Reaktive Sicherheit

Übungsblatt 1

Jakob Kretz, Bünyamin Sarikaya, Balduin Binder

Aufgabe 1

Aufgabe 1.1

Claudia Eckert benutzt bei ihrer Defintion den Begriff eines *Funktionssicheren* Systems, der jedoch nicht weiter erläutert wird. Das BSI hingegen definiert die Sicherheit eines Systems so, dass die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, welche die wesentlichen Schutzziele der IT-Sicherheit sind, gewahrt werden. In der Definition von Klaudia Eckert wird nicht konkret auf Schutzziele eingegangen. Man könnte die Definition von Klaudia Eckert als abgeschwächte Beschreibungen der beiden Schutzziele Integrität und Vertraulichkeit ansehen, jedoch ist diese in ihrer Formulierung zu ungenau. Das BSI definiert die IT-Sicherheit außerdem weitreichender und spricht von *Informationssicherheit*. Hierbei geht es primär um die Sicherheit einer Information und den Schutz (bezüglich der zuvor genannten Schutzziele) einer Information und nicht nur die eines Systems.

Aufgabe 1.2

- **Integrität:** Alice signiert ihre Emails an Bob mit ihrem geheimen Schlüssel, somit kann Bob sich sicher sein, dass die Email wirklich von Alice stammt.
- **Verfügbarkeit:** Alice macht immer Backups von ihren Daten, somit kann sie sich sicher sein, dass ihre Daten verfügbar sind, falls ihr Computer mal crashen sollte.
- **Authentizität:** Alice signiert ihre Email an Bob mit ihrem geheimen Schlüssel, somit kann Bob überprüfen ob Alice die Email geschrieben hat. Die Email stammt also nachweislich von Alice, somit ist das Schutzziel der Authentizität gewährleistet.
- **Zurechenbarkeit:** In einem Online-Forum X müssen sich alle Teilnehmer mit ihrem Ausweis registrieren und dürfen keine Nick-Names benutzen. Jeder kann nun jeden Post in diesem Forum eindeutig einer Person zuordnen, somit ist das Schutzziel der Zurechenbarkeit gewährleistet.