

# Inhaltsverzeichnis

---

<b>Vorwort</b> <b>Über dieses Lehrmittel</b>	<b>5</b>
<hr/>	
<b>Teil A Grundlagen</b>  <b>1 Begriffe und Normen</b> 1.1 Sicherheitspolitik 1.2 Vision und Sicherheitsziele 1.3 Schichten der Systemsicherheit 1.4 IT-Sicherheit und Informationssicherheit 1.5 Rechtliche Aspekte 1.6 Verantwortung des Managements  <b>Repetitionsfragen</b>	<b>9</b>
<hr/>	
<b>2 Gefahren und Risiken</b> 2.1 Angriffsflächen und Sicherheitslücken 2.2 Mängel und Fehler bei der Konfiguration 2.3 Mängel und Fehler bei der Software  <b>Repetitionsfragen</b>	<b>24</b>
<hr/>	
<b>3 Standards und Best Practices</b> 3.1 Allgemeine Anforderungen 3.2 Überblick über Sicherheitsstandards 3.3 Normenreihe ISO 27000 3.4 Vorgehen nach BSI 100-2 3.5 Kontrollen und Audits  <b>Repetitionsfragen</b>	<b>25</b>
<hr/>	
<b>4 Tools und Hilfsmittel</b> 4.1 Vulnerability- und Analysetools 4.2 Spezialisierte Webseiten und Newsletter 4.3 Checklisten 4.4 Systemdokumentation und Softwareinventar 4.5 Lizenzmanagement  <b>Repetitionsfragen</b>	<b>30</b>
<hr/>	
<b>Teil B Systemsicherheit analysieren und entwerfen</b>  <b>5 Sicherheitssituation und -risiken analysieren</b> 5.1 Risikoanalyse 5.2 Informationen und Prozesse klassifizieren 5.3 Sicherheitseinstellungen überprüfen 5.4 Sicherheitslücken und -risiken analysieren  <b>Repetitionsfragen</b>	<b>53</b>
<hr/>	
<b>6 Sicherheitsvorgaben und -anforderungen analysieren</b> 6.1 Externe Sicherheitsvorgaben berücksichtigen 6.2 Interne Sicherheitsanforderungen berücksichtigen 6.3 System-Anomalien erkennen und berücksichtigen  <b>Repetitionsfragen</b>	<b>55</b>
<hr/>	
<b>7 Geeignete Massnahmen ableiten</b> 7.1 Was ist ein Sicherheitsvorfall und wie wird er behandelt? 7.2 Notfälle behandeln 7.3 Sofortmassnahmen definieren  <b>Repetitionsfragen</b>	<b>63</b>
<hr/>	

<b>8</b>	<b>Kosten und Nutzen von Sicherheitsmassnahmen ermitteln</b>	<b>80</b>
8.1	Einzelschäden abschätzen	80
8.2	Einzelrisiken abschätzen	81
8.3	Möglichen Gesamtschaden berechnen	81
8.4	Investitionen in Sicherheitsmassnahmen	81
	<b>Repetitionsfragen</b>	<b>82</b>
<b>Teil C</b>	<b>Systemsicherheit planen und umsetzen</b>	<b>83</b>
<b>9</b>	<b>Grundschutz, Datenschutz und Systembetrieb sicherstellen</b>	<b>85</b>
9.1	Grundschutz gewährleisten	85
9.2	Datenschutz gewährleisten	89
9.3	Systembetrieb gewährleisten	91
	<b>Repetitionsfragen</b>	<b>91</b>
<b>10</b>	<b>Organisatorische Massnahmen vorbereiten und implementieren</b>	<b>92</b>
10.1	Awareness	92
10.2	Systemüberwachung	92
10.3	Regelmässiger Prozess zur Aktualisierung	97
10.4	Forensische Analysen	97
	<b>Repetitionsfragen</b>	<b>98</b>
<b>11</b>	<b>Technische Massnahmen vorbereiten und implementieren</b>	<b>99</b>
11.1	System aktualisieren	99
11.2	System härten	103
11.3	Minimale Rechte	104
11.4	Intrusion Detection	106
	<b>Repetitionsfragen</b>	<b>111</b>
<b>12</b>	<b>Sicherheitsprüfungen vorbereiten und implementieren</b>	<b>112</b>
12.1	Testbestandteile	112
12.2	Physikalische Kontrollen planen und umsetzen	113
12.3	Technische Kontrollen planen und umsetzen	113
12.4	Administrative Kontrollen planen und umsetzen	114
	<b>Repetitionsfragen</b>	<b>115</b>
<b>Teil D</b>	<b>Anhang</b>	<b>117</b>
	<b>Standards zur Systemsicherheit</b>	<b>118</b>
	<b>Gesamtzusammenfassung</b>	<b>123</b>
	<b>Antworten zu den Repetitionsfragen</b>	<b>127</b>
	<b>Glossar</b>	<b>133</b>
	<b>Stichwortverzeichnis</b>	<b>139</b>