

Aufgabe 2:

Konzeption sicherer Software

Die Entwicklung von Anwendungs-Software ist schwer. Wesentlich schwerer ist es, gute Software zu entwickeln. Wie kompliziert ist es dann erst, sichere und gute Software zu entwickeln? Ihre Aufgabe ist es, herauszufinden, ob es grundsätzliche Verfahren zur Konzeption sicherer Software gibt.

Klären sie u.a. die folgenden Fragen:

- Wie wird bei der Software-Konzeption bzw. im Software-Engineering vorgegangen?
- An welchen Stellen müssen sie Sicherheitsbetrachtungen in den Engineering-Prozess einfließen lassen?
- Produktzertifizierungen nach den *Common Criteria* erfordern beispielsweise eine „methodische Entwicklung“, einen „semiformalen Entwurf“ oder gar einen „formal verifizierten Entwurf“ von Software. Was verbirgt sich dahinter?
- Mit welchen Methoden können diese Sicherheitsstufen *EAL 4* bis *EAL 7* der *Common Criteria* erreicht werden, was sagt das letztlich über die Funktionssicherheit und die Informationssicherheit einer Software aus?