INHALT

Der Aufbau dieser Lernunterlage ist der Gliederung des ECDL-Lernzielkatalog 2.0 angepasst. Kapitel und Unterkapitel sind daher in der gleichen Nummerierung, wie sie im ECDL-Lernzielkatalog verwendet wird.

1 GRUNDBEGRIFFE ZU SICHERHEIT 9

1.1 Datenbedrohung 9

1.1.1 Zwischen Daten und Informationen unterscheiden können 9

1.1.2 Die Begriffe Cybercrime und Hacken verstehen 10

1.1.3 Böswillige und unabsichtliche Bedrohung für Daten durch Einzelpersonen, Dienstleister und externe Organisationen kennen 12

1.1.4 Bedrohung für Daten durch höhere Gewalt kennen, wie: Feuer, Hochwasser, Krieg, Erdbeben 13

1.1.5 Bedrohung für Daten durch die Verwendung von Cloud-Computing kennen, wie: Datenkontrolle, möglicher Verlust der Privatsphäre 14

1.2 Wert von Informationen 15

1.2.1 Grundlegende Merkmale von Datensicherheit verstehen, wie: Vertraulichkeit, Integrität, Verfügbarkeit 15

1.2.2 Verstehen, weshalb personenbezogene Daten zu schützen sind, zB um Identitätsdiebstahl und Betrug zu verhindern, zum Schutz der Privatsphäre 16

1.2.3 Verstehen, weshalb Firmendaten auf Computern und mobilen Geräten zu schützen sind, zB um Diebstahl, betrügerische Verwendung, unabsichtlichen Datenverlust und Sabotage zu verhindern 17

1.2.4 Allgemeine Grundsätze für Datenschutz/Privatsphäre-Schutz, Datenaufbewahrung und Datenkontrolle kennen, wie: Transparenz, Notwendigkeit, Verhältnismäßigkeit 17

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 20

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 20

1.3 Persönliche Sicherheit 22

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 22

1.3.2 Methoden des Social Engineering kennen, wie: Telefonanrufe, Phishing, Shoulder Surfing 22

1.3.3 Den Begriff Identitätsdiebstahl verstehen und die Folgen von Identitätsmissbrauch in persönlicher, finanzieller, geschäftlicher und rechtlicher Hinsicht kennen 24

1.3.4 Methoden des Identitätsdiebstahls kennen, wie: Information Diving, Skimming, Pretexting 24

1.4 Sicherheit für Dateien 25

1.4.1 Die Auswirkung von aktivierten und deaktivierten Makro-Sicherheitseinstellungen verstehen 26

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 26

1.4.3 Eine Datei, einen Ordner oder ein Laufwerk verschlüsseln 27

1.4.4 Dateien mit einem Passwort schützen, zB: Dokumente, Tabellenkalkulationsdateien, komprimierte Dateien 33

2 MALWARE 35

2.1 Arten und Funktionsweisen 35

2.1.1 Den Begriff Malware verstehen; verschiedene Möglichkeiten kennen, wie Malware auf Computern und anderen Geräten verborgen werden kann, wie: Trojaner, Rootkit, Backdoor 35

2.1.2 Arten von sich selbst verbreitender Malware kennen und ihre Funktionsweise verstehen, wie: Virus, Wurm 36

2.1.3 Arten von Malware und ihre Funktionsweise für Datendiebstahl, Betrug oder Erpressung kennen, wie: Adware, Ransomware, Spyware, Botnet, Keylogger, Dialer. 37

2.2 Schutz 39

2.2.1 Die Funktionsweise und die Grenzen von Antiviren-Software verstehen 40

2.2.2 Verstehen, dass Antiviren-Software auf Computern und mobilen Geräten installiert sein soll 40

2.2.3 Die Bedeutung von regelmäßigen Software-Updates für Antiviren-Software, Web-Browser, Plug-ins, Anwendungsprogramme, Betriebssysteme verstehen ..41

2.2.4 Laufwerke, Ordner und Dateien mit Antiviren-Software scannen; Zeitplan für Scans mit Antiviren-Software festlegen 42

2.2.5 Verstehen, dass die Verwendung veralteter und nicht mehr unterstützter Software mit Risiken verbunden ist, wie: zunehmende Gefährdung durch Malware, Inkompatibilität. 43

2.3 Problemlösung und -behebung 43

2.3.1 Den Begriff Quarantäne verstehen und die Auswirkung auf infizierte oder verdächtige Dateien kennen 43

2.3.2 Infizierte oder verdächtige Dateien unter Quarantäne stellen oder löschen 44

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 44

Wissens-Check 45

3 SICHERHEIT IM NETZWERK 47

3.1 Netzwerke und Verbindungen 47

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) 47

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 48

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 48

3.1.4 Die Funktion und die Grenzen einer Firewall bei der privaten Computernutzung und in einer Arbeitsumgebung verstehen. 49

3.1.5 Personal Firewall ein- und ausschalten; den durch die Personal Firewall laufenden Datenverkehr für eine Anwendung, einen Dienst/Funktion zulassen bzw. blockieren 50

3.2 Sicherheit im drahtlosen Netz 52

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. 53

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 55

3.2.3 Den Begriff Persönlicher Hotspot verstehen. 56

3.2.4 Einen sicheren Persönlichen Hotspot einschalten und ausschalten; Geräte sicher damit verbinden und trennen. 57

Wissens-Check 58

4 ZUGRIFFSKONTROLLE 59

4.1 Methoden 59

4.1.1 Maßnahmen kennen, um unberechtigten Zugriff auf Daten zu verhindern, wie: Benutzername, Passwort, PIN, Verschlüsselung, Multi-Faktor-Authentifizierung 59

4.1.2 Den Begriff Einmal-Passwort und die typische Verwendung verstehen 60

4.1.3 Verstehen, wozu ein Netzwerk-Konto dient 60

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 61

4.1.5 Biometrische Verfahren zur Zugangskontrolle kennen, wie: Fingerabdruck, Auge scannen, Gesichtserkennung, Handgeometrie 61

4.2 Passwort-Verwaltung 62

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 63

4.2.2 Die Funktion und die Grenzen einer Passwort-Verwaltung verstehen 64

5 SICHERE WEB-NUTZUNG 65

5.1 Browser-Einstellungen 65

5.1.1 Einstellungen zum Ausfüllen von Formularen aktivieren und deaktivieren, wie: automatische Vervollständigung, automatisches Speichern 66

5.1.2 In einem Browser persönliche Daten löschen, wie: Browserverlauf, Downloadverlauf, temporäre Internetdateien, Passwörter, Cookies, Formulardaten 67

5.2 Sicheres Surfen 67

5.2.1 Sich bewusst sein, dass bestimmte Online-Aktivitäten (Einkaufen, E-Banking) nur auf sicheren Webseiten über eine gesicherte Netzwerkverbindung erfolgen sollen 68

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 68

5.2.3 Den Begriff Pharming verstehen 69

5.2.4 Den Zweck und die Funktionsweise von Software zur Inhaltskontrolle kennen, wie: Internet-Filterprogramme, Kinderschutz-Software 70

Wissens-Check 74

6 KOMMUNIKATION 75

6.1 E-Mail 75

6.1.1 Verstehen, weshalb eine E-Mail verschlüsselt und entschlüsselt wird 75

6.1.2 Den Begriff Digitale Signatur verstehen 77

6.1.3 Arglistige und unerwünschte E-Mails erkennen 78

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 79

6.1.5 Wissen, dass Phishing-Attacken den betroffenen seriösen Unternehmen und zuständigen Behörden/Organisationen gemeldet werden können 82

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 83

6.2 Soziale Netzwerke 84

6.2.1 Verstehen, dass es wichtig ist, vertrauliche oder personenbezogene Informationen nicht in sozialen Netzwerken zu veröffentlichen 84

6.2.2 Sich der Notwendigkeit bewusst sein, in sozialen Netzwerken geeignete Konto-Einstellungen auszuwählen und regelmäßig zu überprüfen, wie: Privatsphäre, Standort 84

6.2.3 Konto-Einstellungen in sozialen Netzwerken anwenden: Privatsphäre, Standort 85

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 86

6.2.5 Wissen, dass missbräuchliche Verwendung oder Fehlverhalten in sozialen Netzwerken dem jeweiligen Service-Provider und zuständigen Behörden/Organisationen gemeldet werden kann 87

6.3 VoIP und Instant Messaging 88

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 89

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 89

6.4 Mobile Geräte 90

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 91

6.4.2 Den Begriff App-Berechtigungen verstehen 92

6.4.3 Wissen, dass mobile Anwendungen private Informationen von mobilen Geräten auslesen können, wie: Kontaktdaten, Standortverlauf, Bilder 92

Wissens-Check 94

7 SICHERE DATEN-VERWALTUNG 95

7.1 Daten sichern und Backups erstellen 95

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 95

7.1.2 Wissen, wie wichtig eine Sicherungskopie für den Fall des Datenverlusts auf Computern und anderen Geräten ist 96

7.1.3 Wesentliche Merkmale eines Konzepts zur Datensicherung kennen, wie: Regelmäßigkeit/Häufigkeit, Zeitplan, Ablageort, Datenkompression 97

7.1.4 Backup an einem Speicherort erstellen, wie: lokale Laufwerke, externe Laufwerke/Datenträger, Cloud-Speicher.....97

7.1.5 Daten von einem Backup-Speicherort wiederherstellen, wie: lokale Laufwerke, externe Laufwerke/Datenträger, Cloud-Speicher.....99

7.2 Daten sicher löschen und vernichten 101

7.2.1 Den Unterschied zwischen der Löschung von Daten und der endgültigen Löschung/Vernichtung von Daten kennen.....101

7.2.2 Den Sinn und Zweck einer endgültigen Löschung/Vernichtung von Daten auf Laufwerken oder Geräten verstehen.....101

7.2.3 Sich bewusst sein, dass das Löschen von Inhalten bei manchen Diensten nicht endgültig ist, wie: Soziale Netzwerke, Blogs, Internetforen, Cloud-Dienste 102

7.2.4 Methoden zur endgültigen Datenvernichtung kennen, wie: Laufwerke/Datenträger zerstören, zB schreddern; Entmagnetisierung; Software zur Datenvernichtung verwenden.....102

Wissens-Check..... 104

GLOSSAR 105

Gewinnspiel.....114

ANHANG 115

INDEX 117

Die Nummerierung der Inhaltsangabe nimmt Bezug auf den jeweiligen Punkt des Lernzielkatalogs (Version 2.0), den Sie unter http://www.ecdl.at/downloads-ecdl finden.