Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 5. Übung im SoSe 2025:

Risk Assessment

5.1 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:

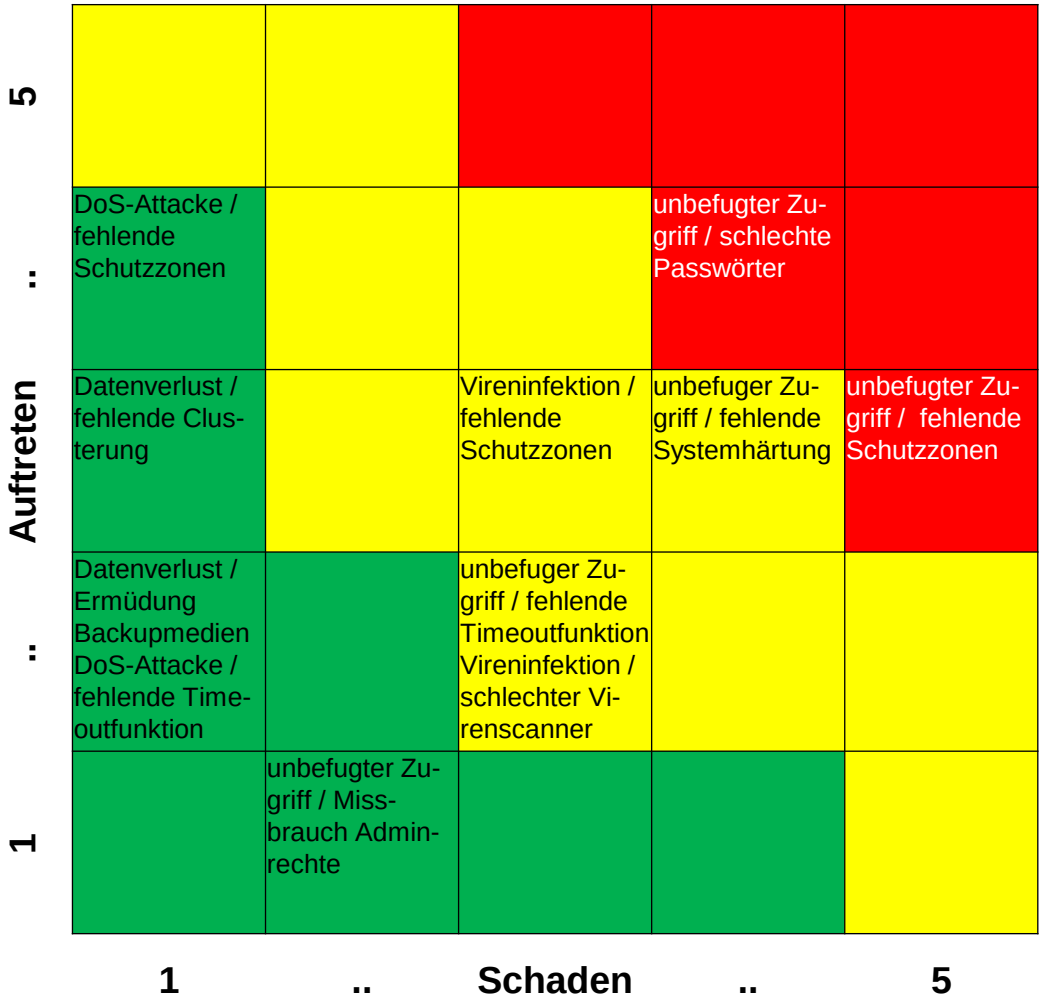
° Felder, die ein Risiko bis max. den Wert 4 aufweisen, gelten dabei als akzeptabel.

° 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?

5.1 Risikoportfolio Vertraulichkeit (1)



5.1 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):

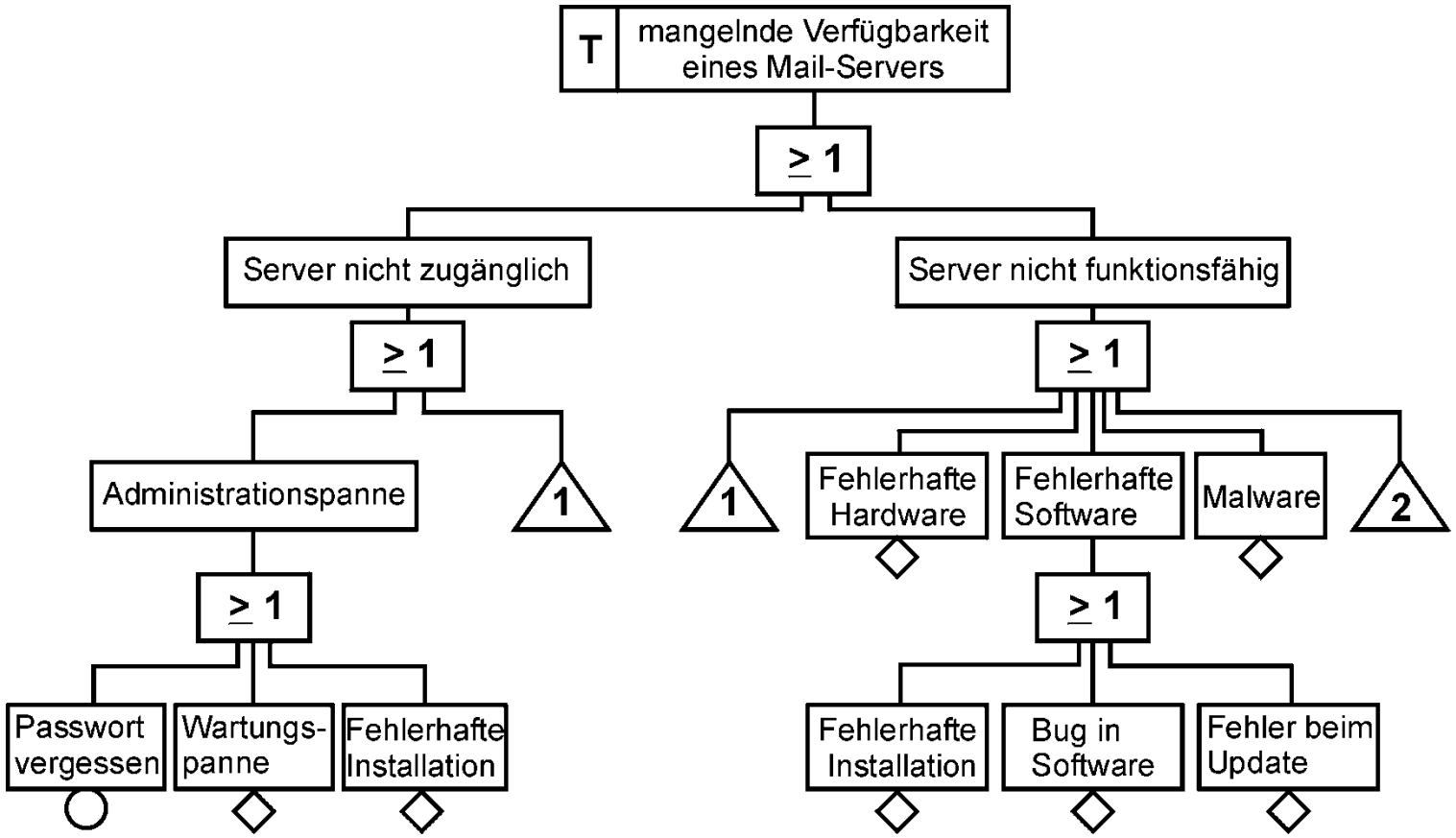
- Die Server sollen auf gehärteten Systemen betrieben werden, indem alle nicht notwendigen Dienste entfernt werden.
- Auf jedem Server soll ein Virenschutz implementiert sein (durch die bereits erfolgte Schutzzoneneinführung greift das bereits voll).

5.2 Fehlerbaum

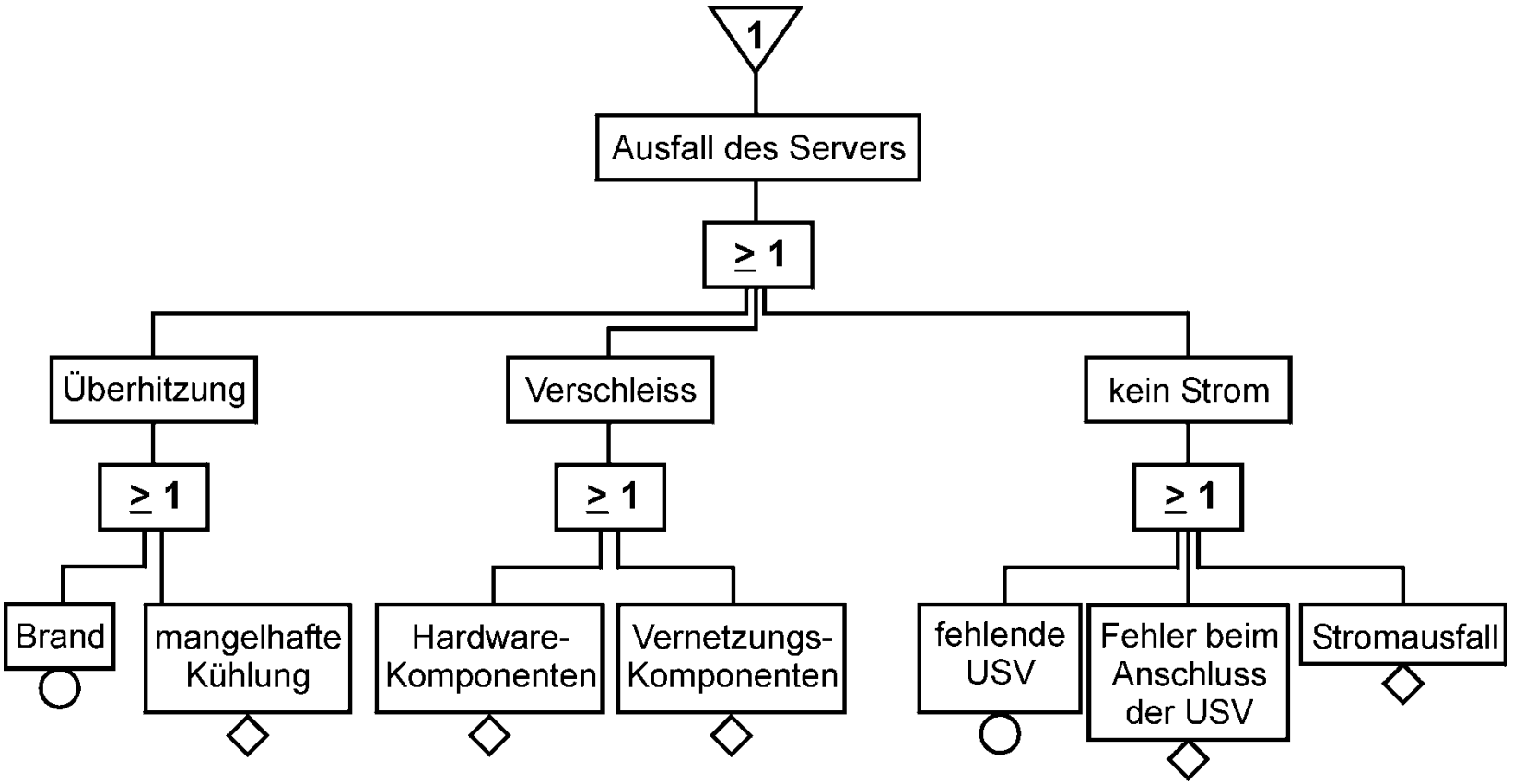
Aufgabe:

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

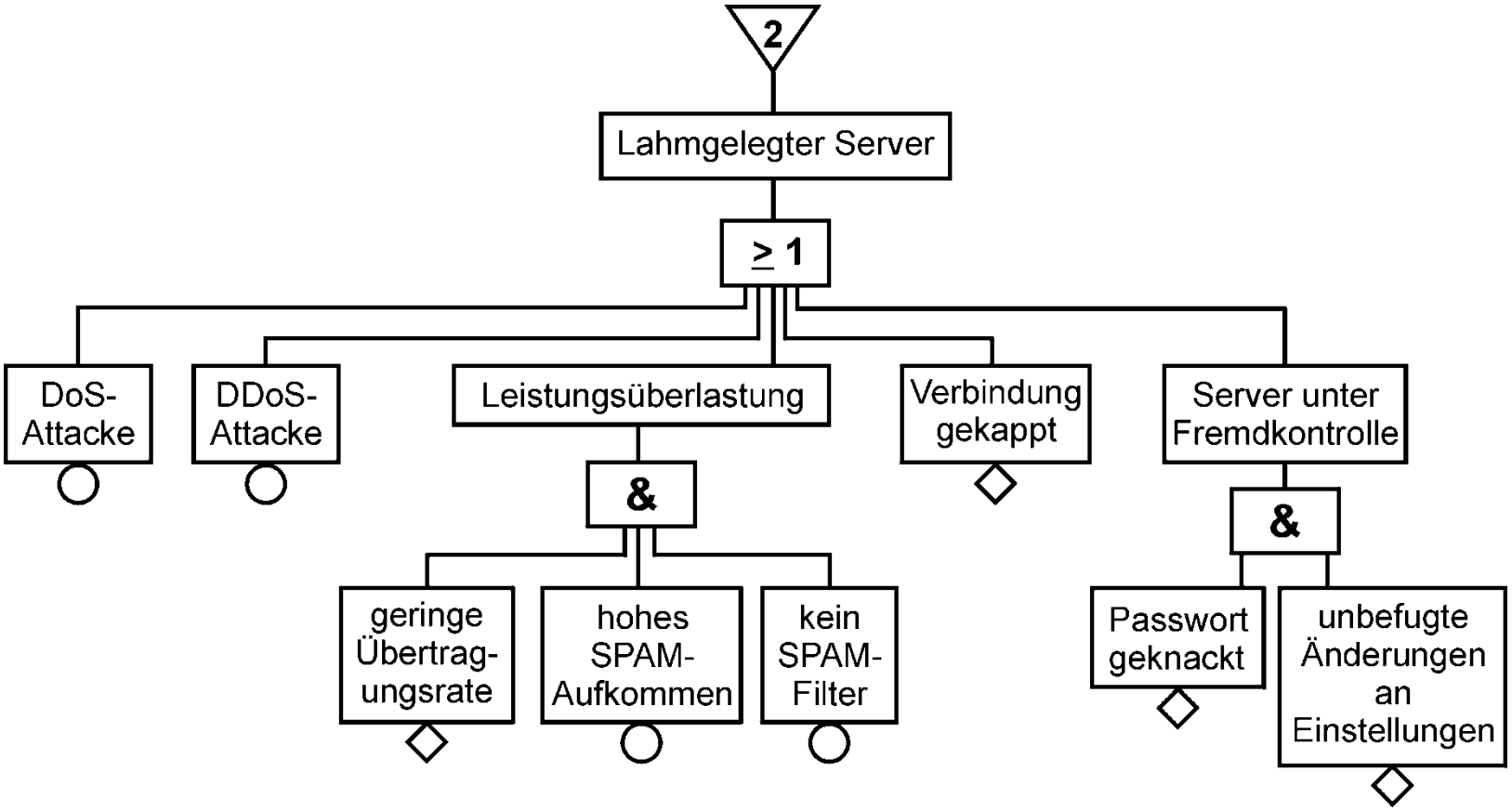
5.2 Fehlerbaum (1)



5.2 Fehlerbaum (2)



5.2 Fehlerbaum (3)



5.2 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:

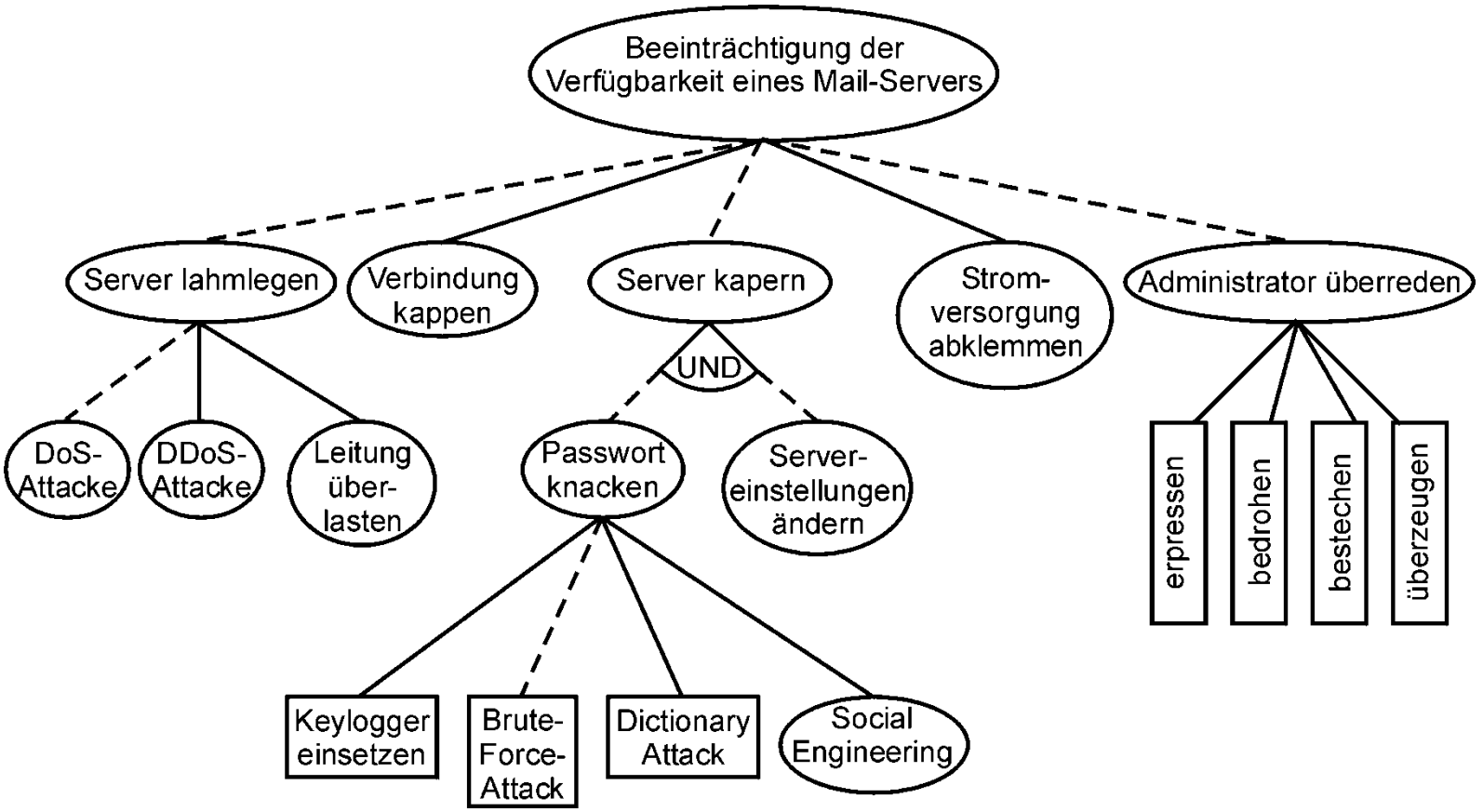
- lahmgelegter Server aufgrund
  - DoS-Attacke
  - DDoS-Attacke
  - Leitungsüberlastung
  - gekappten Verbindungen
  - Server unter Fremd-kontrolle
- Malware

5.3 Angriffsbaum

Aufgabe:

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

5.3 Angriffsbaum



5.4 Fehlerbaum vs. Angriffsbaum

Aufgabe:

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

5.4 Fehlerbaum vs. Angriffsbaum (1)

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

5.4 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

5.4 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
- Unzureichender Schutz gegen Malware und informationstechnische Angriffe
  → geeignete Gegenmaßnahmen ergreifen (Virenscanner, Intrusion Detection System, Penetrationstests, need-to-know-Prinzip bei Rechtevergabe, komplexe Passwörter, ...)

5.4 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 ;-)

5.5 Authentizität vs. Integrität

Aufgabe:

- Beschreiben Sie drei Vorgänge (z.B. Angriffsvektoren oder Schutzvorkehrungen), bei denen **Authentizität** (im Sinne von Zurechenbarkeit) als relevantes Sicherheitsziel betroffen ist, **nicht** jedoch **Integrität**! Begründen Sie dies.

5.5 Authentizität vs. Integrität (1)

- Bei der Authentizität (im Sinne von Zurechenbarkeit) ist maßgeblich, dass der Auslöser eines Prozesses feststellbar ist, bei Integrität dagegen, dass Veränderungen nur durch Befugte erfolgen (siehe Begriffsdefinition aus der Vorlesung)
  - Beim zugrunde liegenden Prozess ist es soweit unerheblich, ob eine Veränderung durchgeführt worden ist, so lange eindeutig der Verursacher feststellbar ist (→ **Authentizität = Vertrauenswürdigkeit des Auslösers**)
  - Bei der Integrität dagegen wird nur darauf geachtet, ob die Veränderung durch einen Befugten durchgeführt worden ist (→ **Integrität = Vertrauenswürdigkeit des Datenbestandes bzw. Systemzustandes**)
  - **Die Zurechenbarkeit unterstützt bei der Vertrauenswürdigkeit des Datenbestandes bzw. Systemzustandes also die Integrität, ohne selbst Bestandteil der Integrität zu sein**
  - Eine Veränderung, die nachweislich auf die Aktivität eines Unbefugten zurückzuführen ist, widerspricht jedoch nicht der Authentizität

→ Beispiel Angriffsvektor: Bei einem Ransomware-Angriff offenbart i.d.R. die auslösende Mail bei genauerer Analyse, dass diese Mail faktisch von einem Dritten stammt, die Integrität der Mail ist dabei hingegen gar nicht verletzt worden, nur der Anschein, von wem die Mail stammt (außer Mailkonto wurde durch Angreifer gekapert, so dass Headerdaten korrekt zu sein scheinen)

5.5 Authentizität vs. Integrität (2)

- **Authentizität** wird in digitaler Datenverarbeitung vor allem **mittels digitaler Signaturen** nachgewiesen, während **Integrität im Sinne digitaler Siegel** bestätigt, dass Daten nicht verfälscht worden sind
  - Digitale Siegel werden dabei i.d.R. automatisiert erzeugt und zeigen z.B. durch Hashwert nach Erzeugung des Datenbestandes an, ob der zugrunde liegende Datensatz noch originalgetreu ist
  - Digitale Signaturen dagegen benötigen i.d.R. eine Aktivität durch einen Menschen, wodurch die Echtheit des Absenders nachgewiesen wird (entsprechende Mechanismen sind derzeit daher bewusst so konstruiert, dass KI diese Aktivität nicht präzise genug nachbilden kann)

→ Beispiel Schutzvorkehrung: **symmetrische Authentication weist Integrität** der Daten **nach**, **während asymmetrische Authentication neben der Integrität auch die Zurechenbarkeit nachweist**, da der zugehörige Schlüssel unter alleiniger Kontrolle des Schlüsselinhabers stehen muss, was weder bei symmetrischer Authentication noch bei maschinell erzeugten digitalen Siegeln der Fall ist (siehe auch zugehörige Ausführung in der Vorlesung)

5.5 Authentizität vs. Integrität (3)

- Der Nachweis von Integrität kann z.B. durch Mechanismen wie Speicherung auf WORM-Medien oder durch unverfälschte Protokollierung von Änderungsaktivitäten erfolgen, während die Überprüfung der Identität eines Ändernden mittels Authentifizierungsmechanismen wie Multi-Faktor-Authentifizierung nachgewiesen werden kann

→ Beispiel Schutzvorkehrung: Durch **Einsatz von Multi-Faktor-Authentifizierung** wird **neben der Zurechenbarkeit auch die Vertraulichkeit der Daten sichergestellt**, da sowohl der Nachweis der Identität des Zugreifenden durch den Einsatz des zweiten Faktors bestätigt wird als auch damit sichergestellt ist, dass nur ein Befugter betreffende Daten interpretieren kann, was folglich überhaupt nicht die Integrität der Daten betrifft, sondern nur den Zugang bzw. Zugriff auf diese Daten (Voraussetzung für Auslesen als auch Abänderung oder Löschung von Daten); damit Authentizität grundlegender als Integrität, d.h. **Integrität kann auf Basis von Authentizität nachgewiesen werden, nicht aber Authentizität auf Basis von Integrität**

Hilfreiche Sammlung zur Begriffsklärung (im Rahmen von NIST-Standards):

- https://csrc.nist.gov/glossary/term/authentication
- https://csrc.nist.gov/glossary/term/integrity