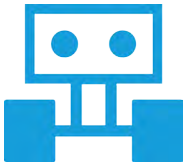
ICDL
The Digital Skills Standard

OESTERREICHISCHE COMPUTER GESELLSCHAFT ®
AUSTRIAN COMPUTER SOCIETY

ICDL Workforce

TECHNICIAN BASIC



Lernzielkatalog

www.ocg.at

Zweck dieses Dokuments

Dieses Dokument listet die Lerninhalte für das ECDL/ICDL Package ***Technician Basic*** auf und beschreibt, welche Fertigkeiten von den Absolvent*innen des Moduls erwartet werden. Die theoretischen und praktischen Aufgaben der Tests zu diesem Modul beruhen auf den Inhalten dieses Lernzielkatalogs. Appobierte Lernmaterialien decken dessen Inhalte ab.

Der ECDL/ICDL ist eine Initiative der ICDL Foundation und wird in Österreich von der OCG betreut.

ICDL Foundation

The Grange
Stillorgan Road
Blackrock
Co. Dublin
Republic of Ireland
Web: www.icdl.org

Österreichische Computer Gesellschaft (OCG)

Wollzeile 1
A-1010 Wien
Tel: +43 1 512 02 35-0
E-Mail: info@ocg.at
Web: www.ocg.at

Hinweis

Die aktuelle deutschsprachige Version von ECDL Lernzielkatalogen für Österreich ist auf der ECDL Website www.ecdl.at veröffentlicht.

Haftung

Die OCG hat dieses Dokument mit Sorgfalt erstellt, kann aber weder Richtigkeit und Vollständigkeit der enthaltenen Informationen zusichern noch Haftung für durch diese Informationen verursachte Schäden übernehmen.

Urheberrecht

ICDL TECHNICIAN BASIC

Das ICDL Package besteht aus folgenden Modulen:

ICDL Remote Work 5
ICDL Computing 10
ICDL Cyber-Security 15
ICDL Robotik Basic 23

ZIELE DES LEHRGANGS

Nach dem Lehrgang ICDL Technician Basic

- beherrschen Sie die wichtigsten Richtlinien des Remote-Arbeitens und können so in einem virtuellen Team gut zusammenarbeiten.
- verstehen Sie die wichtigsten Gefahrenpotenziale für Ihre Arbeit von zu Hause aus und wissen sich gegen diese zu schützen.
- verstehen Sie die Denkweise des Programmierens und können erste kleine Programme selbstständig erstellen.
- verstehen Sie die wichtigsten Gefahrenpotenziale für Ihre Arbeit am Computer und mit mobilen Geräten und können sich kompetent dagegen schützen.
- kennen Sie die Grundkomponenten eines Roboters und verstehen die Schlüsselkonzepte von Robotiksystemen.

REMOTE WORK

Dieses Modul umfasst die wichtigsten Kenntnisse und Fertigkeiten für ein effizientes Arbeiten aus der Ferne (Fernarbeit, Telearbeit).

LERNZIELE

Absolvent*innen dieses Moduls sollen

- den Begriff Remote Work (Fernarbeit bzw. Telearbeit) verstehen; verschiedene Modelle für Remote Work kennen; die Vorteile und Herausforderungen des Remote Work für Gesellschaft, Unternehmen und Arbeitende verstehen,
- die Wichtigkeit von Selbstmanagement und Teamwork in der Remote Work Arbeitsumgebung kennen; die wesentlichen Skills für das selbständige Arbeiten sowie das Arbeiten im Team beherrschen,
- über die wichtigsten Richtlinien für das Setup im Remote Work, wie Gesundheit und Sicherheit sowie die Anforderungen an Technik und Sicherheit Bescheid wissen,
- die wichtigsten Tools zur Unterstützung von Remote Work kennen und effizient einsetzen.

1 BEGRIFFE IM BEREICH REMOTE WORK

1.1 Schlüsselbegriffe

1.1.1 Den Begriff Remote Work definieren; verschiedene Arten von Remote Work kennen, wie: alternierend und permanent

1.1.2 Verschiedene Remote Work Modelle für Arbeitende kennen, wie: mobiles Arbeiten, Homeoffice, Coworking Spaces; verschiedene Remote Work Modelle für Unternehmen kennen: verteilt, hybrid

1.2 Vorteile und Herausforderungen

1.2.1 Die möglichen Vorteile von Remote Work für Wirtschaft und Gesellschaft kennen, wie: weniger Verkehr daher weniger Umweltverschmutzung, weniger Druck zu Zentralisierung in Ballungsräume

1.2.2 Die möglichen Herausforderungen von Remote Work für Wirtschaft und Gesellschaft kennen, wie: fehlende politische Rahmenbedingungen und gesetzliche Regelungen, fehlende Infrastruktur

1.2.3 Die möglichen Vorteile von Remote Work für Unternehmen kennen, wie: höhere Produktivität, weniger Abwesenheitszeiten, geringere Gemeinkosten, Zugang zu einem breiteren Kreis an Arbeitskräften

1.2.4 Die möglichen Herausforderungen von Remote Work für Unternehmen kennen, wie: Investitionen in Tools, Geräte, Netzwerke und Kompetenzen; Schutz von Geräten und Daten; mehr Autonomie für Mitarbeitende, neue Managementaufgaben; Personalführung von Neuzugängen; Beziehungen und Teams aufbauen und pflegen

1.2.5 Die möglichen Vorteile von Remote Work für Arbeitende kennen, wie: mehr Flexibilität, weniger Zeit und Kosten für Pendeln

1.2.6 Die möglichen Herausforderungen von Remote Work für Arbeitende kennen, wie: Ermüdung durch lange Arbeitszeiten, Arbeiten trotz Krankheit, Schwierigkeit von der Arbeit abzuschalten, Isolation und Stress durch mangelnde Unterstützung, Feedback, Kommunikation und Zusammenarbeit, Auswirkungen von ergonomisch schlechtem Arbeitsplatz

2 SELBSTMANAGEMENT, TEAMWORK

2.1 Selbstmanagement

2.1.1 Wissen, welche persönlichen Skills Remote Work unterstützen, wie: Organisation, Disziplin, Problemlösungskompetenz, Selbstmotivation

2.1.2 Wissen, wie die Gefahr von Überarbeitung bei Remote Work vermieden werden kann: eine Arbeitsroutine entwickeln, Pausen machen, Arbeitszeitplan festlegen, bei Krankheit frei nehmen, Arbeitsbereich und persönlichen Bereich trennen, in der Freizeit Arbeitstools ausschalten

2.1.3 Wissen, wie man bei Remote Work produktiv sein kann: tägliche und wöchentliche Ziele setzen, den eigenen Fortschritt dokumentieren, projektbezogene und technische Fragen selbstständig zu lösen versuchen, Probleme – wenn nötig – weiterleiten (eskalieren)

2.2 Teamwork

2.2.1 Effiziente Kommunikationsformen für Remote Work kennen, wie: regelmäßige informelle Kommunikation mit der Kollegenschaft, regelmäßige Team-Kommunikation, regelmäßige Kommunikation mit Vorgesetzten

2.2.2 Passende und professionelle Formen der Kommunikation (Netiquette) kennen, wie: klare und präzise Sprache verwenden, keine beleidigende Sprache verwenden, keine anstößigen und unnötigen Inhalte teilen, anderen verständnisvoll zuhören

2.2.3 Effiziente Arten der Zusammenarbeit im Team für Remote Work kennen, wie: auf gemeinsame Ziele hinarbeiten, offener Meinungs- und Ideenaustausch, Rollen und Verantwortlichkeiten verstehen, kollaborative Tools passend einsetzen

3 SETUP

3.1 Richtlinien

3.1.1 Richtlinien in Bezug auf Remote Work kennen, die von den Unternehmen umgesetzt werden müssen, wie: Informationssicherheit, Datenschutz, Gesundheit und Sicherheit

3.1.2 Wissen, dass die Richtlinien des Unternehmens in Bezug auf Remote Work sowie den Einsatz von Tools und Geräten einzuhalten sind

3.1.3 Elemente einer ergonomischen Arbeitsumgebung nennen, wie: Arbeitsplatz, Sitzgelegenheit, Licht

3.1.4 Wissen, dass es wichtig ist beim Remote Work entsprechende Kontaktpersonen zu kennen, wie: Team-Mitglieder, Personalabteilung, Buchhaltung, technischer Support

3.2 Technologien

3.2.1 Grundlegende technische Anforderungen für Remote Work kennen, wie: schnelle und verlässliche Internetverbindung, geeignete Computer/Geräte, Kamera, Mikrophon, Laufsprecher, verschiedene Online-Tools

3.2.2 Die wichtigsten Online-Tools zur Unterstützung von Remote Work kennen, wie: Kommunikationstools, Tools für Meetings, Ideenfindung, Erstellung und Teilen von Inhalten, Kalender und Aufgabenverwaltung

3.2.3 Wichtige Eigenschaften von Tools zum Remote Work kennen, wie: multiple User, synchrone/asynchrone Kommunikation, globale Reichweite, gleichzeitiger Zugriff

3.2.4 Kriterien für die Auswahl von Tools zum Remote Work kennen, wie: leichte Bedienbarkeit, Sicherheit und Datenschutz, organisatorische und technische Konsistenz, Kosten

3.3 Sicherheit

3.3.1 Verstehen, dass es wichtig ist, Kompetenzen für den sicheren und effizienten Einsatz der IT zu erwerben; die wichtigsten Sicherheitsbestimmungen für Remote Work kennen, wie: sichere Verwahrung der Geräte, regelmäßiges Update der Betriebssysteme und Software, Einsatz und regelmäßiges Ändern von starken Passwörtern, Abmelden von Konten, Geräte sperren bzw. ausschalten, wenn sie nicht im Einsatz sind

3.3.2 Wichtige Sicherheitsbestimmungen für mobile Geräte kennen, wie: PIN verwenden, regelmäßiges Backup der Inhalte, WLAN/Bluetooth an- bzw. ausschalten, eine sichere Internetverbindung verwenden

4 TOOLS

4.1 Kommunikationstools

4.1.1 Gängige asynchrone Kommunikationstools und deren Einsatzbereich kennen, wie: E-Mail, Messenger, Sprachaufzeichnung, Soziale Medien

4.1.2 Gängige synchrone Kommunikationstools und deren Einsatzbereich kennen, wie: Chat, VoIP, Meetings, Webinare

4.2 Meetings

4.2.1 Beispiele für gängige Online-Meeting und Online-Webinar Tools kennen

4.2.2 Die Eigenschaften von Online-Meeting und Online-Webinar Tools kennen, wie: Arten der Verbindung, Passwortanforderungen, Zeitzonen, Dauer

4.2.3 Faktoren für effiziente Online-Meetings kennen, wie: Zeitzonen beachten, Teilnehmende aktiv einbinden, pünktlich enden

4.3 Ideenfindung

4.3.1 Online-Tools zur Ideenfindung kennen, wie: Soziale Medien, Notizen, virtuelles Whiteboard

4.3.2 Die Hauptschritte der Ideenfindung nennen: Sammeln, Organisieren, Zusammenfassen

4.4 Erstellen und Teilen

4.4.1 Wissen, dass gängige Produktivitäts-Applikationen lokal oder online verfügbar sind; Beispiele für Produktivitäts-Applikationen kennen, wie: Textverarbeitung, Tabellenkalkulation, Präsentation

4.4.2 Kollaborative Eigenschaften von Online-Produktivitäts-Applikationen kennen, wie: Teilen von Dateien, Update durch mehrere User in Echtzeit, Kommentare in Echtzeit, automatisches Speichern von Versionen

4.4.3 Beispiele für Tools zum Online-Speichern und -Teilen von Inhalten kennen

4.4.4 Eigenschaften von Tools zum Online-Speichern und -Teilen von Inhalten kenne, wie: Zugriffsrechte einstellen, Zugriffszeiten festsetzen, verfügbare Speichermenge kennen

4.4.5 Die Risiken beim Arbeiten mit geteilten Dateien kennen: Zugriff auf falsche Versionen, irrtümliches Update von Dateien

4.5 Kalender und Aufgabenverwaltung

4.5.1 Den Einsatz von Kalender-Tools zur Planung von Aktivitäten und Meetings verstehen

4.5.2 Beispiele für Tools zur Aufgabenverwaltung kennen

4.5.3 Die wichtigsten Schritte beim Einsatz von Tools zur Aufgabenverwaltung kennen: Definieren und Zuteilen von Aufgaben und Ressourcen; Kriterien wie Erledigungsdatum und Dauer wählen; Fortschritt überwachen

COMPUTING

Dieses Modul behandelt grundlegende Kenntnisse und Fertigkeiten, die erforderlich sind, um Computational Thinking und Coding zur Erstellung einfacher Computerprogramme anzuwenden.

LERNZIELE

Die Absolvent*innen sollen

- Grundlagen des Computing und typische Schritte beim Erstellen eines Programmes verstehen,
- Methoden des Computational Thinking wie Problemzerlegung, Mustererkennung, Abstraktion und algorithmisches Design zur Problemanalyse und Lösungsentwicklung verstehen und anwenden,
- Algorithmen für ein Programm unter Verwendung von Flussdiagrammen und Pseudocode schreiben, testen und bearbeiten,
- Wesentliche Grundsätze und Schlüsselbegriffe des Codings und die Bedeutung von gutstrukturiertem und dokumentiertem Code verstehen,
- Programmierbegriffe wie Variablen, Datentypen und Logik in einem Programm verstehen und verwenden,
- Effizienz und Funktionalität verbessern, indem Iteration, bedingte Anweisungen, Prozeduren und Funktionen sowie Events und Commands in einem Programm eingesetzt werden,
- Programm testen, Fehler bereinigen (Debugging) und vor der Auslieferung sicherstellen, dass die erforderlichen Bedingungen erfüllt sind.

1 BEGRIFFE IM BEREICH COMPUTING

1.1 Schlüsselbegriffe

1.1.1 Begriffswelt im Bereich Computing kennenlernen

1.1.2 Identifikation bestimmter Denkweisen als Computational Thinking

1.1.3 Den Begriff Programm kennen

1.1.4 Den Begriff Code kennen; zwischen Quellcode und Maschinencode unterscheiden

1.1.5 Wissen, wozu die Programmbeschreibung und wozu die Programmspezifikation dient

1.1.6 Erforderliche Schritte bei der Erstellung eines Programms kennen: Analyse, Entwurf, Programmierung, Testen, Erweiterung

1.1.7 Unterschied zwischen einer formalen und einer natürlichen Sprache kennen

2 METHODEN DES COMPUTATIONAL THINKING

2.1 Problemanalyse

2.1.1 Typische Methoden des Computational Thinking erläutern: Zerlegung, Mustererkennung, Abstraktion, Algorithmen

2.1.2 Problemzerlegung verwenden, um umfangreiche Daten und Prozesse zu bewältigen oder um ein komplexes Problem in kleinere Teile zu zerlegen

2.1.3 Standardlösungen (Muster) in den zerlegten Teilproblemen identifizieren können

2.1.4 Abstraktion verwenden, um unnötige Einzelheiten bei der Problemanalyse aus dem Weg zu räumen

2.1.5 Die Rolle von Algorithmen beim Computational Thinking verstehen

2.2 Algorithmisches Design

2.2.1 Rolle des Konzepts Sequenz in den Abläufen verstehen

2.2.2 Möglichkeiten der Hilfe bei der Problemanalyse kennen, wie: Flussdiagramme, Pseudocode

2.2.3 Symbole in Flussdiagrammen kennen, wie: Start/Stopp, Prozess, Entscheidung, Ein-/Ausgabe, Verbinder, Pfeil

2.2.4 Abfolge der wichtigsten Schritte mit einem Flussdiagramm oder mit Pseudocode beschreiben

2.2.5 Detaillierten Ablauf (Algorithmus) unter Verwendung von Flussdiagramm oder Pseudocode beschreiben

2.2.6 Fehler in einem Algorithmus verbessern, wie: fehlendes Programmelement, falsche Sequenz, falsches Entscheidungskriterium bei der Verzweigung

3 CODING

3.1 Erste Schritte

3.1.1 Stileigenschaften eines optisch gut strukturierten und dokumentierten Programmcodes kennen, wie: Einrückung, geeignete Kommentare und aussagekräftige Bezeichnungen

3.1.2 Einfache arithmetische Operatoren verwenden, um Rechenschritte in einem Programm auszuführen: +, -, /, *

3.1.3 Prioritäten der Operatoren und Reihenfolge der Evaluation in arithmetischen, logischen und zeichenverarbeitenden Ausdrücken kennen; Verstehen, wie Klammern zur Strukturierung komplexer Ausdrücke eingesetzt werden

3.1.4 Verwendung von Parametern in einem Programm kennen

3.1.5 Verwendung von Kommentaren in einem Programm verstehen und erläutern

3.1.6 Zweckmäßige Kommentare in einem eigenen Programm setzen

3.2 Variablen und Daten

3.2.1 Konzept Variable kennen und erläutern; Variablen in einem Programm verwenden

3.2.2 Definition, Initialisierung und Verwendung einer Variablen unterscheiden

3.2.3 Zuweisung von Werten an eine Variable

3.2.4 Geeigneten Namen für Berechnungen und zur Speicherung von Werten verwenden

3.2.5 Einfache Datentypen in einem Programm verwenden: Zeichenkette (string), Zeichen (character), Ganzzahlen (integer), Gleitkommazahlen (float), Logische Aussagen (boolean)

3.2.6 Strukturierte Datentypen in einem Programm verwenden, wie: Array, Liste, Tupel

3.2.7 In einem interaktiven Programm auf Dateneingaben reagieren

3.2.8 In einem interaktiven Programm die Datenausgabe auf dem Bildschirm gestalten

4 KONSTRUKTIVE VERWENDUNG VON CODE-ELEMENTEN

4.1 Logik

4.1.1 Korrekte Formulierung von logischen Tests beherrschen; zweckmäßige Verwendung eines logischen Tests in einem Programm kennen und erläutern

4.1.2 Boolesche Logikaussagen mit Variablen, Vergleichsoperatoren und Booleschen Operatoren als Ausdrücke formulieren; Verwendung der Operatoren: =, >, <, >=, <=, <>, !=, ==, AND, OR, NOT

4.1.3 Logikaussagen in einem Programm einbauen

4.2 Schleifen (Iteration)

4.2.1 Korrekte Formulierung von Schleifen beherrschen; zweckmäßige Verwendung von Schleifen in einem Programm kennen und erläutern

4.2.2 Verschiedene Arten von Schleifen unterscheiden, wie: FOR, WHILE, REPEAT

4.2.3 Schleifen wie FOR, WHILE, REPEAT in einem Programm verwenden

4.2.4 Konzept einer Endlosschleife verstehen

4.2.5 Konzept der Rekursion verstehen, Unterschied zur Iteration kennen

4.3 Bedingte Anweisung

4.3.1 Korrekte Formulierung von bedingten Anweisungen beherrschen; zweckmäßige Verwendung einer bedingten Anweisung in einem Programm kennen und erläutern

4.3.2 Mehrweganweisung IF...THEN...ELSE in einem Programm verwenden

4.4 Prozeduren und Funktionen

4.4.1 Konzept der Prozedur verstehen; zweckmäßige Verwendung einer Prozedur in einem Programm verstehen und erläutern

4.4.2 In einem Programm einen Teil davon korrekt in eine Prozedur ausgliedern und benennen

4.4.3 Konzept der Funktion verstehen; zweckmäßige Verwendung einer Funktion in einem Programm kennen und erläutern

4.4.4 Einen geeigneten Teil eines Programms in eine Funktion ausgliedern und benennen

4.4.5 Funktionen mit Parametern schreiben können

4.4.6 Funktionen schreiben können, die sich selber aufrufen (Rekursion)

4.5 Ereignisse (Events) und Aufrufe (Commands)

4.5.1 Konzept eines Ereignisses (Events) verstehen; zweckmäßige Verwendung eines Ereignisses (Events) in einem Programm erläutern

4.5.2 Ereignisbehandlungsroutine (Event-Handler) erstellen und verwenden, wie: Mausklick, Tastatureingabe, Klick auf Schaltfläche, Timer

4.5.3 Funktionen aus Standardbibliotheken verwenden, wie: math, random, time

5 TESTEN, FEHLERSUCHE, AUSLIEFERUNG

5.1 Programm ausführen, testen, Fehler beseitigen

5.1.1 Möglichkeiten von Test und Beweis zur Erreichung eines möglichst korrekten Programms richtig einschätzen

5.1.2 Verschiedene Arten von Fehlern in einem Programm kennen und unterscheiden, wie: Programmsyntax und Programmlogik

5.1.3 Programme ausführen

5.1.4 Syntaxfehler in einem Programm suchen und beheben, wie: falsche Schreibweise, fehlende Trennzeichen.

5.1.5 Logikfehler in einem Programm suchen und beheben, wie: inkorrekter boolescher Ausdruck, inkorrekter Datentyp

5.2 Auslieferung des Programms

5.2.1 Erstelltes Programm mit den Anforderungen der ursprünglichen Problembeschreibung vergleichen

5.2.2 Erstelltes Programm beschreiben, Zweck und Wert kommunizieren

5.2.3 Erweiterungen und Verbesserungen für das Programm vorschlagen, die einen zusätzlichen Nutzen bringen würden

CYBER-SECURITY

Diese Modul vermittelt Kenntnisse für eine sichere Nutzung der IKT im Alltag, über geeignete Maßnahmen für eine sichere Netzwerkverbindung, über Sicherheit im Internet und über die richtige Handhabung von Daten und Informationen.

LERNZIELE

Die Absolvent*innen sollen

- verstehen, wie wichtig die Sicherheit von Daten und Informationen ist und die Grundsätze zum Datenschutz, zur Datenspeicherung, zur Datenkontrolle und zum Schutz der Privatsphäre kennen,
- Bedrohungen für die persönliche Sicherheit durch Identitätsdiebstahl sowie die mögliche Gefährdung von Daten durch Cloud-Computing kennen,
- Passwörter und Verschlüsselung zur Sicherung von Dateien und Daten einsetzen können,
- die Bedrohung durch Malware verstehen und Computer, mobile Geräte und Netzwerke vor Malware schützen sowie auf Malware-Attacken richtig reagieren können,
- übliche Sicherheitsmerkmale von Netzwerken und Drahtlosverbindungen kennen sowie Personal Firewalls und persönliche Hotspots verwenden können,
- Computer und mobile Geräte vor unberechtigtem Zugriff schützen sowie Passwörter sicher handhaben und ändern können,
- geeignete Web-Browser-Einstellungen verwenden können, wissen, wie man die Vertrauenswürdigkeit einer Website feststellt und sicher im Internet surft,
- verstehen, dass Sicherheitsprobleme bei der Online-Kommunikation per E-Mail, VoIP, Instant Messaging und in sozialen Netzwerken und durch die Nutzung mobiler Geräte auftreten können,
- Daten auf lokalen Speicherorten und in der Cloud sichern und wiederherstellen können sowie Daten sicher löschen und Geräte entsorgen können.

GRUNDBEGRIFFE ZU SICHERHEIT

1.1 Datenbedrohung

1.1.1 Zwischen Daten und Informationen unterscheiden können

1.1.2 Die Begriffe Cybercrime und Hacken verstehen

1.1.3 Böswillige und unabsichtliche Bedrohung für Daten durch Einzelpersonen, Dienstleister und externe Organisationen kennen

1.1.4 Bedrohung für Daten durch höhere Gewalt kennen, wie: Feuer, Hochwasser, Krieg, Erdbeben

1.1.5 Bedrohung für Daten durch die Verwendung von Cloud-Computing kennen, wie: Datenkontrolle, möglicher Verlust der Privatsphäre

1.2 Wert von Informationen

1.2.1 Grundlegende Merkmale von Datensicherheit verstehen, wie: Vertraulichkeit, Integrität, Verfügbarkeit

1.2.2 Verstehen, weshalb personenbezogene Daten zu schützen sind, z. B. um Identitätsdiebstahl und Betrug zu verhindern, zum Schutz der Privatsphäre

1.2.3 Verstehen, weshalb Firmendaten auf Computern und mobilen Geräten zu schützen sind, z. B. um Diebstahl, betrügerische Verwendung, unabsichtlichen Datenverlust und Sabotage zu verhindern

1.2.4 Allgemeine Grundsätze für Datenschutz/Privatsphäre-Schutz, Datenaufbewahrung und Datenkontrolle kennen, wie: Transparenz, Notwendigkeit, Verhältnismäßigkeit

1.2.5 Die Begriffe Betroffene und Auftraggeber verstehen. Verstehen, wie die Grundsätze für Datenschutz/Privatsphäre-Schutz, Datenaufbewahrung und Datenkontrolle für Betroffene und Auftraggeber angewendet werden

1.2.6 Verstehen, dass bei der Nutzung von IKT die Einhaltung von Grundsätzen und Richtlinien wichtig ist; wissen, wie die Richtlinien üblicherweise bekanntgemacht werden bzw. zugänglich sind

1.3 Persönliche Sicherheit

1.3.1 Den Begriff Social Engineering verstehen und die Ziele kennen, wie: unberechtigter Zugriff auf Computer und mobile Geräte, unerlaubtes Sammeln von Informationen, Betrug

1.3.2 Methoden des Social Engineering kennen, wie: Telefonanrufe, Phishing, Shoulder Surfing

1.3.3 Den Begriff Identitätsdiebstahl verstehen und die Folgen von Identitätsmissbrauch in persönlicher, finanzieller, geschäftlicher und rechtlicher Hinsicht kennen

1.3.4 Methoden des Identitätsdiebstahls kennen, wie: Information Diving, Skimming, Pretexting

1.4 Sicherheit für Dateien

1.4.1 Die Auswirkung von aktivierten und deaktivierten Makro-Sicherheitseinstellungen verstehen

1.4.2 Die Vorteile und die Grenzen von Verschlüsselung verstehen. Wissen, wie wichtig es ist, das Passwort, den Schlüssel und das Zertifikat der Verschlüsselung nicht offenzulegen und nicht zu verlieren

1.4.3 Eine Datei, einen Ordner oder ein Laufwerk verschlüsseln

1.4.4 Dateien mit einem Passwort schützen, z. B.: Dokumente, Tabellenkalkulationsdateien, komprimierte Dateien

2 MALWARE

2.1 Arten und Funktionsweisen

2.1.1 Den Begriff Malware verstehen; verschiedene Möglichkeiten kennen, wie Malware auf Computern und anderen Geräten verborgen werden kann, wie: Trojaner, Rootkit, Backdoor

2.1.2 Arten von sich selbst verbreitender Malware kennen und ihre Funktionsweise verstehen, wie: Virus, Wurm

2.1.3 Arten von Malware und ihre Funktionsweise für Datendiebstahl, Betrug oder Erpressung kennen, wie: Adware, Ransomware, Spyware, Botnet, Keylogger, Dialer

2.2 Schutz

2.2.1 Die Funktionsweise und die Grenzen von Antiviren-Software verstehen.

2.2.2 Verstehen, dass Antiviren-Software auf Computern und mobilen Geräten installiert sein soll

2.2.3 Die Bedeutung von regelmäßigen Software-Updates für Antiviren-Software, Web-Browser, Plug-ins, Anwendungsprogramme, Betriebssysteme verstehen

2.2.4 Laufwerke, Ordner und Dateien mit Antiviren-Software scannen; Zeitplan

für Scans mit Antiviren-Software festlegen

2.2.5 Verstehen, dass die Verwendung veralteter und nicht mehr unterstützter Software mit Risiken verbunden ist, wie: zunehmende Gefährdung durch Malware, Inkompatibilität

2.3 Problemlösung und -behebung

2.3.1 Den Begriff Quarantäne verstehen und die Auswirkung auf infizierte oder verdächtige Dateien kennen

2.3.2 Infizierte oder verdächtige Dateien unter Quarantäne stellen oder löschen

2.3.3 Wissen, dass ein Malware-Angriff mithilfe von Online-Ressourcen identifiziert und bekämpft werden kann, wie: Websites der Anbieter von Betriebssystemen, Antiviren-Software und Web-Browser; Websites von zuständigen Behörden/Organisationen

3 SICHERHEIT IM NETZWERK

3.1 Netzwerke und Verbindungen

3.1.1 Den Begriff Netzwerk verstehen und übliche Netzwerktypen kennen, wie: Local Area Network (LAN), Wireless Local Area Network (WLAN), Wide Area Network (WAN), Virtual Private Network (VPN)

3.1.2 Verstehen, wodurch sich eine Verbindung zu einem Netzwerk auf die Sicherheit auswirken kann, wie: Malware, unberechtigter Zugriff auf Daten, Schutz der Privatsphäre

3.1.3 Die Aufgaben der Netzwerk-Administration verstehen, wie: Authentifizierung, Benutzerrechte verwalten, Nutzung dokumentieren, sicherheitsrelevante Patches und Updates überwachen und installieren, Netzwerkverkehr überwachen, Malware im Netzwerk bekämpfen

3.1.4 Die Funktion und die Grenzen einer Firewall bei der privaten Computernutzung und in einer Arbeitsumgebung verstehen

3.1.5 Personal Firewall ein- und ausschalten; den durch die Personal Firewall laufenden Datenverkehr für eine Anwendung, einen Dienst/Funktion zulassen bzw. blockieren

3.2 Sicherheit im drahtlosen Netz

3.2.1 Verschiedene Möglichkeiten zum Schutz von drahtlosen Netzwerken und deren Grenzen kennen, wie: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) / Wi-Fi Protected Access 2 (WPA2),

Media Access Control (MAC) Filter, Service Set Identifier (SSID) verbergen

3.2.2 Sich bewusst sein, dass auf ein ungeschütztes drahtloses Netzwerk Angriffe erfolgen können, wie: unbefugter Zugriff durch Eindringlinge, Hijacking, Man-in-the-Middle-Angriff

3.2.3 Den Begriff persönlicher Hotspot verstehen

3.2.4 Einen sicheren persönlichen Hotspot einschalten und ausschalten; Geräte sicher damit verbinden und trennen

4 ZUGRIFFSKONTROLLE

4.1 Methoden

4.1.1 Maßnahmen kennen, um unberechtigten Zugriff auf Daten zu verhindern, wie: Benutzername, Passwort, PIN, Verschlüsselung, Multi-Faktor-Authentifizierung

4.1.2 Den Begriff Einmal-Passwort und die typische Verwendung verstehen

4.1.3 Verstehen, wozu ein Netzwerk-Konto dient

4.1.4 Verstehen, dass der Zugang zu einem Netzwerk-Konto mit Benutzername und Passwort erfolgen soll, und dass der Zugang bei Nichtgebrauch durch Sperren oder Abmelden geschlossen werden soll

4.1.5 Biometrische Verfahren zur Zugangskontrolle kennen, wie: Fingerabdruck, Augenscan, Gesichtserkennung, Handgeometrie

4.2 Passwort-Verwaltung

4.2.1 Richtlinien für ein gutes Passwort kennen, wie: angemessene Mindestlänge beachten, aus Buchstaben und Ziffern und Sonderzeichen zusammensetzen, geheim halten, regelmäßig ändern, unterschiedliche Passwörter für unterschiedliche Dienste verwenden

4.2.2 Die Funktion und die Grenzen einer Passwort-Verwaltungssoftware verstehen

5 SICHERE WEB-NUTZUNG

5.1 Browser-Einstellungen

5.1.1 Einstellungen zum Ausfüllen von Formularen aktivieren und deaktivieren, wie: automatische Vervollständigung, automatisches Speichern

5.1.2 In einem Browser persönliche Daten löschen, wie: Browserverlauf, Downloadverlauf, temporäre Internetdateien, Passwörter, Cookies, Formulardaten

5.2 Sicheres Surfen

5.2.1 Sich bewusst sein, dass bestimmte Online-Aktivitäten (Einkaufen, E-Banking) nur auf sicheren Webseiten über eine gesicherte Netzwerkverbindung erfolgen sollen

5.2.2 Kriterien zur Beurteilung der Vertrauenswürdigkeit einer Website kennen, wie: inhaltliche Qualität, Aktualität, gültige URL, Information zum Inhaber der Webseite (Impressum), Kontaktdaten, Sicherheitszertifikat, Überprüfung der Domain-Inhaberschaft

5.2.3 Den Begriff Pharming verstehen

5.2.4 Den Zweck und die Funktionsweise von Software zur Inhaltskontrolle kennen, wie: Internet-Filterprogramme, Kinderschutz-Software

6 KOMMUNIKATION

6.1 E-Mail

6.1.1 Verstehen, weshalb eine E-Mail verschlüsselt und entschlüsselt wird

6.1.2 Den Begriff Digitale Signatur verstehen

6.1.3 Arglistige und unerwünschte E-Mails erkennen

6.1.4 Typische Merkmale von Phishing kennen, wie: Verwendung der Namen von seriösen Unternehmen und Personen, Verwendung von Logos und Markenzeichen, Links zu gefälschten Webseiten, Aufforderung zur Bekanntgabe persönlicher Daten

6.1.5 Wissen, dass Phishing-Attacken den betroffenen seriösen Unternehmen und zuständigen Behörden/Organisationen gemeldet werden können

6.1.6 Sich der Gefahr bewusst sein, dass ein Computer oder mobiles Gerät mit Malware infiziert werden kann, wenn ein E-Mail-Attachment geöffnet wird, das ein Makro oder eine ausführbare Datei enthält

6.2 Soziale Netzwerke

6.2.1 Verstehen, dass es wichtig ist, vertrauliche oder personenbezogene Informationen nicht in sozialen Netzwerken zu veröffentlichen

6.2.2 Sich der Notwendigkeit bewusst sein, in sozialen Netzwerken geeignete Konto-Einstellungen auszuwählen und regelmäßig zu überprüfen, wie: Privatsphäre, Standort

6.2.3 Konto-Einstellungen in sozialen Netzwerken anwenden: Privatsphäre, Standort

6.2.4 Mögliche Gefahren bei der Nutzung von sozialen Netzwerken kennen, wie: Cyber-Mobbing, Cyber-Grooming, bösartige Veröffentlichung persönlicher Inhalte, falsche Identitäten, betrügerische oder arglistige Links, Inhalte oder Nachrichten

6.2.5 Wissen, dass missbräuchliche Verwendung oder Fehlverhalten in sozialen Netzwerken dem jeweiligen Service-Provider und zuständigen Behörden/ Organisationen gemeldet werden kann

6.3 VoIP und Instant Messaging

6.3.1 Schwachstellen bei der Sicherheit von Instant Messaging (IM) und Voice over Internet Protocol (VoIP) verstehen und Gefahren kennen, wie: Malware, Backdoor-Zugang, Zugriff auf Dateien, Lauschangriff

6.3.2 Methoden kennen, um beim Gebrauch von IM und VoIP Vertraulichkeit sicherzustellen, wie: Verschlüsselung, Nicht-Veröffentlichung von wichtigen Informationen, Zugriff auf Daten einschränken

6.4 Mobile Geräte

6.4.1 Verstehen, welche Folgen die Verwendung von Anwendungen aus inoffiziellen App-Stores haben kann, wie: mobile Malware, unnötiger Ressourcenverbrauch, Zugriff auf persönliche Daten, schlechte Qualität, versteckte Kosten

6.4.2 Den Begriff App-Berechtigungen verstehen

6.4.3 Wissen, dass mobile Anwendungen private Informationen von mobilen Geräten auslesen können, wie: Kontaktdaten, Standortverlauf, Bilder

6.4.4 Für den Fall, dass ein mobiles Gerät abhandenkommt, Sofortmaßnahmen und Vorsichtsmaßnahmen kennen, wie: Fernsperrung, Fernlöschung, Geräteortung

7 SICHERE DATENVERWALTUNG

7.1 Daten sichern und Backups erstellen

7.1.1 Maßnahmen zur physischen Sicherung von Computern und mobilen Geräten kennen, wie: nicht unbeaufsichtigt lassen, Standort der Geräte und weitere Details aufzeichnen, Sicherungskabel verwenden, Zugangskontrolle

7.1.2 Wissen, wie wichtig eine Sicherungskopie für den Fall des Datenverlusts auf Computern und anderen Geräten ist

7.1.3 Wesentliche Merkmale eines Konzepts zur Datensicherung kennen, wie: Regelmäßigkeit/Häufigkeit, Zeitplan, Ablageort, Datenkompression

7.1.4 Backup an einem Speicherort erstellen, wie: lokale Laufwerke, externe Laufwerke/Datenträger, Cloud-Speicher

7.1.5 Daten von einem Backup-Speicherort wiederherstellen, wie: lokale Laufwerke, externe Laufwerke/Datenträger, Cloud-Speicher

7.2 Daten sicher löschen und vernichten

7.2.1 Den Unterschied zwischen der Löschung von Daten und der endgültigen Löschung/Vernichtung von Daten kennen

7.2.2 Den Sinn und Zweck einer endgültigen Löschung/Vernichtung von Daten auf Laufwerken oder Geräten verstehen

7.2.3 Sich bewusst sein, dass das Löschen von Inhalten bei manchen Diensten nicht endgültig ist, wie: Soziale Netzwerke, Blogs, Internetforen, Cloud-Dienste

7.2.4 Methoden zur endgültigen Datenvernichtung kennen, wie: Laufwerke/Datenträger zerstören, z. B. schreddern; Entmagnetisierung; Software zur Datenvernichtung verwenden

ROBOTIK BASIC

In diesem Modul werden die Grundprinzipien der Robotik, der Zusammenbau, die Programmierung und die Steuerung eines einfachen Roboters erläutert.

LERNZIELE

Die Absolvent*innen können

- Schlüsselkonzepte im Zusammenhang mit Robotern und Robotiksystemen verstehen und Beispiele für Roboter identifizieren,
- die wesentlichen Teile eines Roboters und ihre Funktion erkennen, einschließlich Mikrocontroller, Antriebe, Sensoren und Energiequellen,
- die Elemente eines einfachen Steuerungssystems verstehen und ein Steuerungssystem testen,
- grundlegende Programmierkonzepte verstehen sowie ein Programm in einer visuellen Programmiersprache erstellen und ausführen,
- einen Roboter einrichten, Bewegungen implementieren und den Roboter in einer Umgebung steuern.

1 GRUNDKONZEPTE DER ROBOTIK

1.1 Roboter und automatisierte Systeme

1.1.1 Definition der Begriffe Roboter und Robotiksysteme

1.1.2 Verstehen, dass Roboter ferngesteuert, teilautonom oder autonom sein können

1.1.3 Verstehen, dass Roboter stationär oder mobil sein können

1.2 Verwendung von Robotern

1.2.1 Häufige Anwendungen von Robotern in verschiedenen Umgebungen kennen, wie: Zuhause, Schule, Produktion, Gesundheitswesen.

1.2.2 Fortgeschrittene Anwendungen von Robotern kennen, wie: selbstfahrende Autos, robotergestützte Operationen

1.2.3 Ethische Probleme bei der Verwendung von Robotern kennen, wie: Menschen Schaden zufügen

2 ROBOTIK TEILE

2.1 Wesentliche Teile und Komponenten

2.1.1 Wesentliche Teile von Robotern erkennen, wie: Antrieb, Mikrocontroller, Sensoren, Energiequellen

2.1.2 Komponenten eines Roboter-Sets kennen, wie: Chassis, Elektronikteile, Kabel, Werkzeuge und Teile für den Zusammenbau

2.2 Mikrocontroller

2.2.1 Wissen, dass der Mikrocontroller Informationen von Eingabegeräten wie Sensoren sammelt, Programme ausführt und Ausgabegeräte wie LEDs und Audiogeräte steuert

2.2.2 Wesentliche Anschlüsse von Mikrocontrollern kennen, wie: Stromanschluss, USB, kabellos, Ein- und Ausgang

2.3 Antriebsysteme

2.3.1 Hauptteile von Aktuatoren kennen, wie: Schalter und Motor

2.3.2 Verstehen, dass der Aktuator elektrische Energie in mechanische Energie umwandelt, um den Roboter anzutreiben.

2.4 Sensoren

2.4.1 Verstehen, dass ein Sensor Änderungen in der Umgebung wahrnehmen kann, wie: Lichtstärke, Entfernung, Winkel

2.4.2 Die Funktion von verschiedenen Sensortypen kennen, wie: Licht, Klang, Gyroskop

2.5 Fortbewegung und Energiequellen

2.5.1 Teile kennen, welche die Bewegung eines Roboters unterstützen, wie: Arme, Räder

2.5.2 Energiequellen kennen, wie: Batterien, Sonnenenergie

3 EINFACHE STEUERUNGSSYSTEME

3.1 Übersicht der Steuerungssysteme

3.1.1 Elemente eines Steuerungssystems kennen; grundlegende Arten einer Steuerung verstehen, wie: offener und geschlossener Regelkreis

3.1.2 Anbindungen an den Mikrocontroller verstehen, wie: Taster, Strom, Motor, USB-Eingang, kabellose Technologien, Sensoren, Ausgabegeräte

3.1.3 Verbindungen zum Mikrocontroller in einem Blockdiagramm verstehen

3.1.4 Ein einfaches Steuerungssystem aufsetzen, z. B mit Energiequellen, Motoren und Sensoren

3.2 Einfache Steuersysteme testen

3.2.1 Vordefinierte Programme ausführen, um Ausgabewerte bereitzustellen, wie: Lichtstärke, Klang, Entfernung, Winkel.

3.2.2 Verstehen, dass es zwischen Eingang und Ausgabe der Daten eine Verzögerung gibt

3.2.3 Verstehen, dass das Verändern von Variablen in einem Programm die Ausgabe beeinflusst

4 VISUELLE PROGRAMMIERUNG

4.1 Programmiergrundlagen

4.1.1 Definition der Begriffe Programm und Programmiersprache

4.1.2 Wissen, dass Blöcke grundlegende Elemente in einer visuellen Programmiersprache sind; häufige Blockkategorien kennen, wie: Ereignisse, Steuerung.

4.1.3 Typische Tätigkeiten bei der Erstellung eines Programms kennen, wie: Analysieren einer Aufgabe, Entwerfen einer Lösung, Schreiben eines Programms, Testen und Verbessern eines Programms

4.1.4 Grundlegende Elemente eines Programms kennen, wie: Ablauf, Entscheidungen, Schleifen

4.1.5 Verstehen wie ein Flussdiagramm verwendet werden kann, um die Schritte einer Lösung darzustellen

4.2 Konstante, Variable

4.2.1 Zwischen den Begriffen Konstante und Variable im Kontext eines Programms unterscheiden

4.2.2 Neue Variablen erstellen und passende Werte zuweisen

4.3 Ereignisse, Steuerung

4.3.1 Verwendung eines Ereignisblocks in einem Programm, wie: wenn

4.3.2 Verwendung eines Steuerungsblocks in einem Programm, wie: warten, warten bis

4.3.3 Eine Schleife oder endlose Fortsetzung mit Blöcken implementieren, wie: für immer, wiederholen

4.3.4 Bedingungen mit Blöcken implementieren, wie: wenn, dann, sonst

4.3.5 Logische Operatoren verwenden, wie: und, nicht, oder

4.4 Erstellen und Ausführen eines Programms

4.4.1 Einen Plan skizzieren und ein Problem lösen, wie: Steuerung einer Ausgabe, eine Reihe von Aktionen durchführen

4.4.2 Zeichnen eines Flussdiagramms, um die Schritte einer Lösung abzubilden

4.4.3 Erstellen eines Programms in einer visuellen Programmiersprache, um ein Problem zu lösen, wie: Steuerung einer Ausgabe, eine Reihe von Aktionen durchführen

4.4.4 Verstehen, dass es mehr als einen Weg gibt ein Programm zu schreiben, um dasselbe Problem zu lösen

4.4.5 Ausführen eines Programms; Identifizieren und Lösen von Fehlern in einem Programm

5 ARBEITEN MIT ROBOTERN

5.1 Einrichten

5.1.1 Sicherheitsrichtlinien verstehen und implementieren, wie: sicherer Umgang mit elektronischen Teilen und Werkzeug; Bewusstsein um die eigene Sicherheit und um die anderer

5.1.2 Zusammenbauen eines Roboters mit dem vorhandenen Werkzeug

5.2 Implementierung der Roboterbewegung

5.2.1 Implementierung von einfachen Roboterbewegungen, wie: Stopp, Vorwärts- und Rückwärtsbewegung, Drehen

5.2.2 Verständnis für die Zusammenhänge zwischen Energie, Entfernung, Geschwindigkeit und Zeit in der Roboterbewegung.

5.2.3 Anwenden von Konzepten wie Energie, Entfernung, Geschwindigkeit und Zeit, um Bewegungen zu steuern: Vorwärts- und Rückwärtsbewegung; verstehen, dass Schwung und Reibung die Bewegung beeinflussen können

5.2.4 Zusammenhänge von Energie, Rotationsgeschwindigkeit und Winkel der Rotation in der Roboterbewegung verstehen

5.3 Implementierung der Robotersteuerung

5.3.1 Verwendung eines Roboters, um Sensordaten zu sammeln, wie: Entfernung, Klang, Winkel, Licht

5.3.2 Bauen, Testen und Verbessern eines Programms, um den Roboter mittels eines Sensors zu steuern, wie: Licht, Klang, Gyroskop.

5.3.3 Die Wichtigkeit des Testens verstehen, um Fehler zu beseitigen

5.3.4 Verstehen, dass manche Fehler zufällig auftreten, wie: Staub, unbekannte Variablen.

5.4 Steuerung in einer Umgebung

5.4.1 Navigation eines Roboters in einer Umgebung, um Aufgaben mithilfe verschiedener Funktionalitäten abzuschließen, wie: einer Linie folgen oder ausweichen; einem Objekt / einem Hindernis folgen oder ausweichen; eine Rampe hinauf- oder hinunterfahren

5.4.2 Navigation eines Roboters in einer Umgebung, um verschiedene Szenarien mithilfe passender Kombinationen von Bewegung und Funktionalitäten abzuschließen

5.4.3 Wissen, dass Teamwork bei der gemeinsamen Arbeit an einem Roboter wichtig ist; Bedeutung von Fähigkeiten/Skills kennen, wie: Planung, Kommunikation, Aufgabenzuteilung

ICDL WORKFORCE

Digitale Kompetenzen für Beruf und Produktivität

GRUNDLAGEN

- Computer-Grundlagen
- Online-Grundlagen
- Online-Zusammenarbeit
- Cyber-Security

OFFICE ANWENDUNGEN

- Textverarbeitung
- Tabellenkalkulation
- Präsentation
- Datenbanken anwenden

PRAKTISCHE ANWENDUNGEN

- Bildbearbeitung
- Computing

ICDL
The Digital Skills Standard

www.icdleurope.org