

Inhalt

Vorwort.....	I
So benutzen Sie dieses Buch.....	II
Inhalt.....	V
Grundbegriffe zu Sicherheit.....	1
Datenbedrohungen	1
Daten und Informationen.....	2
Datenbedrohung durch Internetkriminalität	3
Datenbedrohung durch höhere Gewalt.....	5
Datenbedrohung durch menschliches Fehlverhalten	5
Datenbedrohung durch Cloud-Computing.....	6
Wert von Informationen.....	7
Personenbezogene Daten	7
Firmendaten.....	8
Schutz durch Passwörter und Verschlüsselung.....	8
Datensicherheit.....	9
Datenschutz	9
Persönliche Sicherheit	11
Social Engineering	12
Identitätsdiebstahl	13
Übungsbeispiel – Sicherheit für Dateien.....	15
Makro-Sicherheitseinstellungen kontrollieren	15
Dokumente und Tabellenkalkulationsdateien schützen	17
Komprimierte Dateien schützen.....	18
Dateien, Ordner und Laufwerke Verschlüsseln.....	19
Vorteile und Grenzen von Verschlüsselung	24

Zusammenfassung.....	25
Malware	29
Definition und Funktionsweise	29
Den Begriff Malware verstehen.....	29
Verbergen von Malware	29
Typen von Malware	30
Sich selbst verbreitende Malware	30
Malware für Datendiebstahl, Erpressung und Betrug.....	31
Schutz vor Malware – Antiviren-Software	34
Funktionsweise von Antiviren-Software	34
Grenzen eines Antivirenprogramms	35
Quarantäne	36
Virensignatur und Heuristik.....	37
Übungsbeispiel – Computer scannen.....	38
Scan planen nach Zeit	38
Scan planen nach Ordnern	40
Scanvorgang spontan durchführen.....	41
Zusammenfassung.....	42
Sicherheit im Netzwerk.....	45
Netzwerke	45
Netzwerk und Netzwerktypen	45
Netzwerk-Administration	46
Funktion einer Firewall	48
Grenzen einer Firewall.....	49
Übungsbeispiel – Firewall Einstellungen verändern.....	49
Personal Firewall ein- und ausschalten.....	49
Datenverkehr zulassen oder blockieren.....	51
Netzwerkverbindungen	53

Kabelgebundenes Netzwerk.....	53
Drahtloses Netzwerk	54
Konsequenzen eines Netzwerkzugriffs	54
Sicherheit im drahtlosen Netzwerk.....	55
SSID verbergen	55
WEP.....	55
WPA und WPA2.....	55
MAC-Listen.....	56
Gefahren eines ungesicherten WLANs	56
Übungsbeispiel – Mobiler Hotspot	57
Mobilen Hotspot einrichten	57
Verbindung zu einem mobilen Hotspot herstellen	59
Netzwerkzugang.....	60
Benutzername und Kennwort	60
Passwortrichtlinien.....	60
Biometrische Verfahren	62
Zusammenfassung.....	63
Sichere Web-Nutzung.....	67
Browser verwenden	67
Sichere Verbindungen	67
Pharming.....	69
Einmalkennwort.....	69
Der Browser als Risikofaktor.....	69
Übungsbeispiel – Mit dem Browserverlauf arbeiten.....	70
Temporäre Internetdateien.....	70
Formulardaten und Kennwörter speichern	71
Browserverlauf bzw. Browserdaten löschen	72
Kontrolle der Internetnutzung.....	73

Soziale Netzwerke	74
Soziale Netzwerke und Privatsphäre	74
Zusammenfassung.....	76
Kommunikation.....	79
E-Mail	79
E-Mails können missbräuchlich verwendet werden	80
E-Mails verschlüsseln und entschlüsseln	80
Digitale Signatur	82
Spam-Mails, Junk-Mails	83
Arglistige, betrügerische Mails	83
Phishing-Mails	84
Infizierte Attachments	85
Instant Messaging und VoIP	85
Schwachstellen und Gefahren	86
VoIP	86
Sicherheit erhöhen	87
Zusammenfassung.....	89
Sicheres Daten-Management.....	93
Daten sichern und Backups erstellen	93
Physische Sicherung von Geräten.....	93
Sicherungskopie (Backup).....	94
Übungsbeispiel – Datensicherung erstellen	97
Backup erstellen	97
Daten wiederherstellen und überprüfen	101
Sichere Datenvernichtung	103
Sinn einer Datenvernichtung	103
Unterschied Löschen und Vernichten	103
Zusammenfassung.....	105

Lernziele ICDL® Standard Modul IT-Security	109
ICDL Standard Modul IT-Security	109
Index.....	116