ICDL
The Digital Skills Standard

ICDL Workforce
IT-Sicherheit
Syllabus 2.0

Syllabus Dokument

ICDL Germany

Zweck

Dieses Dokument beschreibt den Lehrplan für das ICDL Modul IT-Sicherheit. Der Lehrplan beschreibt anhand der Lernziele die Kenntnisse und Fähigkeiten, die ein Kandidat für dieses Modul besitzen sollte. Der Lehrplan bildet auch die Grundlage für den theoretischen und praktischen Test zu diesem Modul.

Disclaimer

Obwohl bei der Erstellung dieser Publikation alle Sorgfalt aufgewendet wurde, übernimmt die ICDL Foundation als Herausgeber der englischen Originalversion keine Gewähr für die Vollständigkeit der darin enthaltenen Informationen. Weiterhin übernimmt die ICDL Foundation keine Verantwortung oder Haftung für etwaige Fehler, Auslassungen, Ungenauigkeiten, Verluste oder Schäden, die aufgrund von Informationen, Anweisungen oder Ratschlägen in dieser Veröffentlichung entstehen. Änderungen können von der ICDL Foundation nach eigenem Ermessen und jederzeit ohne vorherige Ankündigung vorgenommen werden.

DLGI
Dienstleistungsgesellschaft für Informatik
Am Bonner Bogen 6
53227 Bonn
Tel.: 0228- 688-448-0 Fax: 0228- 688-448-99

E-Mail: info@dlgi.de
URL: www.dlgi.de
URL: www.icdl.de

IT-Sicherheit

Dieses Modul beinhaltet die wichtigsten Begriffe und Konzepte für den sicheren Umgang mit Informations- und Kommunikationstechnologie, sowie die Kenntnisse und Fertigkeiten, die erforderlich sind, um eine sichere Netzwerkverbindung herzustellen, sich im Internet gefahrlos zu bewegen, und um sachgerecht mit Daten und Informationen umgehen zu können.

Ziele

Die Kandidatinnen und Kandidaten sollen:

- verstehen, dass es wichtig ist, Informationen und Daten sicher aufzubewahren, und allgemeine Grundlagen des Datenschutzes, der Speicherung und Kontrollmechanismen kennen,
- Bedrohungen der persönlichen Sicherheit erkennen können, von Identitätsdiebstahl bis hin zu potentieller Bedrohung von Daten durch die Verwendung von Cloud-Computing,
- in der Lage sein, Passwörter und Verschlüsselung zu verwenden, um Dateien und Daten zu schützen,
- die Bedrohung durch Malware verstehen und in der Lage sein, Computer, mobile Geräte und Netzwerke vor Malware zu schützen, und Probleme durch Malware-Attacken zu beheben,
- allgemeine Sicherheitstypen von Netzwerken und Drahtlosverbindungen kennen, und in der Lage sein, eine persönliche Firewall und persönliche Hotspots zu verwenden,
- einen Computer oder andere mobile Geräte vor unberechtigtem Zugriff schützen können, und in der Lage sein, Passwortaktualisierungen sicher zu handhaben,
- geeignete Einstellungen im Web-Browser vornehmen können, und wissen, wie man sicher im Internet surft,
- verstehen, welche Sicherheitsprobleme bei der Kommunikation, z.B. mit E-Mail, sozialen Netzwerken, VoIP, Instant Messaging und bei mobilen Geräten auftreten können,
- Daten auf lokalen Speichern oder in der Cloud sichern und rückspielen können, Daten löschen, sowie Daten und Geräte sicher vernichten und entsorgen können.

Kategorie	Wissensgebiet	Nr.	Lernziel
1 Sicherheits-konzepte	*1.1 Bedrohungen für Daten*	1.1.1	Daten und Informationen unterscheiden können.
		1.1.2	Die Begriffe *Cybercrime* und *Hacken* verstehen.
		1.1.3	Böswillige und unbeabsichtigte Bedrohungen für Daten durch Mitarbeiter, Service Provider und externe Organisationen kennen.
		1.1.4	Bedrohungen für Daten durch höhere Gewalt, wie Feuer, Flut, Erdbeben und Krieg erkennen.
		1.1.5	Bedrohung für Daten durch Verwendung von *Cloud*-Computing kennen: Datenschutz, Verlust der Privatsphäre.

Kategorie	Wissensgebiet	Nr.	Lernziel
	1.2 Der Wert von Informationen	1.2.1	Die wesentlichen Eigenschaften von Informationssicherheit verstehen: Vertraulichkeit, Integrität und Verfügbarkeit.
		1.2.2	Gründe für den Schutz von persönlichen Informationen verstehen wie: Identitätsdiebstahl und Betrug verhindern, Erhalt der Privatsphäre.
		1.2.3	Gründe für den Schutz Daten am Arbeitsplatz gespeichrten Daten - auf Computern und mobilen Geräten - verstehen: Diebstahl, betrügerische Verwendung von Daten, unbeabsichtigten Datenverlust und Sabotage verhindern.
		1.2.4	Die wichtigsten Regeln zum Datenschutz, zur Aufbewahrung und zur Kontrolle von Daten kennen: Transparenz, rechtmäßige Zweckverwendung, Verhältnismäßigkeit.
		1.2.5	Die Begriffe *Betroffener* und *Datenverarbeitende Stellen* verstehen. Verstehen, wie Datenschutz, Aufbewahrung und Kontrollmechanismen darauf Anwendung finden.
		1.2.6	Verstehen, dass es wichtig ist, Richtlinien in der Informations- und Kommunikations-technologie einzuführen und einzuhalten.
	1.3 persönliche Datensicherheit	1.3.1	Den Begriff *Social Engineering* im Zusammenhang mit Datensicherheit verstehen: nicht autorisierter Zugriff auf Computer und andere Geräte, nicht autorisierte Datenbeschaffung, Betrug.
		1.3.2	Methoden des *Social Engeneering* kennen: Telefongespräche, *Phishing*, *Shoulder Surfing*.
		1.3.3	Den Begriff Identitätsdiebstahl verstehen und dessen Auswirkungen kennen: auf persönlicher, finanzieller, geschäftlicher und rechtlicher Ebene.
		1.3.4	Methoden des Identitätsdiebstahls, wie *Skimming, Pretexting* und *Information Diving* kennen.
	1.4 Datensicherheit in Programmen	1.4.1	Bedeutung von Makro- Sicherheitseinstellungen verstehen: aktivieren bzw. deaktivieren.
		1.4.2	Vorteile und Grenzen der Datenverschlüsselung verstehen. Verstehen, dass es wichtig ist, das Passwort, den Schlüssel oder das Zertifikat zur Verschlüsselung

Kategorie	Wissensgebiet	Nr.	Lernziel
			nicht zu verlieren und nicht offen zu legen.
		1.4.3	Eine Datei, einen Ordner, ein Laufwerk verschlüsseln.
		1.4.4	Kennwortschutz für ein Dokument, ein Tabellenblatt oder eine komprimierte Datei erstellen.
2 Malware	*2.1 Arten von Malware und ihre, Funktionsweise*	2.1.1	Den Begriff Malware verstehen. Wissen, wie Malware im System versteckt werden kann: Trojaner, *RootKits* oder *Back Doors*.
		2.1.2	Verschiedene Typen von Malware kennen und ihre Funktionsweise verstehen: Viren, Würmer.
		2.1.3	Unterschiedliche Arten des Datendiebstahls und profitorientierter bzw. erpresserischer Malware kennen und ihre Funktionsweise verstehen: *Adware, Spyware, Botnets, keystroke logging, Dialer*.
	2.2 Schutz vor Malware	2.2.1	Verstehen wie Anti-Virus Software arbeitet und die Grenzen des Schutzes kennen.
		2.2.2	Verstehen, dass eine Anti-Viren-Software auf Computern und anderen Geräten installiert sein sollte.
		2.2.3	Verstehen, dass es wichtig ist, Software regelmäßig zu aktualisieren bzw. Updates zu laden: Anti-Virus, Web-Browser, Anwendungen, Betriebssystem.
		2.2.4	Laufwerke, Ordner und Dateien mit Anti-Virus Software überprüfen können. Zeitgesteuerte Scans nutzen.
		2.2.5	Verstehen, dass die Verwendung veralteter und nicht mehr unterstützter Software Risiken mit sich bringt, wie: erhöhte Malware-Bedrohungen, Inkompatibilität.
	2.3 Problemlösung und entfernen	2.3.1	Den Begriff Quarantäne verstehen, und die Auswirkungen auf infizierte und/oder verdächtige Dateien kennen.
		2.3.2	Quarantäne, infizierte/verdächtige Dateien löschen.
		2.3.3	Verstehen, dass eine Malware-Attacke mit Hilfe von Online-Ressourcen diagnostiziert und behoben werden kann wie: Webseiten des Betriebssystems, Anti-Virus-Software, Web-Browser-Software Provider, Webseiten von entsprechenden Behörden.

Kategorie	Wissensgebiet	Nr.	Lernziel
3 Netzwerk-sicherheit	*3.1 Netzwerke und Netzwerk-verbindungen*	3.1.1	Verstehen, was ein Netzwerk ist und die wichtigsten Netzwerkarten kennen: LAN, WLAN, WAN, VPN.
		3.1.2	Die möglichen Auswirkungen einer Netzwerkverbindung auf die Sicherheit verstehen: Malware, unberechtigter Datenzugriff, Gefährdung der Privatsphäre
		3.1.3	Die Aufgaben eines Netzwerk-Administrators in Verbindung mit der Vergabe von Rechten verstehen wie: Autorisierung, Authentifizierung Kontenvergabe für ein Netzwerk, Malwarehandhabung innerhalb eines Netzwerkes.
		3.1.4	Funktionsweise und Leistungsgrenzen einer Firewall am heimischen Computer kennen.
		3.1.5	Eine Firewall ein- und ausschalten. Einer Anwendung, Service/Funktion den Zugriff gestatten oder durch die persönliche Firewall blockieren.
	3.2 Absicherung von drahtlosen Netzwerken	3.2.1	Unterschiedliche Verschlüsslungen und ihre Grenzen für Drahtlosnetzwerke kennen: WEP, WPA, WPA2, SSID und MAC.
		3.2.2	Verstehen, dass die Verwendung eines ungeschützten Drahtlosnetzwerks zu folgenden Attacken führen kann: Lauschangriff, Netzwerk-Übernahme (Hijacking), *man-in-the-middle*.
		3.2.3	Den Begriff persönlichen Hotspot verstehen.
		3.2.4	Einen persönlichen Hotspot aktivieren/deaktivieren, Geräte damit verbinden und trennen.
4 Zugangs-kontrolle	*4.1 Methoden*	4.1.1	Maßnahmen kennen, um den nicht autorisierten Zugriff auf Daten zu verhindern: Benutzername, Kennwort, PIN, Verschlüsselung, Multi-Faktor-Authentifizierung.
		4.1.2	Den Begriff *Einmal-Passwort* verstehen, und die wichtigsten Anwendungsgebiete kennen.
		4.1.3	Sinn und Zweck eines Netzwerkkontos verstehen.

Kategorie	Wissensgebiet	Nr.	Lernziel
		4.1.4	Verstehen, dass man mit Benutzernamen und Passwort auf ein Netzwerkkonto zugreifen sollte, und es sperren bzw. sich ausloggen sollte, wenn man es nicht benutzt.
		4.1.5	Biometrische Zugangskontrollen kennen wie: Fingerabdruck, Iris-Scan, Gesichtserkennung, Handgeometrie.
	4.2 Passwort-Management	4.2.1	Wissen, wie ein gutes Passwort aufgebaut ist, und wie man mit Passwörter umgehen sollte: nicht an Dritte weitergeben, regelmäßiges Ändern der Passwörter, ausreichende Passwortlänge und Zeichenfolge aus Buchstaben, Zahlen und Sonderzeichen.
		4.2.2	Funktion und Grenzen eines Passwort-Managers verstehen.
5 Sicherer Umgang mit Internetdiensten	*5.1 Browser-einstellungen*	5.1.1	Einstellungen für das automatische Speichern und die automatische Vervollständigung eines Formulars auswählen, aktivieren und deaktivieren können.
		5.1.2	Persönliche Daten aus dem Browser löschen: Verlauf, Cache, Passwörter, Cookies, Daten zur automatischen Vervollständigung.
	5.2 Sicheres Surfen	5.2.1	Verstehen, dass bestimmte **Online**-Aktivitäten (Kauf, Online-Banking) nur auf Webseiten mit sicherer Verbindung getätigt werden sollten.
		5.2.2	Methoden kennen, um die Echtheit einer Webseite zu beurteilen wie: Qualität des Inhaltes, Aktualität, gültige URL, Unternehmens- oder Eigentümerinformation, Kontaktinformationen, Sicherheitszertifikat, Validierung des Domaininhabers.
		5.2.3	Wissen, was *Pharming* ist.
		5.2.4	Zweck und die Funktionsweise von Programmen zur Inhaltskontrolle von Webseiten kennen: Internet-Filter-Software, Software zur elterlichen Kontrolle
6 Kommunikation	*6.1 E-Mail*	6.1.1	Sinn und Zweck von Ver- und Entschlüsselung im E-Mail-Verkehr verstehen.
		6.1.2	Den Begriff *Digitale Signatur* verstehen.
		6.1.3	Betrügerische und unerwünschte E-Mails erkennen können.

Kategorie	Wissensgebiet	Nr.	Lernziel
		6.1.4	Verstehen, was *Phishing* ist und *Phishing*-Attacken an ihren typischen Eigenschaften erkennen: Verwendung von wirklichen Firmen- oder Personennamen, Falsche Logos und Branding, falsche Weblinks, Ermutigung zur Offenlegung persönlicher Daten.
		6.1.5	Wissen, dass man *Phishing*-Attacken an legitimierte Stellen und zuständige Behörden melden kann.
		6.1.6	Verstehen, dass beim Öffnen von Dateianhängen mit Makros oder ausführbaren Dateien der Computer oder ein anderes Gerät durch Malware infiziert werden kann.
	6.2 Soziale Netzwerke	6.2.1	Verstehen, dass keine wichtigen oder persönlichen Informationen auf *Social Networking* Seiten offengelegt werden sollten.
		6.2.2	Verstehen, dass man seine Kontoeinstellungen bei einem sozialen Netzwerk im Blick haben, und diese sinnvoll anwenden sollte. Privatsphäre, Standort.
		6.2.3	Einstellungen für ein Netzwerkkonto anwenden: Privatsphäre, Standort.
		6.2.4	Mögliche Gefahren verstehen, die von Seiten sozialer Netzwerke ausgehen können: *Cyber Bullying*, *Grooming*, gefährliche/verwirrende Informationen, falsche Identitäten, betrügerische und böswillige Nachrichten und Links.
		6.2.5	Wissen, dass man die missbräuchliche Nutzung sozialer Netzwerkseiten dem Service Provider oder den entsprechenden Behörden melden kann.
	6.3 VoIP und Instant Messaging	6.3.1	Gefährdung durch *Instant Messaging* und *VoIP* durch *Malware*, *backdoor access*, Lauschangriff, Datenzugriff verstehen.
		6.3.2	Methoden zur sicheren Nutzung von *Instant Messaging (IM)* und *VoIP* kennen: Verschlüsselung, Nicht-Offenlegung wichtiger Daten, Beschränkung der gemeinsamen Dateinutzung.
	6.4 Mobile Geräte	6.4.1	Möglichen Auswirkungen der Verwendung von Anwendungen aus inoffiziellen App-Stores verstehen wie: mobile Malware, unnötige Ressourcennutzung, Zugriff auf personenbezogene Daten, schlechte Qualität, versteckten Kosten.

Kategorie	Wissensgebiet	Nr.	Lernziel
		6.4.2	Den Begriff *Berechtigungen in einer App* verstehen.
		6.4.3	Sich bewusst sein, dass mobile Anwendungen private Informationen von mobilen Geräten extrahieren können wie: Kontaktdaten, Standortverlauf, Bilder.
		6.4.4	Vorsichts- und Hilfsmaßnahmen für den Fall eines Verlustes bei einem mobilen Gerät kennen: Fernsperrung, Fernlöschung, Gerät orten.
7 Sicheres Daten-Management	*7.1 Datensicherung*	7.1.1	Wissen, wie man Computer und mobile Geräte physisch schützen kann: nicht unbeaufsichtigt lassen, Gerät und Gerätestandort sperren bzw. abschließen, Sicherheitskabel, Zugangskontrolle.
		7.1.2	Verstehen, dass eine Routine zur Datensicherung (Backup) notwendig ist, um der Gefahr des Datenverlustes vorzubeugen.
		7.1.3	Wichtige Bedingungen der Datensicherung kennen: Regelmäßige zeitgesteuerte Sicherung, sichere Lagerung, Datenkomprimierung.
		7.1.4	Backup an einem bestimmten Ort erstellen können: lokales Laufwerk, externes Laufwerk/Medium, Cloud-Service.
		7.1.5	Daten von Ort eines Backups wieder herstellen können: lokales Laufwerk, externes Laufwerk/Medium, Cloud-Service.
	7.2 Daten richtig löschen und vernichten	7.2.1	Den Unterschied zwischen dem Löschen von Daten und dauerhafter Datenvernichtung kennen.
		7.2.2	Gründe zur endgültigen Löschung von Daten, Laufwerken und Geräten verstehen.
		7.2.3	Verstehen, dass das Löschen von Inhalten nicht automatisch zu ihrer Vernichtung führt: Seiten sozialer Netzwerke, Blogs, Internetforen, Cloud-Service.
		7.2.4	Methoden zur dauerhaften endgültigen Vernichtung von Daten kennen: Shreddern, Zerstörung des Datenträgers, Entmagnetisierung (Degaussieren), Verwendung von Programmen zur vollständigen Datenvernichtung.