

Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 5. Übung im SoSe 2021:
Sicherheitsziele + Risk Assessment

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:

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

- 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)

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

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

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

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

Teil B)

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

$$\begin{aligned} V_{\text{gesamt_neu}} &= V_{\text{server}} \cdot V_{\text{client}} \cdot V_{\text{netzcluster}} = 99,744\% \cdot 99,487\% \cdot 99,994\% \\ &= 99,226\% \end{aligned}$$

Die Verfügbarkeit des IT-Verbundes erhöht sich um 0,757%-Punkte.

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):

Bedrohung	Verwundbarkeit	Auftreten	Schaden		
			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
Vireninfection	fehlende Schutzzonen	3	3	4	4
Vireninfection	schlechter Virens Scanner	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)

Auftreten 1	5					
	..	DoS-Attacke / fehlende Schutzzonen			unbefugter Zugriff / schlechte Passwörter	
	1	Datenverlust / fehlende Clustering		Vireninfection / fehlende Schutzzonen	unbefugter Zugriff / fehlende Systemhärtung	unbefugter Zugriff / fehlende Schutzzonen
	..	Datenverlust / Ermüdung Backupmedien DoS-Attacke / fehlende Timeoutfunktion		unbefugter Zugriff / fehlende Timeoutfunktion Vireninfection / schlechter Virens Scanner		
	1		unbefugter Zugriff / Missbrauch Adminrechte			
		1	..	Schaden	..	5

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):

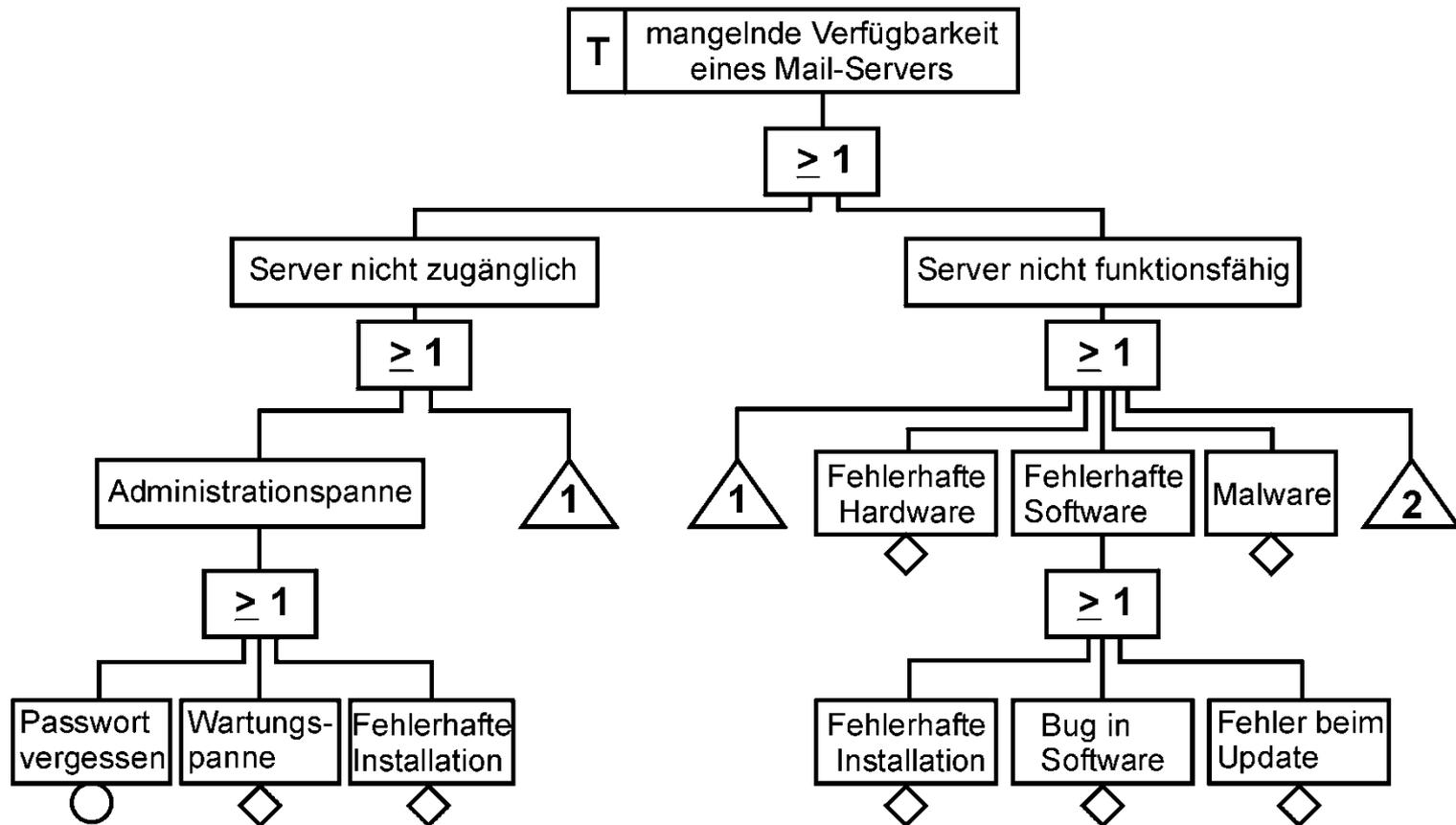
- Die Server sollen auf gehärteten Systemen betrieben werden, indem alle nicht notwendigen Dienste entfernt werden.
- Auf jedem Server soll ein Virenschutz implementiert sein (durch die bereits erfolgte Schutzzoneneinführung greift das bereits voll).

5.3 Fehlerbaum

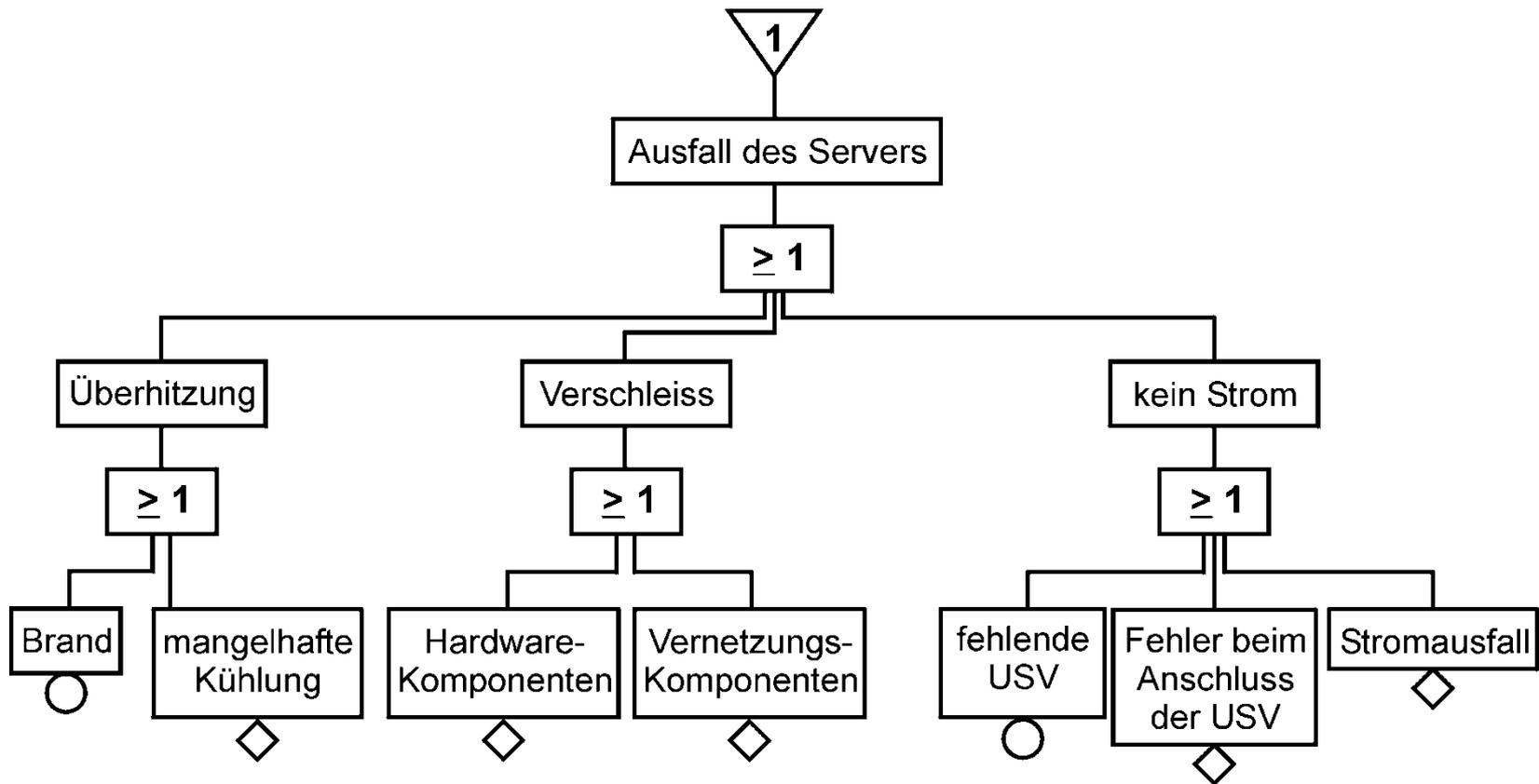
Aufgabe:

- 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)?

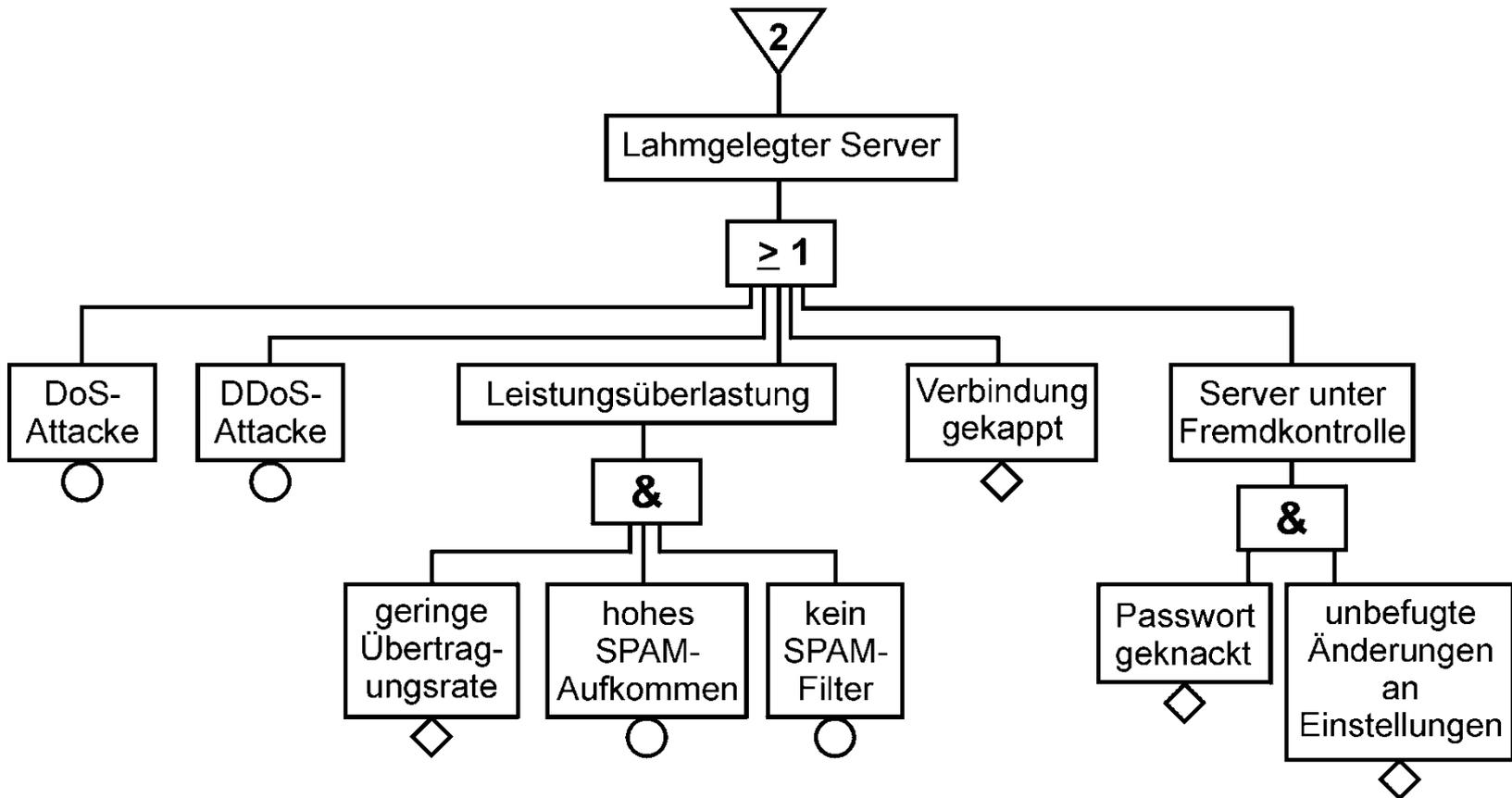
5.3 Fehlerbaum (1)



5.3 Fehlerbaum (2)



5.3 Fehlerbaum (3)



5.3 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:

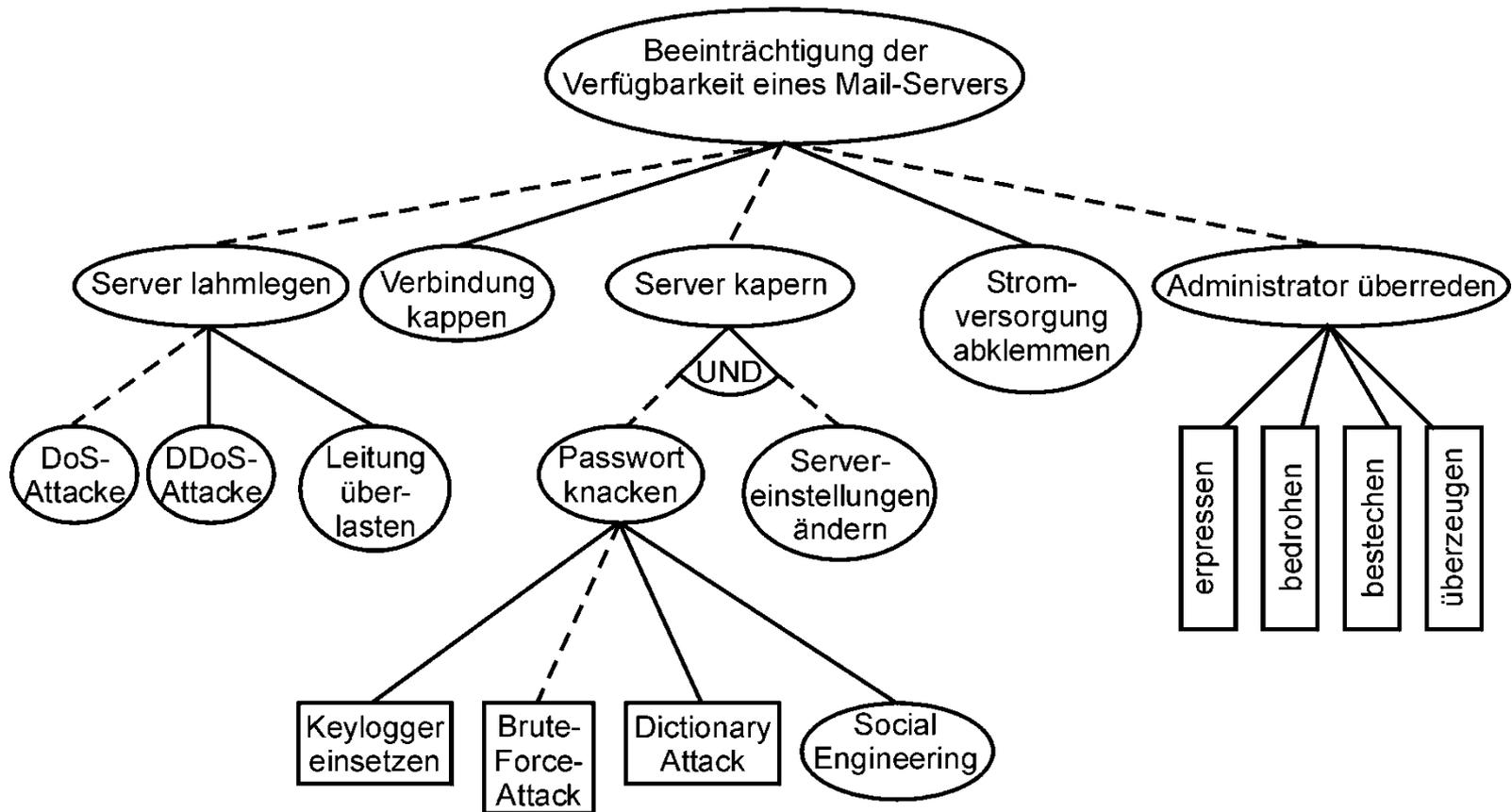
- lahmgelegter Server aufgrund
 - DoS-Attacke
 - DDoS-Attacke
 - Leitungsüberlastung
 - gekappten Verbindungen
 - Server unter Fremdkontrolle
- Malware

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 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?

5.5 Fehlerbaum vs. Angriffsbaum (1)

A) Unterschiede:

- 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

5.5 Fehlerbaum vs. Angriffsbaum (2)

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

5.5 Fehlerbaum vs. Angriffsbaum (3)

B) 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
- Unzureichender Schutz gegen Malware und informationstechnische Angriffe
→ geeignete Gegenmaßnahmen ergreifen (Virens Scanner, Intrusion Detection System, Penetrationstests, need-to-know-Prinzip bei Rechtevergabe, komplexe Passwörter, ...)

5.5 Fehlerbaum vs. Angriffsbaum (4)

Konsequenzen aus den Schwachstellenanalysen:

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