1. Elemente bzw. Stadien der „vollständigen Handlung“ kennen und anordnen können.
2. Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität (und Authentizität) definieren können und deren Beeinträchtigung in realen Schadensszenarien erkennen und zuordnen können.
3. Grundaufbau eines BSI-Bausteins kennen.
4. Genaue Bedeutung der Modalverben „Muss“, „Darf“ und „Sollte“ auch in Kombination mit „Nicht“ kennen und definieren können.
5. Sicherheits-Anforderungs-Niveaus nach BSI-Definition kennen und zueinander in Beziehung setzen können.
6. Kriterien für die Bewertung der Eignung von Verschlüsselungssoftware verstehen und ihre Bedeutung für die Szenarien „Einzelverschlüsselung von Dateien“ oder „Anlegen eines Tresors/Safes“ beurteilen können.
7. Prinzip der Berechnung von Hash-Werten kennen.
8. Grundprinzip der symmetrischen und der asymmetrischen Verschlüsselung kennen.
9. Arten von Cyberangriffen definieren und konkreten Angriffsszenarien zuordnen können: Pishing, Malware, Ransomware, DoS.
10. Gefährdungen aus dem BSI-Katalog den Kategorien „Schaden“ oder „Einfallstor“ zuordnen können.
11. Vom BSI empfohlene Erste-Hilfe-Maßnahmen nach Eintreten eines Sicherheitsvorfalls kennen und ihre Sinnhaftigkeit einordnen und begründen können.
12. Die Anzahl der Kombinationsmöglichkeiten zur Bildung eines Passworts in Abhängigkeit von der Anzahl der möglichen Zeichen und der Anzahl der Stellen berechnen können.