Grundlagen des Datenschutzes und der IT-Sicherheit

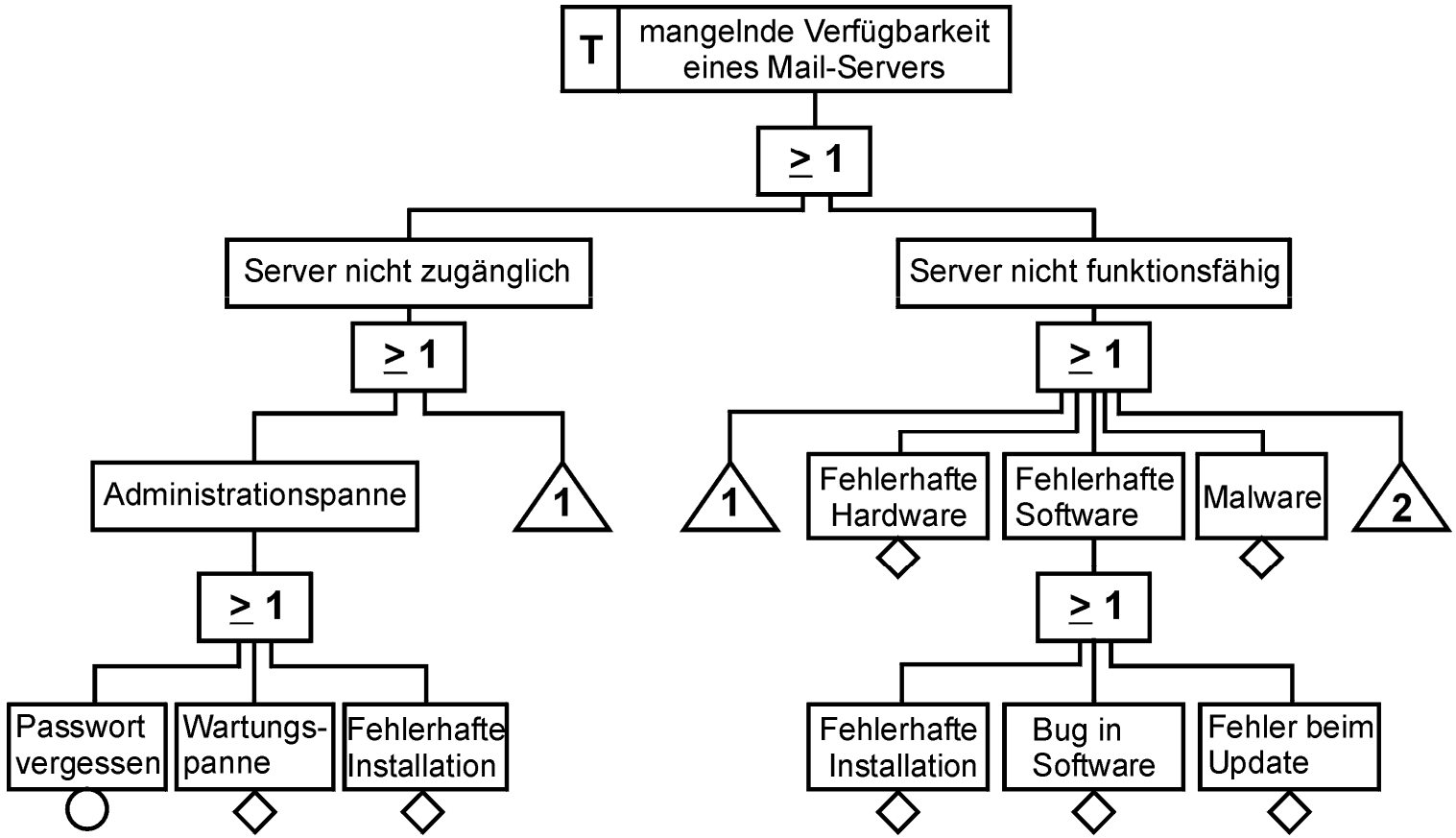
Musterlösung zur 5. Übung im SoSe 2011:
IT-Sicherheit (2)

5.1 Fehlerbaum

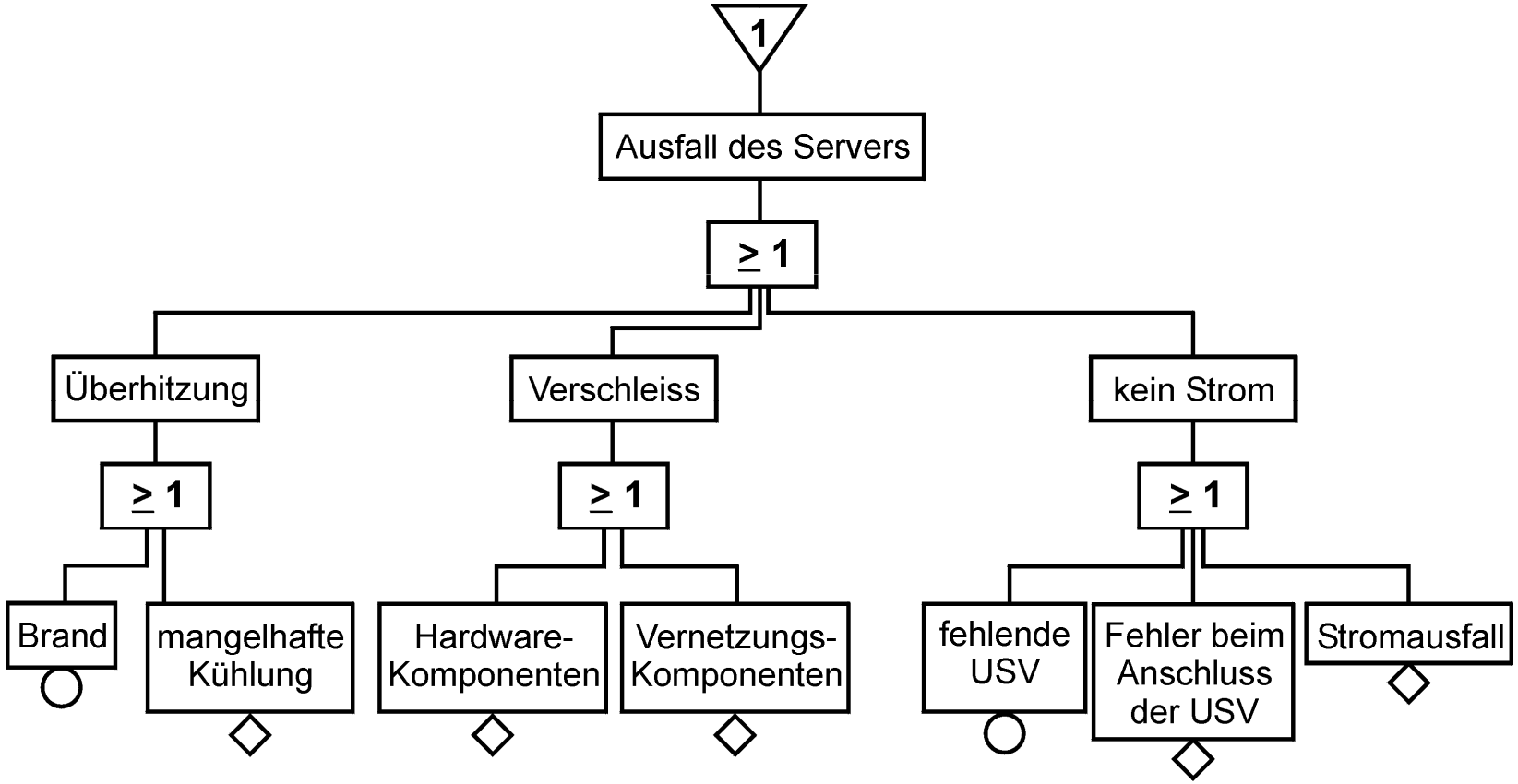
Aufgabe:

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

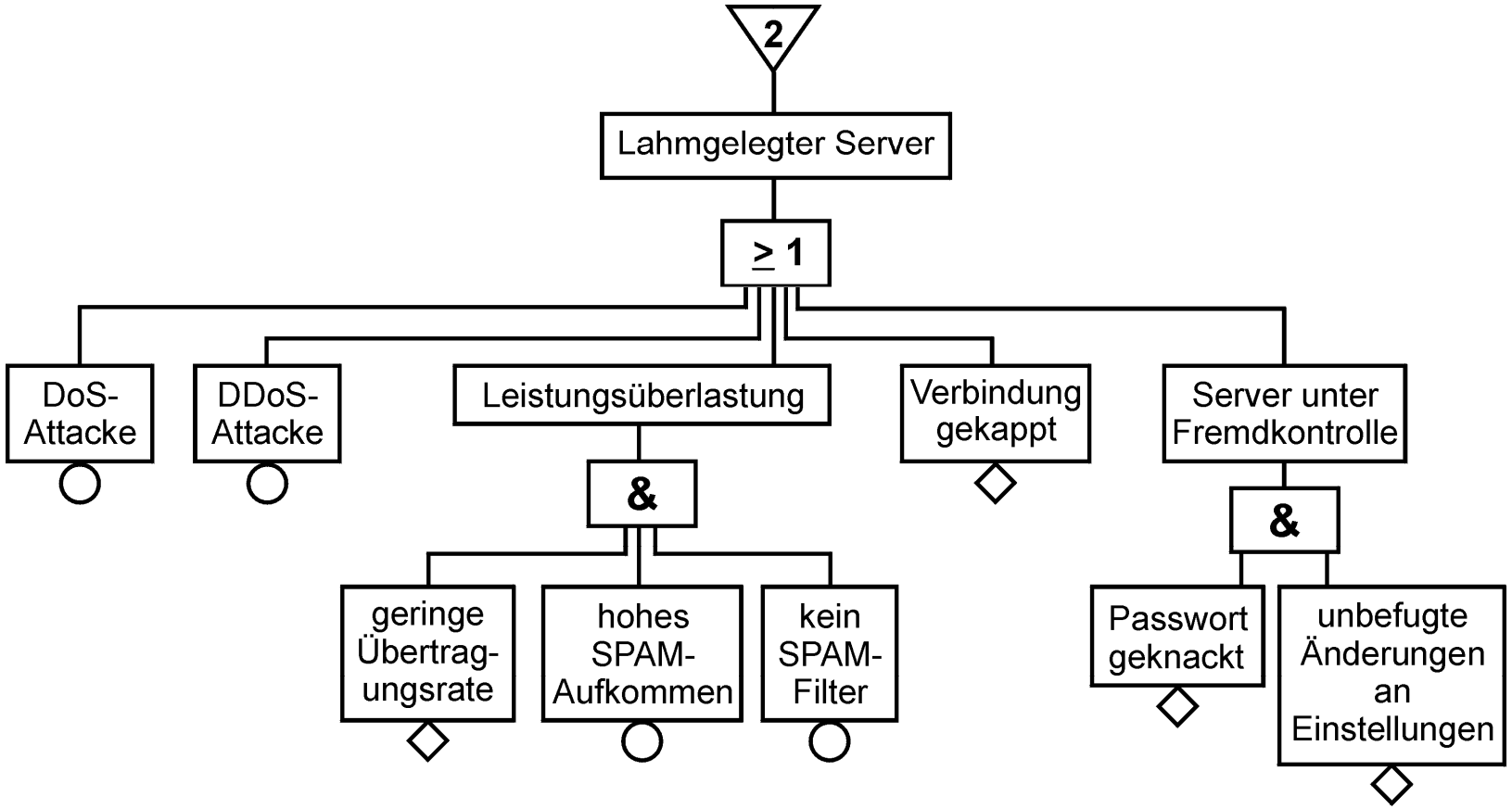
5.1 Fehlerbaum (1)



5.1 Fehlerbaum (2)



5.1 Fehlerbaum (3)

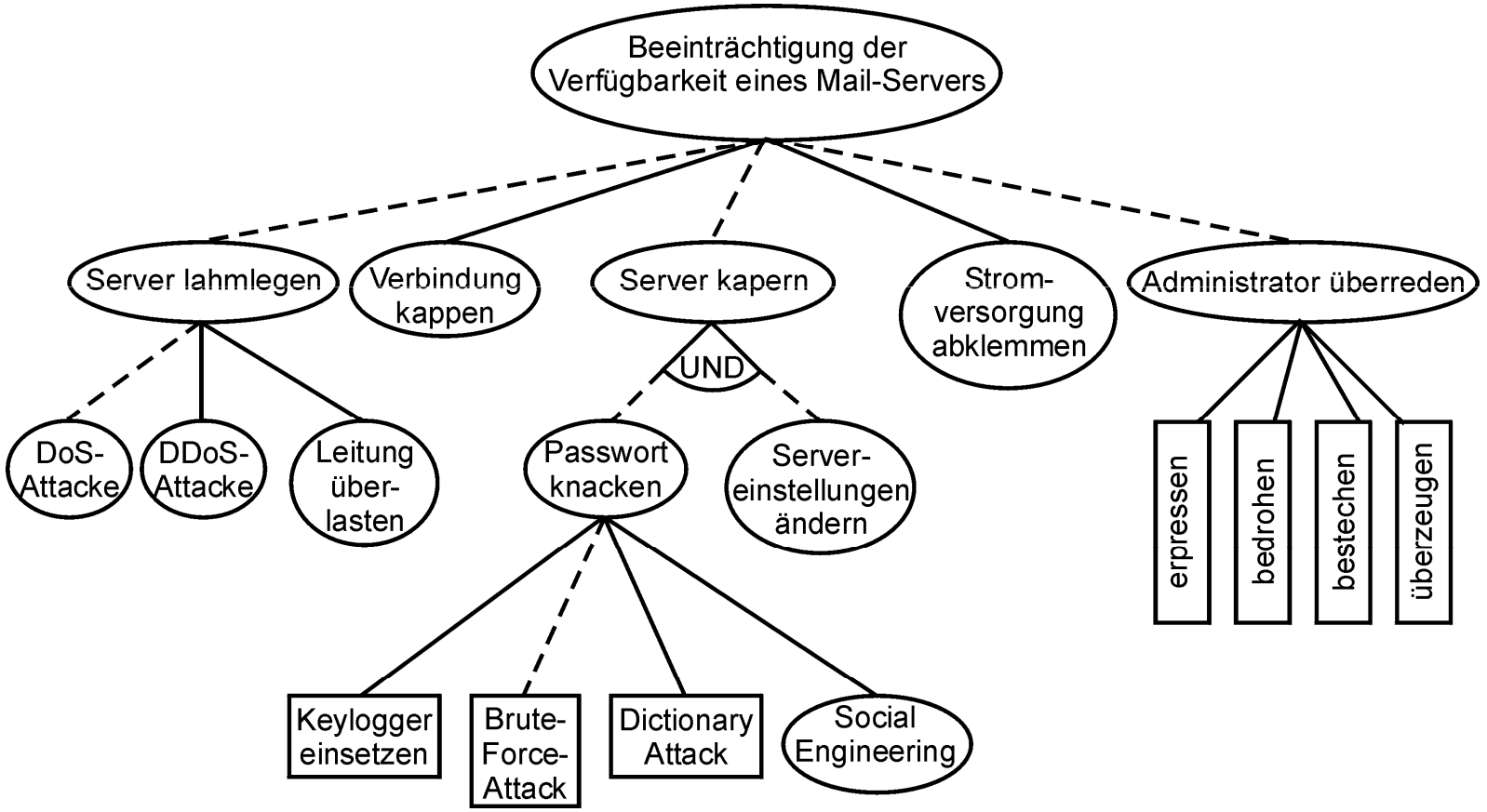


5.2 Angriffsbaum

Aufgabe:

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

5.2 Angriffsbaum



5.3 Fehlerbaum vs. Angriffsbaum

Aufgabe:

- Inwiefern unterscheiden sich Fehlerbaum-Analyse und Angriffsbaum-Analyse voneinander?

5.3 Unterschiede (1)

- Bei der Fehlerbaumanalyse ist der Ausgangspunkt der festgestellte Fehler (mangelnde Verfügbarkeit eines Mail-Servers laut Aufgabenstellung), während bei der Angriffsbaumanalyse die Sicht des potentiellen Angreifers hinsichtlich seines Angriffsziels (Beeinträchtigung der Verfügbarkeit eines Mail-Servers laut Aufgabenstellung) 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

5.3 Unterschiede (2)

- 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

5.3 Unterschiede (3)

Hinweise:

- Üblicherweise werden bei der Fehlerbaumanalyse noch die Ausfallwahrscheinlichkeiten 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

5.4 Tabelle Verfügbarkeitsrisiken

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 die zugehörige Risikomatrix in Form einer Risikotabelle! Betrachten Sie hierzu lediglich die Verfügbarkeitswerte, da der verantwortlichen Stelle die Verfügbarkeit besonders wichtig sei.

5.4 Tabelle Verfügbarkeitsrisiken

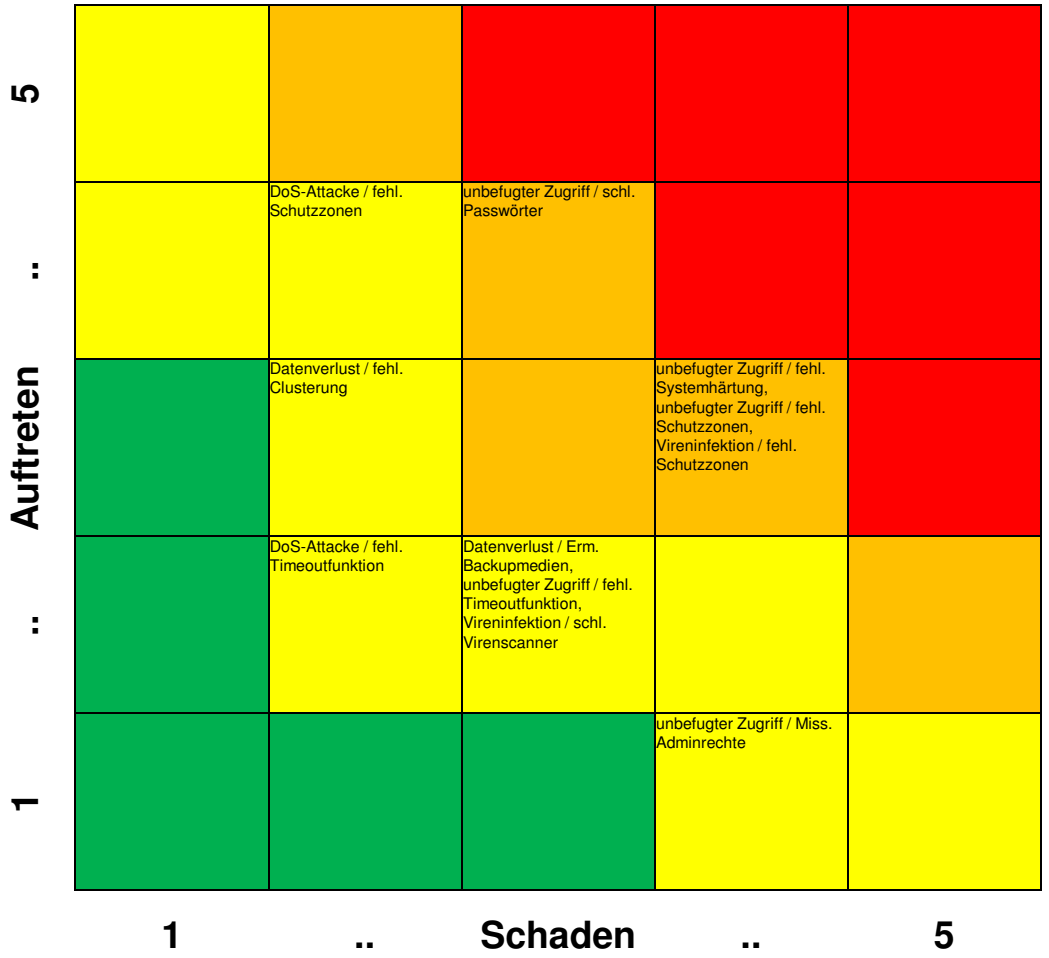
Rg.	Gefährdung	Auftreten	Schaden	Risiko
1.	DoS-Attacke durch fehlende Schutzzonen	4	5	20
2.	unbefugter Zugriff durch fehlende Schutzzonen	3	5	15
3.	unbefugter Zugriff durch fehlende Systemhärtung	3	4	12
3.	Vireninfektion durch fehlende Schutzzonen	3	4	12
5.	Datenverlust durch fehlende Clusterung	3	3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

5.5 Risiko-Portfolio

Aufgabe:

- Erstellen Sie für die unter 5.4 aufgelisteten Werte das zugehörige Risiko-Portfolio unter Berechnung des jeweiligen Durchschnittsschadens unter Beachtung aller aufgelisteten Bedrohungen und Verwundbarkeiten! Markieren Sie dabei die Felder, die inakzeptable gravierende Risiken beinhalten, sowie die Felder, die akzeptable niedrige Risiken beinhalten. Verwenden Sie dabei eine 5x5-Felder-Matrix. Welche Maßnahmen sollte Ihrer Ansicht nach die Geschäftsleitung dringend einleiten, um das entsprechende Risiko zu minimieren?

5.5 Risiko-Portfolio (1)



5.5 Risiko-Portfolio (2)

- Das Risiko-Portfolio zeigt **keine inakzeptablen Risiken** (rot unterlegt)
- **Handlungsrelevante Risiken** (orange unterlegt) sind:
  - unbefugter Zugriff durch schlechte Passwörter
  - unbefugter Zugriff durch fehlende Systemhärtung
  - unbefugter Zugriff durch fehlende Schutzzonen
  - Vireninfektion durch fehlende Schutzzonen
- Somit ist in jedem Fall die Einrichtung konsequenter Schutzzonen (durch wirksame Netzwerksegregation) zu empfehlen! (Etwa durch Einrichtung einer DMZ)
- Beim kritischen IT-System sollten unbenötigte Dienste entfernt werden und die Komplexitätsanforderung bei Passwörtern aktiviert werden!