



# Inhalt

---

<b>Vorwort.....</b>	I
<b>So benutzen Sie dieses Buch.....</b>	II
<b>Inhalt.....</b>	V
<b>Grundbegriffe zu Sicherheit.....</b>	1
Datenbedrohungen .....	1
Daten und Informationen .....	2
Datenbedrohung durch Internetkriminalität .....	3
Datenbedrohung durch höhere Gewalt .....	5
Datenbedrohung durch menschliches Fehlverhalten .....	5
Wert von Informationen.....	6
Personenbezogene Daten .....	6
Firmendaten.....	7
Schutz durch Passwörter und Verschlüsselung.....	7
Datensicherheit.....	8
Datenschutz.....	9
Persönliche Sicherheit .....	10
Social Engineering .....	11
Identitätsdiebstahl .....	12
Sicherheit für Dateien.....	14
Makro-Sicherheitseinstellungen .....	14
Dokumente und Tabellenkalkulationsdateien schützen .....	16
Komprimierte Dateien schützen .....	17
Vorteile und Grenzen von Verschlüsselung.....	18
Zusammenfassung.....	19
<b>Malware.....</b>	23



Definition und Funktionsweise .....	23
Den Begriff Malware verstehen .....	23
Verbergen von Malware.....	23
Typen von Malware .....	24
Sich selbst verbreitende Malware.....	24
Malware für Datendiebstahl, Erpressung und Betrug.....	25
Schutz vor Malware - Antivirensoftware .....	27
Funktionsweise von Antivirensoftware .....	27
Grenzen eines Antivirenprogramms .....	27
Quarantäne .....	28
Virensignatur und Heuristik .....	29
Übungsbeispiel – Computer scannen .....	29
Scan planen .....	30
Scan durchführen .....	33
Zusammenfassung.....	34
<b>Sicherheit im Netzwerk.....</b>	<b>37</b>
Netzwerke .....	37
Netzwerk und Netzwerktypen .....	37
Netzwerk-Administration.....	38
Funktion einer Firewall.....	40
Grenzen einer Firewall .....	41
Netzwerkverbindungen .....	41
Kabelgebundenes Netzwerk.....	41
Drahtloses Netzwerk .....	41
Konsequenzen eines Netzwerkzugriffs.....	42
Sicherheit im drahtlosen Netzwerk .....	43
WEP .....	43
WPA und WPA2 .....	43



MAC-Listen .....	43
Gefahren eines ungesicherten WLANs.....	44
Übungsbeispiel – Verbindung mit einem WLAN .....	44
Verbindung zu einem geschützten WLAN .....	45
Verbindung mit einem ungeschützten WLAN .....	46
Netzwerkzugang .....	47
Benutzername und Kennwort .....	47
Passwortrichtlinien.....	47
Biometrische Verfahren .....	48
Zusammenfassung.....	49
<b>Sichere Web-Nutzung.....</b>	<b>53</b>
Browser verwenden .....	53
Sichere Verbindungen .....	53
Pharming .....	56
Einmalkennwort .....	56
Der Browser als Risikofaktor .....	56
Übungsbeispiel – Mit dem Browserverlauf arbeiten.....	57
Temporäre Internetdateien .....	57
Formulardaten speichern.....	58
Cookies .....	60
Browserverlauf löschen.....	61
Kontrolle der Internetnutzung .....	62
Soziale Netzwerke .....	63
Soziale Netzwerke und Privatsphäre .....	63
Zusammenfassung.....	64
<b>Kommunikation.....</b>	<b>67</b>
E-Mail .....	67
E-Mails können missbräuchlich verwendet werden .....	68





E-Mails verschlüsseln und entschlüsseln.....	68
Übungsbeispiel – Digitale Signatur .....	70
Digitale Signatur erstellen .....	70
Digitale Signatur hinzufügen .....	74
Spam-Mails, Junk-Mails.....	75
Arglistige, betrügerische Mails .....	75
Phishing-Mails .....	75
Infizierte Attachments.....	76
Instant Messaging .....	77
Schwachstellen und Gefahren.....	78
Sicherheit erhöhen.....	78
Zusammenfassung.....	79
<b>Sicheres Daten-Management.....</b>	<b>83</b>
Daten sichern und Backups erstellen .....	83
Physische Sicherung von Geräten .....	83
Sicherungskopie (Backup) .....	84
Übungsbeispiel – Datensicherung erstellen .....	86
Backup erstellen.....	86
Daten wiederherstellen und überprüfen .....	90
Sichere Datenvernichtung .....	92
Sinn einer Datenvernichtung.....	92
Unterschied Löschen und Vernichten .....	92
Zusammenfassung.....	94
<b>Lernziele ECDL Standard Modul IT-Security, Syllabus 1.0 .....</b>	<b>97</b>
Modul IT-Security .....	97
<b>Index .....</b>	<b>103</b>

