ICDL
The Digital Skills Standard

OESTERREICHISCHE COMPUTER GESELLSCHAFT®
AUSTRIAN COMPUTER SOCIETY

IT-SECURITY

Lernzielkatalog Version 2.0

www.ocg.at

Zweck dieses Dokuments

Dieses Dokument listet die Lerninhalte für das ICDL Modul ***IT-Security*** Version 2.0 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. Approbierte Lernmaterialien decken dessen Inhalte ab.

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

ICDL Foundation

Arkle Road
Sandyfod
Co. Dublin
D18 Y3X2
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 ICDL Lernzielkatalogen für Österreich ist auf der ICDL Website www.icdl.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

IT-SECURITY

Dieses 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

Absolvent*innen dieses Moduls 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 und Personal Firewalls und Persönliche Hotspots verwenden können,
- Computer und mobile Geräte vor unberechtigtem Zugriff schützen und Passwörter sicher handhaben und ändern können,
- geeignete Webbrowser-Einstellungen verwenden können und wissen, wie man die Vertrauenswürdigkeit einer Website feststellt und sicher im Internet surft,
- verstehen, dass Sicherheitsprobleme bei der Kommunikation per E-Mail, VoIP, Instant Messaging und in sozialen Netzwerken sowie 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.

1. GRUNDBEGRIFFE ZUR 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 Information

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 der 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 unterstützte 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, Auge scannen, Gesichtserkennung, Handgeometrie.

4.2. Passwort-Verwaltung

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

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 Massaging

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

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

ICDL Zertifikate

ICDL STANDARD (UMFASST 7 MODULE)

4 Base Module

- Computer-Grundlagen
- Online-Grundlagen
- Textverarbeitung
- Tabellenkalkulation

+

3 Wahlmodule

- Präsentation
- IT-Security
- Online-Zusammenarbeit
- Computing*
- Datenbanken anwenden
- Bildbearbeitung*
- Künstliche Intelligenz*
- Robotik*

ICDL ADVANCED EXPERT

- Textverarbeitung Advanced*
- Tabellenkalkulation Advanced*
- Präsentation Advanced*
- Datenbanken Advanced*

*** Modul auch als Einzelzertifikat verfügbar**

Österreichische Computer Gesellschaft (OCG) | Wollzeile 1 | 1010 Wien
+43 1 512 02 35 - 0 | info@ocg.at | ocg.at | icdl.at

ICDL
The Digital Skills Standard