- **c. Softwareanwendungen**
- **d. Zusammenfassung**

3. Exkurs: Virtualisierung

4. Netzwerke und Netzwerktechnik

5. Spezielle Netzwerktechnologien

- **a. WWW – Webseiten, Webanwendungen**
- **b. E-Mail, *instant messaging, chat***
- **c. DNS**
- **d. *cloud computing***

6. Datensicherheit als technische Zuverlässigkeit

7. Exkurs 2: Künstliche Intelligenz und *machine learning*

F. Angriff - Hacker als Gegner

1. Angriffsziele

2. Angriffsvektoren / Wege und Verfahren der Angriffe

3. Angriffsarten, Werkzeuge und Probleme im Detail

- **a. Buffer overflow**
- **b. Virus**
- **c. Computerwurm**
- **d. Trojaner**
- **e. Bot-Netz**
- **f. SPAM**
- **g. Meltdown / Spectre**

4. Risikosphäre Internet

a. Angriffsansätze in den Internetprotokollen

b. Probleme der Netzdienste

c. WWW: HTTP als verbindungsloses Protokoll

d. OWASP TOP 10

5. Spezielle Problemkategorie: mobile computing

6. Rechtsrahmen

G. Umgang mit Datensicherheit

1. Grundlagen des *security engineering* bzw. des Sicherheitsmanagements

a. Sicherheitsprozess - kontinuierliche Verbesserung

b. Konstruktion sicherer Systeme aus technischer Sicht

c. Vorgehensweise - die wichtigsten Schritte

- Erfassung relevanter Systemeigenschaften
- Ermittlung des Schutzbedarfs
- Erfassung der Bedrohungen
- Schaffung von Sicherheitsstrategien und Sicherheitsarchitektur

d. Rolle der Dokumentation

- Sicherheitsleitlinie
- Geschäftsprozesse,
- Sicherheitskonzepte (ISO 27001 / IT-Grundschutz des BSI)
- spezielle Sicherheitsrichtlinien
- Arbeitsanweisungen (mit Checklisten?)
- Inventarisierungsdaten

2. Maßnahmen

a. Systematik

- Verträge und andere rechtliche Regelungen
- Organisation
- Personal
- Infrastruktur
- Technik