zugrunde gelegt wird, und es ist effektiver zu ermitteln, welche Maßnahmen zur Abwehr zu ergreifen sind

7.5 Fehlerbaum vs. Angriffsbaum (2)

Hinweise:

- Üblicherweise werden bei der Fehlerbaumanalyse noch die Ausfall-wahrscheinlichkeiten betrachtet
- Bei der Angriffsbaumanalyse werden die einzelnen Maßnahmen üblicherweise noch bewertet (anhand benötigter Ressourcen)
- In beiden Fällen können die Risiken auf der Basis der Analyse mathematisch berechnet werden

7.5 Fehlerbaum vs. Angriffsbaum (3)

Konsequenzen aus den Schwachstellenanalysen:

- Administrationspannen vermeidbar
  → Administrationspasswort im Safe hinterlegen, keine unmittelbaren Änderungen am Produktivsystem vornehmen, sondern immer erst an einem Testsystem, Standardisierungen vornehmen
- Ausfall des Servers durch Beeinträchtigung der Safety
  → Notfall-Vorsorge-Konzept unter Berücksichtigung physischer Sicherheit
- Bedrohungen durch Malware und informations-technischen Angriffen
  → geeignete Gegenmaßnahmen ergreifen (Virenscanner, Intrusion Detection System, Penetrationstests, need-to-know-Prinzip bei Rechtevergabe, komplexe Passwörter, ...)

7.5 Fehlerbaum vs. Angriffsbaum (4)

Konsequenzen aus den Schwachstellenanalysen:

- Softwarefehler reduzieren
  → eingesetzte Software umfassend testen, nur von vertrauenswürdigen Stellen beziehen und aufgrund von Zertifikaten einsetzen
- Mitarbeiterattacken vermeiden
  → Mitarbeiter schulen und durch leistungsgerechte Bezahlung und guter Atmosphäre motivieren ;-)