# Klausurfragen (Beispiele)

Skript Abschnitt 2 Allgemein: Definition IT-Sicherheit, was ist das, welche Teilbereiche gibt es, Beispiele?

Was bedeutet der „Kostenfaktor“ IT-Sicherheit in Bezug auf den Business Value of IT?

Z.B. „Was versteht man unter ‚Vertraulichkeit der Daten‘? Nennen Sie ein Beispiel, in dem die Vertraulichkeit verletzt wird. (Je 1-2 Punkte, nach Schwierigkeit der Frage)

Abschnitt 3 (Verschlüsselung):

Welche Arten von Verschlüsselung gibt es? Wie unterscheiden sich diese bzw. wo sind die kritischen Stellen der jeweiligen Verschlüsselungsart?

Wie funktioniert eine elektronische Unterschrift?

Authentifizierung per SSL, wie geht das?

Datenträger-Sicherheit, welche Maßnahmen können der Vertraulichkeit und Authentizität dienen?

Abschnitt 4 (Sicherheit im Netzwerk)

Welche Gefahren sind bei vernetzten Systemen besonders evident?

Wie erkennt man Schwachstellen (hierzu gibt es ggf. Beispiele, die Sie erklären sollen), wie kann man z.B. bei einem offenen Router-Port für Abhilfe sorgen? Wie kann man inhärent unsichere Systeme im Netz schützen? (Stichwort BYOD)

Angriffswerkzeuge/Diagnosewerkzeuge kennen, Warnungen auswerten und Abhilfemaßnahmen ergreifen können (Beispiele…)

Was ist Schadsoftware, und über welche Wege gelangt sie über das Netzwerk in ein System?

Z.B.: Bei einem System-Upgrade meldet das System „nicht signiertes Paket. Trotzdem installieren?“ Was bedeutet dies, was könnte passieren, wenn man einfach auf „Weiter“ klickt?

Normen und Zertifizierungen zu IT-Sicherheit benennen können (zusammenfassend, was drin steht, nicht im Detail), z.B. „Grundschutzhandbuch“ (BSI), ISO2700x.

Wozu dient ein SSL-Zertifikat, wer erzeugt und wer „zertifiziert“ es? Was bedeutet „selbstsigniertes Zertifikat“?

Verschlüsselungs-Standards, die als sicher gelten (z.B. AES, was hat das mit „Open Source“ zu tun?).

Daten-Forensik: Auf „gelöschte“ Daten zugreifen, Daten ausspähen, wie kann dies verhindert werden?

Nennen Sie eine Software, mit der architekturunabhängig Festplatten verschlüsselt werden können.

Netzwerk: TCP-IP: Wie funktioniert die Kommunikation zwischen Rechnern im Internet (Schichtenmodell), wo liegen hier die Angriffsvektoren? Stichwort Arp-Poisoning, was macht das?

Portscanner, Sniffer, Diagnosetools und interaktive Programme für Einbruchsversuche.

„Man in the Middle“ erklären.

Cross Site Skripting: Wer wird hierbei angegriffen, wer kann oder muss Schutzmaßnahmen ergreifen?

SPAM-Filter: Was kann ein Mailfilter, was kann schief gehen, Verbesserungsvorschlag für eine „schlechte“ Konfiguration (Mailserver als Spamschleuder).

Netzneutralität!