Modulidentifikation

Modulnummer	114	
Titel	Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzen	
Kompetenz	Codierungs-, Kompressions- und Verschlüsselungsverfahren im täglichen Berufsalltag korrekt einsetzten.	
Handlungsziele	1	Codierungen von Daten situationsbezogen auswählen und einsetzen. Aufzeigen, welche Auswirkung die Codierung auf die Darstellung von Daten hat.
	2	Kompressionsverfahren gemäss Vorgaben für die Aufbewahrung, Wiederherstellung und Übertragung von Daten auswählen und einsetzen.
	3	Verschlüsselungsverfahren zur Sicherung von Daten gemäss Vorgaben gegen unbefugten Zugriff auf Datenspeicher und Übertragungswegen auswählen und einsetzen.
	4	Gesicherte Übertragungsverfahren für Dateien mit asymmetrischen und symmetrischen Verschlüsselungsverfahren nutzen. Dabei Aspekte wie Public/Private Key, Zertifikate, Protokolle und Standards berücksichtigen.
	5	Verschiedene Verschlüsselungstechnologien hinsichtlich Aktualität, Verbreitung und Sicherheit bewerten. Schwachstellen erkennen und Vorschläge für alternative Technologien machen.
Kompetenzfeld	Security/Risk Management	
Objekt	Zu speichernde und zu übertragende Daten in einem Unternehmen.	
Modulversion	4.0	
Erstellt am	19.03.2021	

Handlungsnotwendige Kenntnisse

Handlungsnotwendige Kenntnisse beschreiben Wissen, das die kompetente Ausführung der Handlungen eines Moduls unterstützt. Diese Kenntnisse dienen der Orientierung und sind nicht abschliessend definiert. Die daraus folgende Konkretisierung der Lernziele und das Festlegen des Lernwegs für den Kompetenzerwerb sind Sache der Bildungsanbieter.

Modulnummer		114
Titel		Codierungs-, Kompressions- und Verschlüsselungsverfahren einsetzen
Kompetenz		Codierungs-, Kompressions- und Verschlüsselungsverfahren im täglichen Berufsalltag korrekt einsetzten.
Handlungsziele und handlungsnotwendige Kenntnisse		
1	1.1	Kennt die wichtigsten Typen von Binärcodes (z.B. ASCII, ANSI-, BCD-, EAN-,1-aus -n-, UTF, Uni-Code) und kann anhand ihrer Merkmale (Zeichenvorrat, Redundanz) aufzeigen, wie sich diese hinsichtlich der Bewertbarkeit, Fehlererkennbarkeit und Rechenfähigkeit unterscheiden.
	1.2	Kennt die wichtigsten Eigenschaften von Bildern (z. B S/W Strichzeichnung, Farbfoto, bewegte/nicht bewegte Bilder, vektorisiert/pixelorientiert usw.) und kann erläutern, wie damit die Bildqualität (z. B Auflösung, Farbtiefe), der Bildaufbau und der Speicherbedarf beeinflusst werden kann, wie auch Sicherheitslücken bezüglich Metadaten aufzeigen.
	1.3	Kennt binäre, oktale und hexadezimale Zahlensysteme, logische Operationen (OR, AND, NOT) und weiss wie diese in der IT eingesetzt inkl. deren Umrechnung in andere Zahlen-systeme werden (z. B Unix-Dateirechte, IP-Adressen, Farben-RGB usw.).
	1.4	Kennt Verfahren zur binären Kodierung von Zahlen (z. B negative Zahlen/Zweierkomplement, Gleitkommazahlen, Exzess).
2	2.1	Kennt Merkmale (z. B Kompressionsrate, Qualitätsverlust) für gängige verlustlose und verlustbehaftetet Kompressionsverfahren und an welchen Stellen, welches sinnvoll eingesetzt wird.
	2.2	Kennt ausgewählte Normen und Standards (z. B. JPEG, PNG, MPEG, H261/263, Huffmann-Verfahren) und kennt typische Anwendungsbereiche wo diese eingesetzt werden, wie auch die Berücksichtigung von mehrfach komprimierten Dateien (z. B JPEG in einem *.Zip) und deren nachteilige Folgen.
3	3.1	Kennt das grundsätzliche Prinzip der Verschlüsselung von Informationen (z. B Kryptografie/Steganografie) und kann anhand eines einfachen Verschlüsselungskonzepts aufzeigen, wie damit Informationen chiffriert und dechiffriert werden können.
	3.2	Kennt mögliche aktuelle oder zukünftige Applikationen, welche für die Verschlüsselung von Daten (z. B. PGP, Keypass) eingesetzt werden können und an welchen Stellen diese Applikationen sinnvoll sind.
	3.3	Kennt die Konfiguration der Verschlüsselungsapplikationen und kann diese gemäss Firmenvorgabe oder Anleitung korrekt in Betreib nehmen.
4	4.1	Kennt die prinzipiellen Unterschiede zwischen einer symmetrischen und asymmetrischen Verschlüsselung (z. B Passwörter, private und öffentliche

Handlungsnotwendige Kenntnisse

		Schlüssel) und kann erläutern, wie sich diese auf den Grad der Datensicherheit auswirken.
	4.2	Kennt das Prinzip elektronischer Signatursysteme und kann anhand von Beispielen aufzeigen, wie damit die Sicherheit (z. B Authentizität, Integrität) der Übermittlung gewährleistet werden kann, wie auch an welchen Stellen heute und in Zukunft diese eingesetzt werden können.
	4.3	Kennt den Zweck digitaler Zertifikate und kann an Beispielen erläutern, wie damit das Vertrauen zwischen Anbieter und Bezüger (einer Leistung, eines Produktes) sichergestellt werden kann.
5	5.1	Kennt mögliche IT bezogene Stellen, wie API-Schnittstellen, Versenden von E-Mails, wie diese bei der Übertragung von Daten verschlüsselt werden sollten und welche minimale Datenverschlüsselung bei der Übertragung gemäss Gesetz verwendet werden muss (z. B Bit-Länge der Verschlüsselung).
	5.2	Kennt mögliche Schwachstellen der Verschlüsselungsverfahren bei Datenverschlüsselung oder Datenübertragung und kann diese aufzeigen.

Modulversion	4.0
Erstellt am	19.03.2021