

Inhalt

1	Einführung	5
1.1	Die Handlungskompetenz von Modul 486	6
1.2	Das Ziel dieses Lehrmittels.....	8
1.3	Persönliches	8
1.4	Links und Literatur	9
2	Wo liegt denn das Problem?	11
2.1	Die Risikolage	11
2.2	Kategorien der Informationssicherheit.....	12
2.3	Lösungsansätze für die Praxis.....	13
3	Die Welt ist böse	15
3.1	Malware ist tatsächlich böse	15
3.2	Social Engineering.....	22
3.3	Angriffe gegen IT-Systeme.....	26
3.4	Gefahren für die Nutzung mobiler Geräte und Dienste.....	28
3.5	APT – Advanced Persistent Threats.....	29
3.6	Gezielte Angriffsformen	30
3.7	Angriffe in Wireless-Netzwerken.....	34
4	Schwachstellen und Attacken	39
4.1	Angriffe gegen IT-Systeme.....	40
4.2	Angriffe gegen Anwendungen	42
4.3	Angriffe gegen Clients	44
4.4	Netzwerkangriffe	45
4.5	Angriffe gegen die Public Cloud	49
5	Grundlegende Sicherheitskonzepte	51
5.1	Kryptografische Konzepte und Umsetzungen.....	51
5.2	Identitäten und deren Rechte.....	60
5.3	Authentifizierungsmethoden.....	61
5.4	Zugriffssteuerungsmodelle.....	63
5.5	Datenhaltungskonzepte.....	66
5.6	Bewusstsein schaffen	67
6	Systemsicherheit realisieren	71
6.1	Konfigurationsmanagement	71
6.2	Das Arbeiten mit Richtlinien.....	72
6.3	Grundlagen der Systemhärtung.....	73
6.4	Softwareaktualisierung ist kein Luxus	77
6.5	Malware bekämpfen	80

6.6	Advanced Threat Protection	84
6.7	Industrie- und IoT-Systeme	87
6.8	Anwendungssicherheit	90
6.9	Fragen rund um BYOD	91
7	Netzwerke sicher gestalten	95
7.1	Trennung von IT-Systemen	95
7.2	VLAN	97
7.3	Die Brandschutzmauer – Firewalls im Einsatz	100
7.4	Anwendungen im Netzwerk	108
7.5	Sicherheit in der Cloud	112
7.6	Virtual Private Network	114
7.7	Protokolle für einen sicheren Zugriff	116
8	Drahtlose Netzwerke sicher gestalten	127
8.1	Entwicklung der WLAN-Standards	127
8.2	Ein WLAN richtig aufbauen	130
8.3	Sicherheit in drahtlosen Verbindungen	133
8.4	Grundlegende Sicherheitsmaßnahmen umsetzen	137
8.5	Bluetooth – Risiken und Maßnahmen	138
9	Planung für den Ernstfall	143
9.1	Was ist denn ein Notfall?	143
9.2	Resilienz durch Fehlertoleranz	144
9.3	Redundante Verbindungen und Systeme	146
9.4	Notfallvorsorgeplanung	148
9.5	Die Umsetzung	150
9.6	Wartung der Disaster Recovery	154
9.7	Merkmale zur Disaster Recovery	155
10	Security-Audit	159
10.1	Grundlagen von Security-Audits	159
10.2	Standards	161
10.3	Nutzung von Sicherheitsvorlagen	162
10.4	Berichtswesen	163
11	Antworten zu den Aufgaben	167
12	Anhänge	169
12.1	Abkürzungsverzeichnis	169
12.2	Index	172