

Inhaltsverzeichnis

	Über dieses Lehrmittel	5
Teil A	Grundlagen und Rahmenbedingungen	9
	Einleitung, Lernziele und Schlüsselbegriffe	10
1	Richtlinien und Grundbegriffe	12
1.1	Wichtige Richtlinien	12
1.2	Merkmale der IT-Sicherheit	14
1.3	Weitere Begriffe rund um IT-Sicherheit	15
	Repetitionsfragen	20
2	Sicherheitsvorgaben aus dem Strafrecht	21
2.1	Datenschutzgesetz	21
2.2	Bedrohung durch Computerkriminalität	23
2.3	Bestimmungen aus dem Strafrecht	23
	Repetitionsfragen	26
3	Grundprinzip einer Risikoanalyse	27
3.1	Systemabgrenzung	27
3.2	Definition des Datenbestandes	28
3.3	Definition der Verletzbarkeit	28
3.4	Definition der Bedrohungen	28
3.5	Risikoanalyse	28
3.6	Schadenausmass und Eintrittswahrscheinlichkeit	29
3.7	Sicherheitsmassnahmen	29
	Repetitionsfragen	31
Teil B	Bedrohungen und Massnahmen	33
	Einleitung, Lernziele und Schlüsselbegriffe	34
4	Allgemeine Gefährdungen	35
4.1	Gefährdungskatalog höhere Gewalt	36
4.2	Gefährdungskatalog menschliche Fehlhandlungen	36
4.3	Gefährdungskatalog technisches Versagen	36
4.4	Gefährdungskatalog vorsätzliche Handlungen	37
4.5	Gefährdungskatalog organisatorische Mängel	37
	Repetitionsfragen	38
5	Sicherheitsmassnahmen im Überblick	39
5.1	Massnahmenkatalog Infrastruktur	40
5.2	Massnahmenkatalog Personal	40
5.3	Massnahmenkatalog Organisation	40
5.4	Massnahmenkatalog Hardware und Software	41
5.5	Massnahmenkatalog Kommunikation	41
5.6	Massnahmenkatalog Notfallvorsorge	42
	Repetitionsfragen	43
Teil C	Aufbau und Funktionsprinzip des IT-Grundschutzes	45
	Einleitung, Lernziele und Schlüsselbegriffe	46
6	Grundgedanke IT-Grundschutz	48
6.1	IT-Grundschutz-Bausteine	48
6.2	Sicherheitsprozess	52
6.3	Definition der Verantwortlichkeiten	53
6.4	Gefährdungsanalyse und Leitlinien	54
6.5	Erstellung des IT-Sicherheitskonzepts	55
6.6	Umsetzung	56

6.7	Aufrechterhaltung im laufenden Betrieb	56
	Repetitionsfragen	58
7	Strukturanalyse	59
7.1	Netzplanerhebung	59
7.2	Komplexitätsreduktion durch Gruppenbildung	61
7.3	Erhebung der Infrastrukturkomponenten	61
7.4	Erfassung der Anwendungen	62
7.5	Erfassung Komponenten pro Applikation	62
	Repetitionsfragen	63
8	Schutzbedarfsfeststellung	64
8.1	Definition Schutzbedarfskategorien	65
8.2	Schutzbedarfsfeststellung für Anwendungen	66
8.3	Schutzbedarfsfeststellung für IT-Systeme	67
8.4	Schutzbedarfsfeststellung für Kommunikationsverbindungen	68
8.5	Schutzbedarfsfeststellung für Räume	68
8.6	Interpretation der Ergebnisse	69
	Repetitionsfragen	70
9	Grundschutz-Modellierung und Basis-Sicherheitscheck	71
9.1	Grundschutz-Modellierung	71
9.2	Sicherheitsanalyse	75
9.3	Basis-Sicherheitscheck	76
	Repetitionsfragen	78
Teil D	Ausgewählte Beispiele	79
	Einleitung, Lernziele und Schlüsselbegriffe	80
10	Internet-Dienste	81
10.1	WWW-Server	81
10.2	E-Mail	83
	Repetitionsfragen	85
11	Mobile Zugriffsdienste	86
11.1	Firewall	86
11.2	Kryptographie	89
11.3	Remote Access	92
11.4	Telearbeit	95
	Repetitionsfragen	96
Teil E	Anhang	97
	Bedrohungen	98
	Sicherheitsmassnahmen	100
	Auszug aus dem Strafgesetzbuch	119
	Gesamtzusammenfassung	121
	Antworten zu den Repetitionsfragen	123
	Glossar	128
	Stichwortverzeichnis	132