Grundlagen des Datenschutzes und der IT-Sicherheit

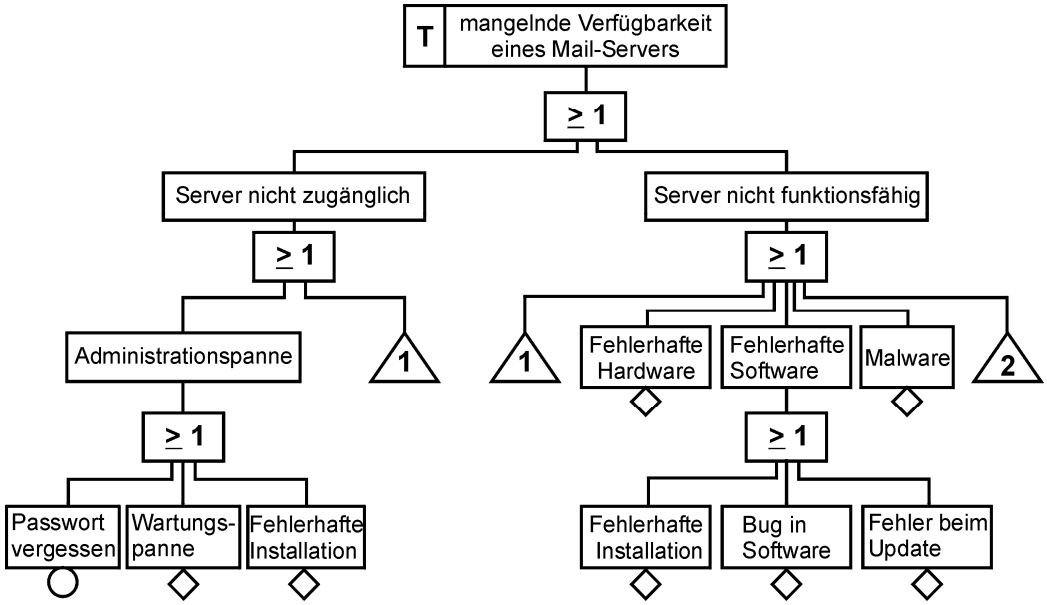
Musterlösung zur 7. Übung im SoSe 2009:
Vergleich Fehlerbaum und Angriffsbaum

7.1 Fehlerbaum

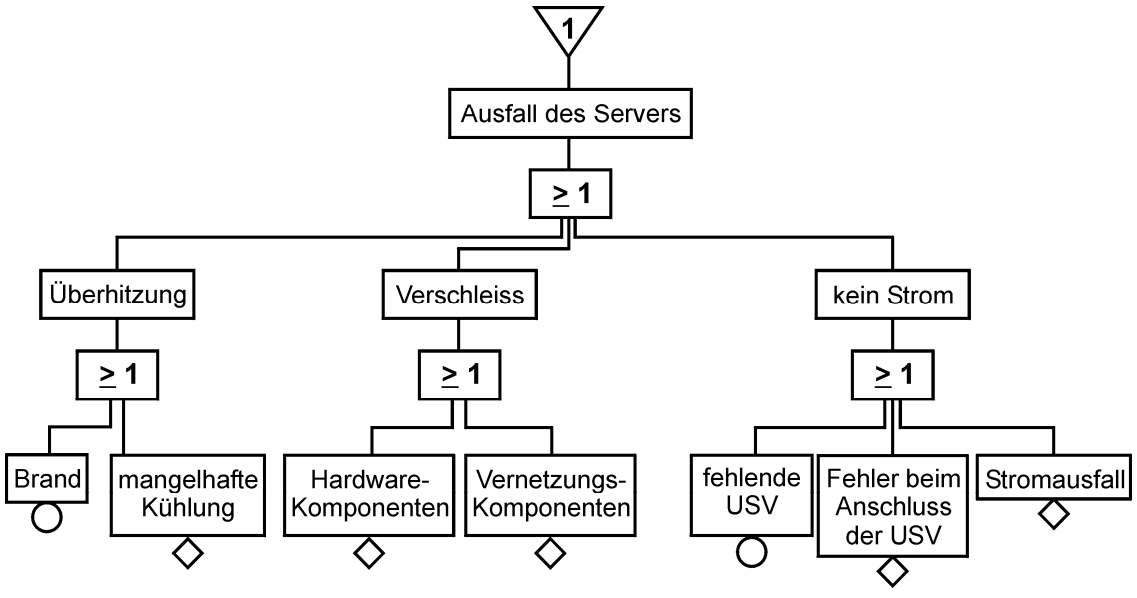
Aufgabe:

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

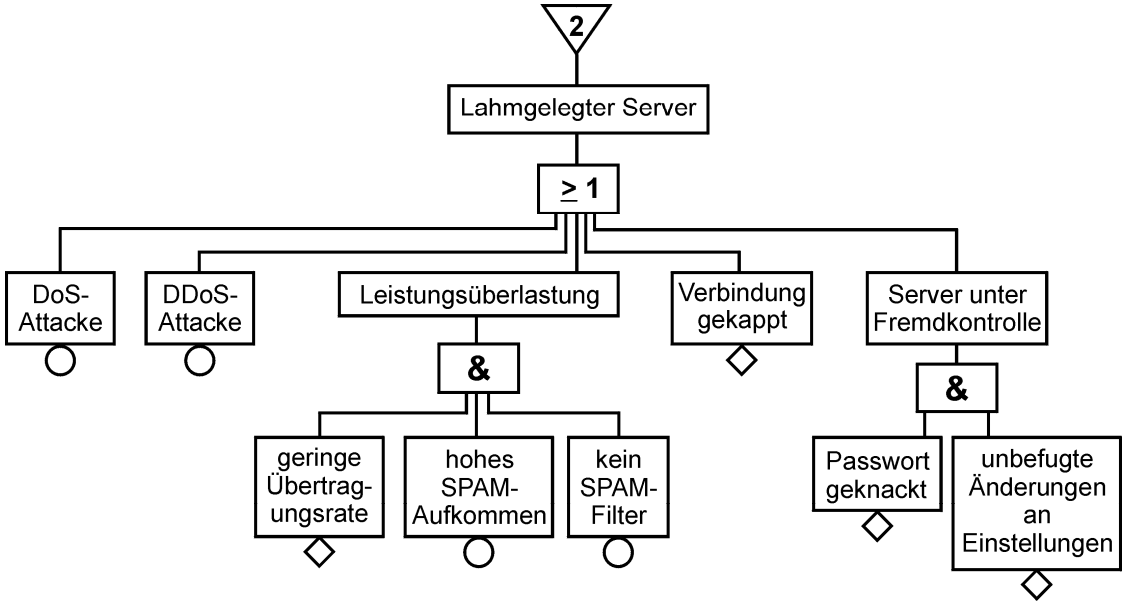
7.1 Fehlerbaum (1)



7.1 Fehlerbaum (2)



7.1 Fehlerbaum (3)



7.2 Analyse des Fehlerbaums: Safety & Security

Aufgabe:

- Welche Gründe (Basisereignisse) sind der Safety zuzuordnen und welche der Security?

7.2 Analyse des Fehlerbaums

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:

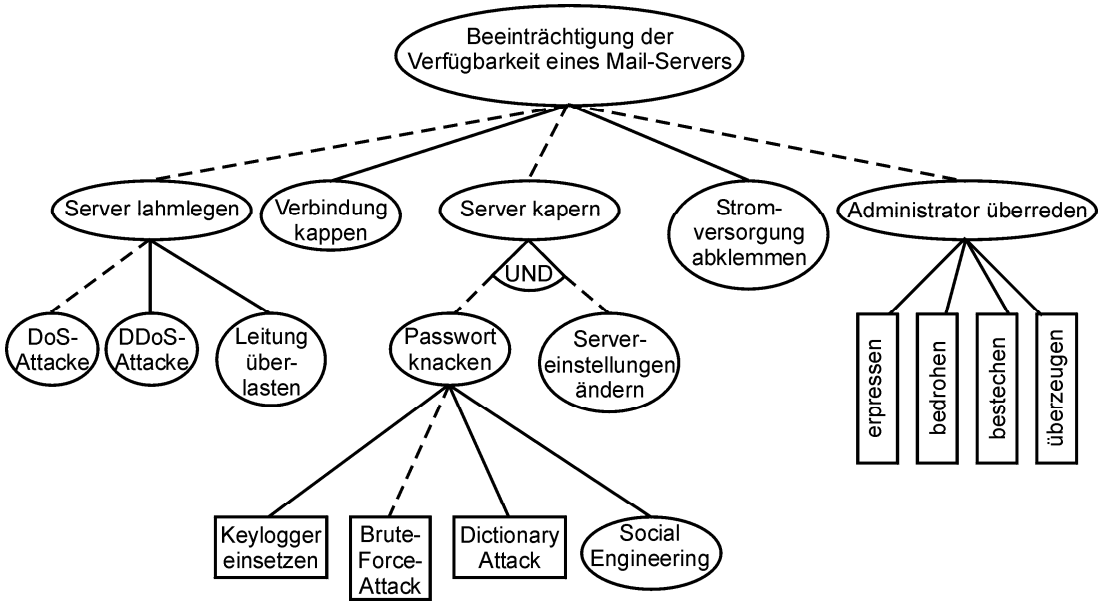
- lahmgelegter Server aufgrund
  - DoS-Attacke
  - DDoS-Attacke
  - Leitungsüberlastung
  - gekappten Verbindungen
  - Server unter Fremd-kontrolle
- Malware

7.3 Angriffsbaum

Aufgabe:

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

7.3 Angriffsbaum



7.4 Fehlerbaum vs. Angriffsbaum

Aufgabe:

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

7.4 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

7.4 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

7.4 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

7.5 Konsequenzen aus Schwachstellenanalysen

Aufgabe:

- Welche Schwachstellen (Vulnerabilities) konnten Sie anhand der beiden Analyse-Methoden feststellen? Welche Konsequenzen würden Sie als IT-Leiter daraus ziehen?

7.5 Konsequenzen aus Schwachstellenanalysen (1)

- 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

7.5 Konsequenzen aus Schwachstellenanalysen (2)

- Bedrohungen durch Malware und informations-technischen Angriffen
  → geeignete Gegenmaßnahmen ergreifen (Virenscanner, Intrusion Detection System, Penetrationstests, need-to-know-Prinzip bei Rechtevergabe, komplexe Passwörter, ...)
- Softwarefehler reduzieren
  → eingesetzte Software umfassend testen, nur von vertrauenswürdigen Stellen beziehen und aufgrund von Zertifikaten einsetzen

7.5 Konsequenzen aus Schwachstellenanalysen (3)

- Mitarbeiterattacken vermeiden
  → Mitarbeiter schulen und durch leistungsgerechte Bezahlung und guter Atmosphäre motivieren ;-)