Lernfeld 4 – Schutzbedarfsanalyse im eigenen Arbeitsbereich durchführen

Lernsituation 4.1 – Schutzbedarfsanalyse für den eigenen IT Arbeitsplatz durchführen

Die Lernenden können…

- die Bedeutung von Datenschutz und Informationssicherheit erläutern.
- rechtliche Regelungen des Datenschutzes wiedergeben.
- betriebliche Vorgaben einer IT-Sicherheitsleitlinie im Hinblick auf die Informationssicherheit bewerten.
- eine Strukturanalyse zur Ermittlung des Schutzbedarfs für einen eingegrenzten Bereich durchführen.
- den Schutzbedarf von Geschäftsprozessen im Hinblick auf die Schutzziele der Informationssicherheit begründen.
- allgemeine Bedrohungen bei Geschäftsprozessen benennen und konkrete Schwachstellen von IT-Systemen identifizieren.
- Schadenspotenziale (direkt oder indirekt) von IT-Sicherheitsvorfällen kriteriengeleitet bewerten.
- eine qualitative Risikoanalyse gemäß BSI 200-3 durchführen und in einem Risikographen darstellen.
- unter Verwendung der IT-Grundschutzkatalogs technische, organisatorische, personelle und infrastrukturelle Maßnahmen zur Steigerung der Informationssicherheit empfehlen.

Lernsituation 4.2 – arbeitsplatzbezogenes Sicherheitskonzept entwickeln

Die Lernenden können…

- typische Angriffsvektoren für den eigenen Arbeitsbereich beschreiben.
- die Bedeutung von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit erläutern.
- Bedrohungen und Schwachstellen im Bezug auf Sensibilisierung zur Informationssicherheit unter Verwendung des IT-Grundschutzbausteins ORP.3 erläutern.
- Erfolgskriterien für zielgerichtete Awareness Schulung formulieren.
- ein Konzept für eine Awareness-Schulung erarbeiten und präsentieren.
- mithilfe eines Hypervisors eine virtuelle Arbeitsumgebung zur Demonstration eines gewählten Angriffsvektors einrichten.
- die Notwendigkeit von komplexen Passwörtern und sicheren Authentifizierungsmethoden mithilfe eines offline Passwortangriffs verdeutlichen.
- mithilfe des Tools Gophish eine Phishing-Kampagne entwerfen und durchführen.
- ein IT-System auf vorhandene Softwareschwachstellen in Diensten analysieren und die Schwachstelle mithilfe eines bekannten Exploits ausnutzen.