# Kompetenzraster

| Kompetenzband: | HZ | Grundkompetenz | Fortgeschrittene-Kompetenz | Erweiterte-Kompetenz |
|---|---|---|---|---|
| A - Sicherheits-schwachstellen und Massnahmen verstehen | 1, 2 | A1G: Ich kann erklären, was eine Sicherheitsschwachstelle bei einer Applikation ist. | A1F: Ich kann aktuelle Sicherheitsschwachstellen, deren Ursachen und Folgen erklären.<br/>(z.B. OWASP Top ten „description“) | A1E: Ich kann Informationsquellen zu Sicherheitsschwachstellen in Bezug auf ihre Relevanz beurteilen. |
| | 1, 2 | A2G: Ich kann erklären, was in Bezug auf eine Sicherheitsschwachstelle unternommen werden muss. (z.B. Sicherheitsschwachstelle identifizieren, Gegenmassnahmen definieren und umsetzen, Wirkung überprüfen) | A2F: Ich kann Massnahmen gegen aktuelle Sicherheitsschwachstellen erklären.<br/>(z.B. OWASP Top ten „how to prevent“) | A2E: Ich kann praktische Beispiele von Sicherheitsschwachstellen und Gegenmassnahmen vorführen. (z.B. Beispiel recherchieren, nachvollziehen, praktisch vorführen. z.B. WebGoat) |
| B - Authentisierungs-verfahren einsetzen | 3 | B1G: Ich kann die Funktionsweise von verschiedenen Authentisierungsverfahren erklären. | B1F: Ich kann Authentisierungsverfahren in einer Applikation umsetzen. | B1E: Ich kann das für einen Use-Case geeignete Authentisierungsverfahren gegenüberstellen und begründet auswählen. |
| C - Logging und Monitoring-Mechanismen implementieren | 5 | C1G: Ich kann die relevanten Informationen für das Monitoring und Logging sammeln. | C1F: Ich kann gesammelten Informationen für das Monitoring und Logging auswerten und relevante Informationen bestimmen. | C1E: Ich kann Monitoring- und Logging-Systeme einrichten, überwachen und Informationen zur Behebung von Sicherheitsproblemen verwenden. |
| | | C2G: Ich kann den Aufbau und Inhalt von Logs und Audit-Trails erkennen und erklären. | C2F: Ich kann aufgrund des Aufbaus und Inhalts von Logs und Audit-Trails einzelne Massnahmen zur Behebung von möglichen Sicherheitsproblemen vorschlagen. | C2E: Ich kann zu Logs und Audit-Trails situativ verschiedene Formen der Alarmierung und Alarmauslösung umsetzen. |
| D - Kryptographie | 2, 3, 4 | D1G: Ich kann Kryptographie Verfahren wie Symmetrische- und Asymmetrische Verschlüsselungen sowie Hash-Funktionen einer Anwendung zuweisen und einordnen. | D1F: Kann symmetrische und asymmetrische Verschlüsselung sowie Hash-Funktionen in der Applikation zum Schutz sensibler Daten einsetzen. | D1E: Kann in einer Applikation eingesetzte kryptographische Massnahmen auf deren Tauglichkeit beurteilen sowie Verbesserungsvorschläge anbringen und umsetzen. |
| E - Sicherheitslücken vermeiden und beheben | 4, 1, 3 | E1G: Ich kann die Sicherheitsrisiken in der Entwicklung von Anwendungen auflisten und erklären. | E1F: Ich kann die Sicherheitsrisiken in der Entwicklung von Anwendungen erkennen und bei der Implementierung vermeiden. | E1E: Ich kann Sicherheitsarchitekturen beim Design von Anwendungen berücksichtigen. |
| | | E2G: Ich kann Massnahmen beschreiben, die Sicherheitslücken in Applikationen beheben. | E2F: Ich kann Massnahmen umsetzen, die Sicherheitslücken in Applikationen beheben. | E2E: Ich kann Massnahmen vergleichen und umsetzen, die die Sicherheit von Systemen und Netzwerken optimieren. |