

Inhaltsverzeichnis

	Seite
Vorwort	V
M 1 Maßnahmenkatalog Infrastruktur	1
M 1.1 Einhaltung einschlägiger Normen und Vorschriften	1
M 1.2 Regelungen für Zutritt zu Verteilern	1
M 1.3 Angepasste Aufteilung der Stromkreise	1
M 1.4 Blitzschutzeinrichtungen	1
M 1.6 Einhaltung von Brandschutzvorschriften	2
M 1.7 Handfeuerlöscher	2
M 1.8 Raumbelagung unter Berücksichtigung von Brandlasten	2
M 1.9 Brandabschottung von Trassen	2
M 1.10 Sichere Türen und Fenster	3
M 1.11 Lagepläne der Versorgungsleitungen	3
M 1.12 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile	3
M 1.13 Anordnung schützenswerter Gebäudeteile	3
M 1.14 Selbsttätige Entwässerung	4
M 1.15 Geschlossene Fenster und Türen	4
M 1.16 Geeignete Standortauswahl	4
M 1.17 Pförtnerdienst	4
M 1.18 Gefahrenmeldeanlage	5
M 1.19 Einbruchsschutz	5
M 1.20 Auswahl geeigneter Kabeltypen unter physikalischmechanischer Sicht	5
M 1.21 Ausreichende Trassendimensionierung	5
M 1.22 Materielle Sicherung von Leitungen und Verteilern	6
M 1.23 Abgeschlossene Türen	6
M 1.24 Vermeidung von wasserführenden Leitungen	6
M 1.25 Überspannungsschutz	6
M 1.26 Not-Aus-Schalter	7
M 1.27 Klimatisierung der Technik / in Technikräumen	7
M 1.28 Lokale unterbrechungsfreie Stromversorgung	7
M 1.29 Geeignete Aufstellung eines IT-Systems	8
M 1.30 Absicherung der Datenträger mit TK-Gebührendaten	8
M 1.31 Fernanzeige von Störungen	8
M 1.32 Geeignete Aufstellung von Druckern und Kopierern	8
M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz	9
M 1.34 Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz	9
M 1.35 Sammelaufbewahrung tragbarer IT-Systeme	9
M 1.36 Sichere Aufbewahrung der Datenträger vor und nach Versand	9
M 1.37 Geeignete Aufstellung eines Faxgerätes	9
M 1.38 Geeignete Aufstellung eines Modems	10
M 1.39 Verhinderung von Ausgleichsströmen auf Schirmungen	10
M 1.40 Geeignete Aufstellung von Schutzschränken	10
M 1.41 Schutz gegen elektromagnetische Einstrahlung	10
M 1.43 Gesicherte Aufstellung aktiver Netzkomponenten	11
M 1.44 Geeignete Einrichtung eines häuslichen Arbeitsplatzes	11
M 1.45 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger	11
M 1.46 Einsatz von Diebstahl-Sicherungen	11
M 1.47 Eigener Brandabschnitt	12
M 1.48 Brandmeldeanlage im Rechenzentrum	12
M 1.49 Technische und organisatorische Vorgaben für das Rechenzentrum	12
M 1.50 Rauchschutz	12
M 1.51 Brandlastreduzierung	13
M 1.52 Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur	13
M 1.53 Videoüberwachung	13
M 1.54 Brandfrüherkennung/Löschtechnik	13
M 1.55 Perimeterschutz	13
M 1.56 Netzersatzanlage	14
M 1.57 Aktuelle Infrastruktur- und Baupläne	14
M 1.58 Technische und organisatorische Vorgaben für Serverräume	14
M 1.59 Geeignete Aufstellung von Speicher- und Archivsystemen	15
M 1.60 Geeignete Lagerung von Archivmedien	15
M 1.61 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes	15
M 1.62 Brandschutz von Patchfeldern	15

	Seite
M 1.63	Geeignete Aufstellung von Access Points 16
M 1.64	Vermeidung elektrischer Zündquellen 16
M 1.65	Erneuerung der IT-Verkabelung 16
M 1.66	Beachtung von Normen bei der IT-Verkabelung 16
M 1.67	Dimensionierung und Nutzung von Schranksystemen 17
M 1.68	Fachgerechte Installation 17
M 1.69	Verkabelung in Serverräumen 17
M 1.70	Zentrale unterbrechungsfreie Stromversorgung 17
M 1.71	Funktionstests der technischen Infrastruktur 18
M 1.72	Baumaßnahmen während des laufenden Betriebs 18
M 1.73	Schutz eines Rechenzentrums gegen unbefugten Zutritt 18
M 1.74	EMV-taugliche Stromversorgung 19
M 1.75	Branderkennung in Gebäuden 19
M 1.76	Geeignete Auswahl und Nutzung eines lokalen Arbeitsplatzes 19
M 1.77	Klimatisierung für Menschen 19
M 1.78	Sicherheitskonzept für die Gebäudenutzung 20
M 1.79	Bildung von Sicherheitszonen 20
M 1.80	Zutrittskontrollsystem und Berechtigungsmanagement 20
M 1.81	Materielle Sicherung von eingebetteten Systemen 20
M 2	Maßnahmenkatalog Organisation 21
M 2.1	Festlegung von Verantwortlichkeiten und Regelungen 21
M 2.2	Betriebsmittelverwaltung 21
M 2.3	Datenträgerverwaltung 21
M 2.4	Regelungen für Wartungs- und Reparaturarbeiten 22
M 2.5	Aufgabenverteilung und Funktionstrennung 22
M 2.6	Vergabe von Zutrittsberechtigungen 22
M 2.7	Vergabe von Zugangsberechtigungen 22
M 2.8	Vergabe von Zugriffsrechten 23
M 2.9	Nutzungsverbot nicht freigegebener Hard- und Software 23
M 2.10	Überprüfung des Hard- und Software-Bestandes 23
M 2.11	Regelung des Passwortgebrauchs 24
M 2.12	Betreuung und Beratung von IT-Benutzern 24
M 2.13	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln 24
M 2.14	Schlüsselverwaltung 25
M 2.15	Brandschutzbegehungen 25
M 2.16	Beaufsichtigung oder Begleitung von Fremdpersonen 25
M 2.17	Zutrittsregelung und -kontrolle 25
M 2.18	Kontrollgänge 25
M 2.19	Neutrale Dokumentation in den Verteilern 26
M 2.20	Kontrolle bestehender Verbindungen 26
M 2.21	Rauchverbot 26
M 2.22	Hinterlegen des Passwortes 26
M 2.23	Herausgabe einer PC-Richtlinie 27
M 2.24	Einführung eines IT-Passes 27
M 2.25	Dokumentation der Systemkonfiguration 27
M 2.26	Ernennung eines Administrators und eines Vertreters 28
M 2.27	Wartung einer TK-Anlage 28
M 2.28	Bereitstellung externer TK-Beratungskapazität 28
M 2.29	Bedienungsanleitung der TK-Anlage für die Benutzer 29
M 2.30	Regelung für die Einrichtung von Benutzern/Benutzergruppen 29
M 2.31	Dokumentation der zugelassenen Benutzer und Rechteprofile 29
M 2.32	Einrichtung einer eingeschränkten Benutzerumgebung 30
M 2.33	Aufteilung der Administrationstätigkeiten unter Unix 30
M 2.34	Dokumentation der Veränderungen an einem bestehenden System 30
M 2.35	Informationsbeschaffung über Sicherheitslücken des Systems 30
M 2.36	Geregelte Übergabe und Rücknahme eines tragbaren PC 31
M 2.37	Der aufgeräumte Arbeitsplatz 31
M 2.38	Aufteilung der Administrationstätigkeiten 31
M 2.39	Reaktion auf Verletzungen der Sicherheitsvorgaben 31
M 2.40	Rechtzeitige Beteiligung des Personal-/Betriebsrates 31
M 2.41	Verpflichtung der Mitarbeiter zur Datensicherung 32
M 2.42	Festlegung der möglichen Kommunikationspartner 32
M 2.43	Ausreichende Kennzeichnung der Datenträger beim Versand 32
M 2.44	Sichere Verpackung der Datenträger 32
M 2.45	Regelung des Datenträgeraustausches 33
M 2.46	Geeignetes Schlüsselmanagement 33

	Seite	
M 2.47	Ernennung eines Fax-Verantwortlichen	33
M 2.48	Festlegung berechtigter Faxbediener	34
M 2.49	Beschaffung geeigneter Faxgeräte	34
M 2.50	Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen	34
M 2.51	Fertigung von Kopien eingehender Faxsendungen	34
M 2.52	Versorgung und Kontrolle der Verbrauchsgüter	35
M 2.53	Abschalten des Faxgerätes außerhalb der Bürozeiten	35
M 2.59	Auswahl eines geeigneten Modems in der Beschaffung	35
M 2.60	Sichere Administration eines Modems	35
M 2.61	Regelung des Modem-Einsatzes	36
M 2.62	Software-Abnahme- und Freigabe-Verfahren	36
M 2.63	Einrichten der Zugriffsrechte	36
M 2.64	Kontrolle der Protokolldateien	36
M 2.65	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System	37
M 2.66	Beachtung des Beitrags der Zertifizierung für die Beschaffung	37
M 2.69	Einrichtung von Standardarbeitsplätzen	37
M 2.70	Entwicklung eines Konzepts für Sicherheitsgateways	37
M 2.71	Festlegung einer Policy für ein Sicherheitsgateway	38
M 2.73	Auswahl geeigneter Grundstrukturen für Sicherheitsgateways	38
M 2.74	Geeignete Auswahl eines Paketfilters	38
M 2.75	Geeignete Auswahl eines Application-Level-Gateways	38
M 2.76	Auswahl und Einrichtung geeigneter Filterregeln	39
M 2.77	Integration von Servern in das Sicherheitsgateway	39
M 2.78	Sicherer Betrieb eines Sicherheitsgateways	39
M 2.79	Festlegung der Verantwortlichkeiten im Bereich Standardsoftware	40
M 2.80	Erstellung eines Anforderungskatalogs für Standardsoftware	40
M 2.81	Vorauswahl eines geeigneten Standardsoftwareproduktes	40
M 2.82	Entwicklung eines Testplans für Standardsoftware	40
M 2.83	Testen von Standardsoftware	41
M 2.84	Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware	41
M 2.85	Freigabe von Standardsoftware	41
M 2.86	Sicherstellen der Integrität von Standardsoftware	42
M 2.87	Installation und Konfiguration von Standardsoftware	42
M 2.88	Lizenzverwaltung und Versionskontrolle von Standardsoftware	42
M 2.89	Deinstallation von Standardsoftware	43
M 2.90	Überprüfung der Lieferung	43
M 2.95	Beschaffung geeigneter Schutzschränke	43
M 2.96	Verschluss von Schutzschränken	43
M 2.97	Korrekturer Umgang mit Codeschlössern	44
M 2.106	Auswahl geeigneter ISDN-Karten in der Beschaffung	44
M 2.107	Dokumentation der ISDN-Karten-Konfiguration	44
M 2.108	Fernwartung der ISDN-Netzkoppelemente	44
M 2.109	Rechtevergabe für den Fernzugriff	44
M 2.110	Datenschutzaspekte bei der Protokollierung	45
M 2.111	Bereithalten von Handbüchern	45
M 2.112	Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution	45
M 2.113	Regelungen für Telearbeit	45
M 2.114	Informationsfluss zwischen Telearbeiter und Institution	46
M 2.115	Betreuungs- und Wartungskonzept für Telearbeitsplätze	46
M 2.116	Geregelte Nutzung der Kommunikationsmöglichkeiten bei Telearbeit	46
M 2.117	Erstellung eines Sicherheitskonzeptes für Telearbeit	46
M 2.122	Einheitliche E-Mail-Adressen	47
M 2.123	Auswahl eines Groupware- oder Mailproviders	47
M 2.124	Geeignete Auswahl einer Datenbank-Software	47
M 2.125	Installation und Konfiguration einer Datenbank	47
M 2.126	Erstellung eines Datenbanksicherheitskonzeptes	48
M 2.127	Inferenzprävention	48
M 2.128	Zugangskontrolle einer Datenbank	48
M 2.129	Zugriffskontrolle einer Datenbank	48
M 2.130	Gewährleistung der Datenbankintegrität	49
M 2.131	Aufteilung von Administrationstätigkeiten bei Datenbanksystemen	49
M 2.132	Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen	49
M 2.133	Kontrolle der Protokolldateien eines Datenbanksystems	49
M 2.134	Richtlinien für Datenbank-Anfragen	50
M 2.135	Gesicherte Datenübernahme in eine Datenbank	50
M 2.137	Beschaffung eines geeigneten Datensicherungssystems	50
M 2.138	Strukturierte Datenhaltung	51

	Seite
M 2.139 Ist-Aufnahme der aktuellen Netzsituation	51
M 2.140 Analyse der aktuellen Netzsituation	51
M 2.141 Entwicklung eines Netzkonzeptes	52
M 2.143 Entwicklung eines Netzmanagementkonzeptes	52
M 2.144 Verwendung von SNMP als Netzmanagement-Protokoll	52
M 2.145 Anforderungen an ein Netzmanagement-Tool	52
M 2.146 Sicherer Betrieb eines Netzmanagementsystems	53
M 2.154 Erstellung eines Sicherheitskonzeptes gegen Schadprogramme	53
M 2.157 Auswahl eines geeigneten Viren-Schutzprogramms	54
M 2.158 Meldung von Schadprogramm-Infektionen	54
M 2.159 Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen	54
M 2.160 Regelungen zum Schutz vor Schadprogrammen	55
M 2.161 Entwicklung eines Kryptokonzeptes	55
M 2.162 Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte	55
M 2.163 Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte	55
M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens	56
M 2.165 Auswahl eines geeigneten kryptographischen Produktes	56
M 2.166 Regelung des Einsatzes von Kryptomodulen	56
M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten	57
M 2.168 IT-System-Analyse vor Einführung eines Systemmanagementsystems	57
M 2.169 Entwickeln einer Systemmanagementstrategie	57
M 2.170 Anforderungen an ein Systemmanagementsystem	58
M 2.171 Geeignete Auswahl eines Systemmanagement-Produktes	58
M 2.172 Entwicklung eines Konzeptes für Webangebote	58
M 2.173 Festlegung einer Webserver-Sicherheitsstrategie	59
M 2.174 Sicherer Betrieb eines Webservers	59
M 2.175 Aufbau eines Webservers	60
M 2.176 Geeignete Auswahl eines Internet Service Providers	60
M 2.177 Sicherheit bei Umzügen	61
M 2.178 Erstellung einer Sicherheitsleitlinie für die Faxnutzung	61
M 2.179 Regelungen für den Faxserver-Einsatz	61
M 2.180 Einrichten einer Fax-Poststelle	62
M 2.181 Auswahl eines geeigneten Faxservers	62
M 2.188 Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	62
M 2.189 Sperrung des Mobiltelefons bei Verlust	63
M 2.190 Einrichtung eines Mobiltelefon-Pools	63
M 2.192 Erstellung einer Leitlinie zur Informationssicherheit	63
M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	64
M 2.195 Erstellung eines Sicherheitskonzeptes	64
M 2.197 Integration der Mitarbeiter in den Sicherheitsprozess	64
M 2.198 Sensibilisierung der Mitarbeiter für Informationssicherheit	65
M 2.199 Aufrechterhaltung der Informationssicherheit	65
M 2.200 Management-Berichte zur Informationssicherheit	65
M 2.201 Dokumentation des Sicherheitsprozesses	65
M 2.204 Verhinderung ungesicherter Netzzugänge	66
M 2.205 Übertragung und Abruf personenbezogener Daten	66
M 2.206 Planung des Einsatzes von Lotus Notes/Domino	66
M 2.207 Sicherheitskonzeption für Lotus Notes/Domino	66
M 2.212 Organisatorische Vorgaben für die Gebäudereinigung	67
M 2.213 Inspektion und Wartung der technischen Infrastruktur	67
M 2.214 Konzeption des IT-Betriebs	67
M 2.215 Fehlerbehandlung	68
M 2.216 Genehmigungsverfahren für IT-Komponenten	68
M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen	68
M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten	69
M 2.219 Kontinuierliche Dokumentation der Informationsverarbeitung	69
M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle	69
M 2.221 Änderungsmanagement	70
M 2.223 Sicherheitsvorgaben für die Nutzung von Standardsoftware	70
M 2.224 Vorbeugung gegen Schadprogramme	70
M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten	71
M 2.226 Regelungen für den Einsatz von Fremdpersonal	71
M 2.229 Planung des Active Directory	71
M 2.230 Planung der Active Directory-Administration	71
M 2.231 Planung der Gruppenrichtlinien unter Windows	72
M 2.232 Planung der Windows-CA-Struktur ab Windows 2000	72
M 2.234 Konzeption von Internet-PCs	72

	Seite
M 2.235 Richtlinien für die Nutzung von Internet-PCs	73
M 2.236 Planung des Einsatzes von Novell eDirectory	73
M 2.237 Planung der Partitionierung und Replikation im Novell eDirectory	73
M 2.238 Festlegung einer Sicherheitsrichtlinie für Novell eDirectory	74
M 2.239 Planung des Einsatzes von Novell eDirectory im Intranet	74
M 2.240 Planung des Einsatzes von Novell eDirectory im Extranet	74
M 2.241 Durchführung einer Anforderungsanalyse für den Telearbeitsplatz	75
M 2.242 Zielsetzung der elektronischen Archivierung	75
M 2.243 Entwicklung des Archivierungskonzepts	75
M 2.244 Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung	76
M 2.245 Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung	76
M 2.246 Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung	77
M 2.247 Planung des Einsatzes von Exchange und Outlook	77
M 2.249 Planung der Migration von Exchange-Systemen	77
M 2.250 Festlegung einer Outsourcing-Strategie	78
M 2.251 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben	78
M 2.252 Wahl eines geeigneten Outsourcing-Dienstleisters	78
M 2.253 Vertragsgestaltung mit dem Outsourcing-Dienstleister	79
M 2.254 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben	79
M 2.255 Sichere Migration bei Outsourcing-Vorhaben	79
M 2.256 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb	80
M 2.257 Überwachung der Speicherressourcen von Archivmedien	80
M 2.258 Konsistente Indizierung von Dokumenten bei der Archivierung	80
M 2.259 Einführung eines übergeordneten Dokumentenmanagements	81
M 2.260 Regelmäßige Revision des Archivierungsprozesses	81
M 2.261 Regelmäßige Marktbeobachtung von Archivsystemen	81
M 2.262 Regelung der Nutzung von Archivsystemen	82
M 2.263 Regelmäßige Aufbereitung von archivierten Datenbeständen	82
M 2.264 Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung	82
M 2.265 Geeigneter Einsatz digitaler Signaturen bei der Archivierung	83
M 2.266 Regelmäßige Erneuerung technischer Archivsystem-Komponenten	83
M 2.272 Einrichtung eines Internet-Redaktionsteams	83
M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	84
M 2.274 Vertretungsregelungen bei E-Mail-Nutzung	84
M 2.276 Funktionsweise eines Routers	84
M 2.277 Funktionsweise eines Switches	84
M 2.278 Typische Einsatzszenarien von Routern und Switches	85
M 2.279 Erstellung einer Sicherheitsrichtlinie für Router und Switches	85
M 2.280 Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches	85
M 2.281 Dokumentation der Systemkonfiguration von Routern und Switches	85
M 2.282 Regelmäßige Kontrolle von Routern und Switches	86
M 2.283 Software-Pflege auf Routern und Switches	86
M 2.284 Sichere Außerbetriebnahme von Routern und Switches	86
M 2.285 Festlegung von Standards für z/OS-Systemdefinitionen	86
M 2.286 Planung und Einsatz von zSeries-Systemen	87
M 2.287 Batch-Job-Planung für z/OS-Systeme	87
M 2.288 Erstellung von Sicherheitsrichtlinien für z/OS-Systeme	87
M 2.289 Einsatz restriktiver z/OS-Kennungen	88
M 2.290 Einsatz von RACF-Exits	88
M 2.291 Sicherheits-Berichtswesen und -Audits unter z/OS	88
M 2.292 Überwachung von z/OS-Systemen	89
M 2.293 Wartung von zSeries-Systemen	89
M 2.294 Synchronisierung von z/OS-Passwörtern und RACF-Kommandos	89
M 2.295 Systemverwaltung von z/OS-Systemen	90
M 2.296 Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren	90
M 2.297 Deinstallation von z/OS-Systemen	90
M 2.298 Verwaltung von Internet-Domännennamen	90
M 2.299 Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway	91
M 2.300 Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways	91
M 2.301 Outsourcing des Sicherheitsgateway	91
M 2.302 Sicherheitsgateways und Hochverfügbarkeit	92
M 2.303 Festlegung einer Strategie für den Einsatz von Smartphones, Tablets oder PDAs	92
M 2.304 Sicherheitsrichtlinien und Regelungen für die Nutzung von Smartphones, Tablets und PDAs	92
M 2.305 Geeignete Auswahl von Smartphones, Tablets oder PDAs	93
M 2.306 Verlustmeldung	93
M 2.307 Geordnete Beendigung eines Outsourcing- oder Cloud-Nutzungs-Verhältnisses	93
M 2.308 Auszug aus Gebäuden	93

	Seite
M 2.309 Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung	94
M 2.310 Geeignete Auswahl von Laptops	94
M 2.311 Planung von Schutzschranken	94
M 2.312 Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit	94
M 2.313 Sichere Anmeldung bei Internet-Diensten	95
M 2.314 Verwendung von hochverfügbaren Architekturen für Server	95
M 2.315 Planung des Servereinsatzes	95
M 2.316 Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server	95
M 2.317 Beschaffungskriterien für einen Server	95
M 2.318 Sichere Installation eines IT-Systems	96
M 2.319 Migration eines Servers	96
M 2.320 Geregelte Außerbetriebnahme eines Servers	96
M 2.321 Planung des Einsatzes von Client-Server-Netzen	96
M 2.322 Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz	97
M 2.323 Geregelte Außerbetriebnahme eines Clients	97
M 2.324 Einführung von Windows auf Clients ab Windows XP planen	97
M 2.325 Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP	98
M 2.326 Planung Gruppenrichtlinien für Clients ab Windows XP	98
M 2.327 SSicherheit beim Fernzugriff auf Clients ab Windows XP	99
M 2.328 Einsatz von Windows XP auf mobilen Rechnern	99
M 2.329 Einführung von Windows XP SP2	99
M 2.330 Regelmäßige Prüfung der Sicherheitsrichtlinien und ihrer Umsetzung bei Windows-Clients ab Windows XP	99
M 2.331 Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen	100
M 2.332 Einrichtung von Besprechungs-, Vortrags- und Schulungsräumen	100
M 2.333 Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen	100
M 2.334 Auswahl eines geeigneten Gebäudes	101
M 2.335 Festlegung der Sicherheitsziele und -strategie	101
M 2.336 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	101
M 2.337 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse	101
M 2.338 Erstellung von zielgruppengerechten Sicherheitsrichtlinien	102
M 2.339 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit	102
M 2.340 Beachtung rechtlicher Rahmenbedingungen	102
M 2.341 Planung des SAP Einsatzes	103
M 2.342 Planung von SAP Berechtigungen	103
M 2.343 Absicherung eines SAP Systems im Portal-Szenario	103
M 2.344 Sicherer Betrieb von SAP Systemen im Internet	104
M 2.345 Outsourcing eines SAP Systems	104
M 2.346 Nutzung der SAP Dokumentation	104
M 2.347 Regelmäßige Sicherheitsprüfungen für SAP Systeme	105
M 2.348 Sicherheit beim Customizing von SAP Systemen	105
M 2.349 Sicherheit bei der Software-Entwicklung für SAP Systeme	105
M 2.350 Aussonderung von SAP Systemen	106
M 2.351 Planung von Speicherlösungen	106
M 2.354 Einsatz einer hochverfügbaren SAN-Konfiguration	106
M 2.355 Auswahl von Lieferanten für eine Speicherlösung	107
M 2.356 Vertragsgestaltung mit Dienstleistern für Speicherlösungen	107
M 2.357 Aufbau eines Administrationsnetzes für Speichersysteme	107
M 2.358 Dokumentation der Systemeinstellungen von Speichersystemen	108
M 2.359 Überwachung und Verwaltung von Speicherlösungen	108
M 2.360 Sicherheits-Audits und Berichtswesen bei Speichersystemen	108
M 2.361 Außerbetriebnahme von Speicherlösungen	109
M 2.362 Auswahl einer geeigneten Speicherlösung	109
M 2.363 Schutz gegen SQL-Injection	109
M 2.364 Planung der Administration ab Windows 2003	110
M 2.365 Planung der Systemüberwachung unter Windows Server 2003	110
M 2.366 Nutzung von Sicherheitsvorlagen unter Windows Server 2003	111
M 2.367 Einsatz von Kommandos und Skripten ab Windows Server 2003	111
M 2.368 Umgang mit administrativen Vorlagen unter Windows ab Server 2003	111
M 2.369 Regelmäßige sicherheitsrelevante Wartungsmaßnahmen eines Windows Server 2003	112
M 2.370 Administration der Berechtigungen ab Windows Server 2003	112
M 2.371 Geregelte Deaktivierung und Löschung ungenutzter Konten	112
M 2.372 Planung des VoIP-Einsatzes	112
M 2.373 Erstellung einer Sicherheitsrichtlinie für VoIP	113
M 2.374 Umfang der Verschlüsselung von VoIP	113
M 2.375 Geeignete Auswahl von VoIP-Systemen	113
M 2.376 Trennung des Daten- und VoIP-Netzes	114
M 2.377 Sichere Außerbetriebnahme von VoIP-Komponenten	114

	Seite
M 2.378 System-Entwicklung	114
M 2.379 Software-Entwicklung durch Endbenutzer	115
M 2.380 Ausnahmegenehmigungen	115
M 2.381 Festlegung einer Strategie für die WLAN-Nutzung	115
M 2.382 Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung	116
M 2.383 Auswahl eines geeigneten WLAN-Standards	116
M 2.384 Auswahl geeigneter Kryptoverfahren für WLAN	116
M 2.385 Geeignete Auswahl von WLAN-Komponenten	117
M 2.386 Sorgfältige Planung notwendiger WLAN-Migrationsschritte	117
M 2.387 Installation, Konfiguration und Betreuung eines WLANs durch Dritte	117
M 2.388 Geeignetes WLAN-Schlüsselmanagement	118
M 2.389 Sichere Nutzung von Hotspots	118
M 2.390 Außerbetriebnahme von WLAN-Komponenten	118
M 2.391 Frühzeitige Information des Brandschutzbeauftragten	118
M 2.392 Modellierung von Virtualisierungsservern und virtuellen IT-Systemen	119
M 2.393 Regelung des Informationsaustausches	119
M 2.394 Prüfung elektrischer Anlagen	119
M 2.395 Anforderungsanalyse für die IT-Verkabelung	120
M 2.396 Vorgaben zur Dokumentation und Kennzeichnung der IT-Verkabelung	120
M 2.397 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten	120
M 2.398 Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten	120
M 2.399 Kriterien für die Beschaffung und geeignete Auswahl von Druckern, Kopierern und Multifunktionsgeräten	121
M 2.400 Sichere Außerbetriebnahme von Druckern, Kopierern und Multifunktionsgeräten	121
M 2.401 Umgang mit mobilen Datenträgern und Geräten	121
M 2.402 Zurücksetzen von Passwörtern	121
M 2.403 Planung des Einsatzes von Verzeichnisdiensten	122
M 2.404 Erstellung eines Sicherheitskonzeptes für Verzeichnisdienste	122
M 2.405 Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten	122
M 2.406 Geeignete Auswahl von Komponenten für Verzeichnisdienste	122
M 2.407 Planung der Administration von Verzeichnisdiensten	123
M 2.408 Planung der Migration von Verzeichnisdiensten	123
M 2.409 Planung der Partitionierung und Replikation im Verzeichnisdienst	123
M 2.410 Geregelte Außerbetriebnahme eines Verzeichnisdienstes	123
M 2.411 Trennung der Verwaltung von Diensten und Daten eines Active Directory	124
M 2.412 Schutz der Authentisierung beim Einsatz von Active Directory	124
M 2.413 Sicherer Einsatz von DNS für Active Directory	124
M 2.414 Computer-Viren-Schutz für Domänen-Controller	125
M 2.415 Durchführung einer VPN-Anforderungsanalyse	125
M 2.416 Planung des VPN-Einsatzes	125
M 2.417 Planung der technischen VPN-Realisierung	126
M 2.418 Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung	126
M 2.419 Geeignete Auswahl von VPN-Produkten	126
M 2.420 Auswahl eines Trusted-VPN-Dienstleisters	126
M 2.421 Planung des Patch- und Änderungsmanagementprozesses	127
M 2.422 Umgang mit Änderungsanforderungen	127
M 2.423 Festlegung der Verantwortlichkeiten für das Patch- und Änderungsmanagement	127
M 2.424 Sicherheitsrichtlinie zum Einsatz von Patch- und Änderungsmanagement-Werkzeugen	127
M 2.425 Geeignete Auswahl von Werkzeugen für das Patch- und Änderungsmanagement	128
M 2.426 Integration des Patch- und Änderungsmanagements in die Geschäftsprozesse	128
M 2.427 Abstimmung von Änderungsanforderungen	128
M 2.428 Skalierbarkeit beim Patch- und Änderungsmanagement	128
M 2.429 Erfolgsmessung von Änderungsanforderungen	129
M 2.430 Sicherheitsrichtlinien und Regelungen für den Informationsschutz unterwegs	129
M 2.431 Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen	129
M 2.432 Richtlinie für die Löschung und Vernichtung von Informationen	130
M 2.434 Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten	130
M 2.435 Auswahl geeigneter Aktenvernichter	130
M 2.436 Vernichtung von Datenträgern durch externe Dienstleister	130
M 2.437 Planung des Einsatzes eines Samba-Servers	131
M 2.438 Sicherer Einsatz externer Programme auf einem Samba-Server	131
M 2.439 Konzeption und Organisation des Anforderungsmanagements	131
M 2.440 Geeignete Auswahl einer Windows-Version für Clients ab Windows Vista	131
M 2.441 Kompatibilitätsprüfung von Software gegenüber Clients ab Windows Vista	132
M 2.442 Einsatz von Client-Betriebssystemen ab Windows Vista auf mobilen Systemen	132
M 2.443 Einführung von Windows Vista SP1	132
M 2.444 Einsatzplanung für virtuelle IT-Systeme	133
M 2.445 Auswahl geeigneter Hardware für Virtualisierungsumgebungen	133

	Seite
M 2.446	Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern 133
M 2.447	Sicherer Einsatz virtueller IT-Systeme 134
M 2.448	Überwachung der Funktion und Konfiguration virtueller Infrastrukturen 134
M 2.449	Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme 134
M 2.451	Planung des DNS-Einsatzes 135
M 2.452	Auswahl eines geeigneten DNS-Server-Produktes 135
M 2.453	Aussonderung von DNS-Servern 135
M 2.454	Planung des sicheren Einsatzes von Groupware-Systemen 135
M 2.455	Festlegung einer Sicherheitsrichtlinie für Groupware 136
M 2.456	Sichere Administration von Groupware-Systemen 136
M 2.457	Konzeption für die sichere Internet-Nutzung 136
M 2.458	Richtlinie für die Internet-Nutzung 136
M 2.460	Geregelte Nutzung von externen Dienstleistungen 137
M 2.461	Planung des sicheren Bluetooth-Einsatzes 137
M 2.463	Nutzung eines zentralen Pools an Bluetooth-Peripheriegeräten 137
M 2.464	Erstellung einer Sicherheitsrichtlinie zur Terminalserver-Nutzung 137
M 2.465	Analyse der erforderlichen Systemressourcen von Terminalservern 138
M 2.466	Migration auf eine Terminalserver-Architektur 138
M 2.467	Planung von regelmäßigen Neustartzyklen von Terminalservern 138
M 2.468	Lizenzierung von Software in Terminalserver-Umgebungen 138
M 2.469	Geregelte Außerbetriebnahme von Komponenten einer Terminalserver-Umgebung 139
M 2.470	Durchführung einer Anforderungsanalyse für TK-Anlagen 139
M 2.471	Planung des Einsatzes von TK-Anlagen 139
M 2.472	Erstellung einer Sicherheitsrichtlinie für TK-Anlagen 139
M 2.473	Auswahl von TK-Diensteanbietern 140
M 2.474	Sichere Außerbetriebnahme von TK-Komponenten 140
M 2.475	Vertragsgestaltung bei Bestellung eines externen IT-Sicherheitsbeauftragten 140
M 2.476	Konzeption für die sichere Internet-Anbindung 140
M 2.477	Planung einer virtuellen Infrastruktur 141
M 2.478	Planung des sicheren Einsatzes von Mac OS X 141
M 2.479	Planung der Sicherheitsrichtlinien von Mac OS X 141
M 2.480	Nutzung der Exchange- und Outlook-Dokumentation 141
M 2.481	Planung des Einsatzes von Exchange für Outlook Anywhere 142
M 2.482	Regelmäßige Sicherheitsprüfungen für Exchange-Systeme 142
M 2.483	Sicherheit beim Customizing von Exchange-Systemen 142
M 2.484	Planung von OpenLDAP 142
M 2.485	Auswahl von Backends für OpenLDAP 143
M 2.486	Dokumentation der Architektur von Webanwendungen und Web-Services 143
M 2.487	Entwicklung und Erweiterung von Anwendungen 143
M 2.489	Planung der Systemüberwachung unter Windows Server 2008 144
M 2.490	Planung des Einsatzes von Virtualisierung mit Hyper-V 144
M 2.491	Nutzung von Rollen und Sicherheitsvorlagen unter Windows Server 2008 144
M 2.492	Integration der Lotus Notes/Domino-Umgebung in die vorhandene Sicherheitsinfrastruktur 144
M 2.493	Lizenzmanagement und Lizenzierungsaspekte in der Beschaffung für Lotus Notes/Domino 145
M 2.494	Geeignete Auswahl von Komponenten für die Infrastruktur einer Lotus Notes/Domino-Umgebung 145
M 2.495	Aussonderung von Lotus Notes/Domino-Komponenten 145
M 2.496	Geregelte Außerbetriebnahme eines Protokollierungsservers 145
M 2.497	Erstellung eines Sicherheitskonzepts für die Protokollierung 146
M 2.498	Behandlung von Warn- und Fehlermeldungen 146
M 2.499	Planung der Protokollierung 146
M 2.500	Protokollierung von IT-Systemen 146
M 2.501	Datenschutzmanagement 147
M 2.502	Regelung der Verantwortlichkeiten im Bereich Datenschutz 147
M 2.503	Aspekte eines Datenschutzkonzeptes 147
M 2.504	Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten 147
M 2.505	Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten 148
M 2.506	Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten 148
M 2.507	Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten 148
M 2.508	Führung von Verfahrensverzeichnis und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten 148
M 2.509	Datenschutzrechtliche Freigabe 149
M 2.510	Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten 149
M 2.511	Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten 149
M 2.512	Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten 149

	Seite	
M 2.513	Dokumentation der datenschutzrechtlichen Zulässigkeit	150
M 2.514	Aufrechterhaltung des Datenschutzes im laufenden Betrieb	150
M 2.515	Datenschutzgerechte Löschung/Vernichtung	150
M 2.516	Bereitstellung von Sicherheitsrichtlinien für Cloud-Anwender	150
M 2.517	Vertragsgestaltung mit Dritt-Dienstleistern	151
M 2.518	Einsatz einer hochverfügbaren Firewall-Lösung	151
M 2.519	Geregelte Benutzer- und Berechtigungsverwaltung im Cloud Computing	151
M 2.520	Sicheres und vollständiges Löschen von Cloud-Anwenderdaten	151
M 2.521	Geregelte Provisionierung und De-Provisionierung von Cloud-Diensten	152
M 2.522	Berichtswesen und Kommunikation zu den Cloud-Anwendern	152
M 2.523	Sichere Automatisierung der Cloud-Regelprozesse	152
M 2.524	Modellierung von Cloud Management	153
M 2.525	Erstellung einer Sicherheitsrichtlinie für Speicherlösungen	153
M 2.526	Planung des Betriebs der Speicherlösung	153
M 2.527	Löschen in SAN-Umgebungen	153
M 2.528	Planung der sicheren Trennung von Mandanten in Speicherlösungen	154
M 2.530	Planung und Vorbereitung von Migrationen	154
M 2.531	Erarbeitung einer Sicherheitsrichtlinie für Web-Services	154
M 2.532	Anbieten von Web-Services für Dritte	155
M 2.533	Vertragliche Aspekte bei der Bereitstellung von Web-Services	155
M 2.534	Erstellung einer Cloud-Nutzungs-Strategie	155
M 2.535	Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung	156
M 2.536	Service-Definition für Cloud-Dienste durch den Anwender	156
M 2.537	Planung der sicheren Migration zu einem Cloud Service	156
M 2.538	Planung der sicheren Einbindung von Cloud Services	157
M 2.539	Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung	157
M 2.540	Sorgfältige Auswahl eines Cloud-Diensteanbieters	157
M 2.541	Vertragsgestaltung mit dem Cloud-Diensteanbieter	158
M 2.542	Sichere Migration zu einem Cloud Service	158
M 2.543	Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb	158
M 2.544	Auditierung bei Cloud-Nutzung	159
M 2.546	Analyse der Anforderungen an neue Anwendungen	159
M 2.547	Ermittlung und Dokumentation der Rechtsgrundlagen für Anwendungen	159
M 2.548	Erstellung eines Lastenheftes	159
M 2.549	Erstellung eines Mandantenkonzeptes	160
M 2.550	Geeignete Steuerung der Anwendungsentwicklung	160
M 2.551	Durchführung eines geeigneten und rechtskonformen Vergabeverfahrens	160
M 2.552	Erstellung eines Pflichtenheftes	160
M 2.553	Entwicklung eines Pflegekonzeptes für Anwendungen	161
M 2.554	Geeignete Vertragsgestaltung bei Beschaffung, Entwicklung und Betriebsunterstützung für Anwendungen	161
M 2.555	Entwicklung eines Authentisierungskonzeptes für Anwendungen	161
M 2.556	Planung und Umsetzung von Test und Freigabe von Anwendungen	161
M 2.557	Konzeption eines Schulungsprogramms zur Informationssicherheit	162
M 2.558	Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs	162
M 2.559	Beschaffung von Windows 8	162
M 2.560	Integration eines SOA-basierten Need-to-share-Konzepts in das Sicherheitsmanagement	162
M 2.562	Regelung des Einsatzes von eingebetteten Systemen	163
M 2.563	Auswahl einer vertrauenswürdigen Lieferanten- und Logistikkette sowie eines qualifizierten Herstellers für eingebettete Systeme	163
M 2.564	Beschaffungskriterien für eingebettete Systeme	163
M 2.565	Protokollierung sicherheitsrelevanter Ereignisse bei eingebetteten Systemen	164
M 2.566	Sichere Aussonderung eines eingebetteten Systems	164
M 2.567	Auswahl vertrauenswürdiger Entwicklungswerkzeuge	164
M 2.568	Testverfahren für Software	165
M 2.569	Definition von Rollen und Verantwortlichkeiten bei der Software-Entwicklung	165
M 2.570	Auswahl eines Vorgehensmodells zur Software-Entwicklung	165
M 2.571	Berücksichtigung von Compliance-Anforderungen für die Software-Entwicklung	165
M 2.572	Beschaffung von Werkzeugen zur Software-Entwicklung	166
M 2.573	Einhaltung einer sicheren Vorgehensweise bei der Software-Entwicklung	166
M 2.574	Ausführliche Dokumentation der Software-Entwicklung	166
M 2.575	Regelmäßige Sicherheitsaudits für die Software-Entwicklungsumgebung	166
M 2.576	Erstellung einer Sicherheitsrichtlinie für den Einsatz von lokalen Netzen	167
M 2.577	Auswahl geeigneter Kryptoverfahren für Netze	167
M 2.578	Installation, Konfiguration und Betreuung eines lokalen Netzes durch Dritte	167
M 2.579	Regelmäßige Audits des lokalen Netzes	167
M 2.580	Außerbetriebnahme von Netzkomponenten	168

	Seite
M 2.581	Aufbau eines Administrationsnetzes für das Netzmanagement 168
M 2.583	Geeignete Auswahl eines Netzmanagementsystems 168
M 2.584	Geregelte Außerbetriebnahme eines Netz- und Systemmanagement-Tools 168
M 2.585	Konzeption eines Identitäts- und Berechtigungsmanagements 169
M 2.586	Einrichtung, Änderung und Entzug von Berechtigungen 169
M 3	Maßnahmenkatalog Personal 171
M 3.1	Geregelte Einarbeitung/Einweisung neuer Mitarbeiter 171
M 3.2	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen 171
M 3.3	Vertretungsregelungen 171
M 3.4	Schulung vor Programmnutzung 171
M 3.5	Schulung zu Sicherheitsmaßnahmen 172
M 3.6	Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern 172
M 3.7	Anlaufstelle bei persönlichen Problemen 172
M 3.8	Vermeidung von Störungen des Betriebsklimas 173
M 3.9	Ergonomischer Arbeitsplatz 173
M 3.10	Auswahl eines vertrauenswürdigen Administrators und Vertreters 173
M 3.11	Schulung des Wartungs- und Administrationspersonals 173
M 3.12	Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne 174
M 3.13	Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen 174
M 3.14	Einweisung des Personals in den geregelten Ablauf der Informationsweitergabe und des Datenträgeraustausches 174
M 3.15	Informationen für alle Mitarbeiter über die Faxnutzung 174
M 3.17	Einweisung des Personals in die Modem-Benutzung 175
M 3.18	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung 175
M 3.20	Einweisung in die Bedienung von Schutzschranken 175
M 3.21	Sicherheitstechnische Einweisung der Telearbeiter 175
M 3.26	Einweisung des Personals in den sicheren Umgang mit IT 175
M 3.27	Schulung zur Active Directory-Verwaltung 176
M 3.28	Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen 176
M 3.29	Schulung zur Administration von Novell eDirectory 176
M 3.30	Schulung zum Einsatz von Novell eDirectory Clientsoftware 176
M 3.31	Schulung zur Systemarchitektur und Sicherheit von Exchange-Systemen für Administratoren 177
M 3.32	Schulung zu Sicherheitsmechanismen von Outlook für Benutzer 177
M 3.33	Sicherheitsüberprüfung von Mitarbeitern 177
M 3.34	Einweisung in die Administration des Archivsystems 177
M 3.35	Einweisung der Benutzer in die Bedienung des Archivsystems 178
M 3.38	Administratorenschulung für Router und Switches 178
M 3.42	Schulung des z/OS-Bedienungspersonals 178
M 3.43	Schulung der Administratoren des Sicherheitsgateways 178
M 3.44	Sensibilisierung des Managements für Informationssicherheit 179
M 3.45	Planung von Schulungsinhalten zur Informationssicherheit 179
M 3.46	Ansprechpartner zu Sicherheitsfragen 179
M 3.47	Durchführung von Planspielen zur Informationssicherheit 179
M 3.48	Auswahl von Trainern oder Schulungsanbietern 180
M 3.49	Schulung zur Vorgehensweise nach IT-Grundschutz 180
M 3.50	Auswahl von Personal 180
M 3.51	Geeignetes Konzept für Personaleinsatz und -qualifizierung 180
M 3.52	Schulung zu SAP Systemen 181
M 3.54	Schulung der Administratoren des Speichersystems 181
M 3.55	Vertraulichkeitsvereinbarungen 181
M 3.56	Schulung der Administratoren für die Nutzung von VoIP 181
M 3.58	Einführung in WLAN-Grundbegriffe 182
M 3.59	Schulung zum sicheren WLAN-Einsatz 182
M 3.60	Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten 182
M 3.62	Schulung zur Administration von Verzeichnisdiensten 182
M 3.63	Schulung der Benutzer zur Authentisierung mit Hilfe von Verzeichnisdiensten 183
M 3.67	Einweisung aller Mitarbeiter über Methoden zur Löschung oder Vernichtung von Daten 183
M 3.68	Schulung der Administratoren eines Samba-Servers 183
M 3.71	Schulung der Administratoren virtueller Umgebungen 184
M 3.73	Schulung der Administratoren eines DNS-Servers 184
M 3.74	Schulung zur Systemarchitektur und Sicherheit von Groupware-Systemen für Administratoren 184
M 3.75	Schulung zu Sicherheitsmechanismen von Groupware-Clients für Benutzer 184
M 3.76	Einweisung der Benutzer in den Einsatz von Groupware und E-Mail 185
M 3.77	Sensibilisierung zur sicheren Internet-Nutzung 185
M 3.78	Korrektes Auftreten im Internet 185
M 3.80	Sensibilisierung für die Nutzung von Bluetooth 185

	Seite
M 3.81 Schulung zum sicheren Terminalserver-Einsatz	185
M 3.82 Schulung zur sicheren Nutzung von TK-Anlagen	186
M 3.83 Analyse sicherheitsrelevanter personeller Faktoren	186
M 3.86 Schulung der Administratoren von OpenLDAP	186
M 3.88 Zielgruppenspezifische Schulungen zu Lotus Notes/Domino	186
M 3.89 Schulung zur Administration der Protokollierung	187
M 3.91 Schulung der Administratoren von Cloud-Infrastrukturen	187
M 3.93 Analyse der Zielgruppen für Sensibilisierungs- und Schulungsprogramme	187
M 3.94 Messung und Auswertung des Lernerfolgs	187
M 3.95 Lernstoffsicherung	187
M 3.96 Unterstützung des Managements für Sensibilisierung und Schulung	188
M 3.97 Schulung des Projektteams für die Software-Entwicklung	188
M 3.98 Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und -mechanismen	188
M 4 Maßnahmenkatalog Hard- und Software	189
M 4.1 Passwortschutz für IT-Systeme	189
M 4.2 Bildschirmsperre	189
M 4.3 Einsatz von Viren-Schutzprogrammen	189
M 4.4 Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern	190
M 4.5 Protokollierung bei TK-Anlagen	190
M 4.6 Revision der TK-Anlagenkonfiguration	190
M 4.7 Änderung voreingestellter Passwörter	190
M 4.9 Einsatz der Sicherheitsmechanismen von X-Window	191
M 4.10 Schutz der TK-Endgeräte	191
M 4.11 Absicherung der TK-Anlagen-Schnittstellen	191
M 4.13 Sorgfältige Vergabe von IDs	191
M 4.14 Obligatorischer Passwortschutz unter Unix	192
M 4.15 Gesichertes Login	192
M 4.16 Zugangsbeschränkungen für Benutzer-Kennungen und/oder Terminals	192
M 4.17 Sperren und Löschen nicht benötigter Accounts und Terminals	192
M 4.18 Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus	193
M 4.19 Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen	193
M 4.20 Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen	193
M 4.21 Verhinderung des unautorisierten Erlangens von Administratorrechten	194
M 4.22 Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System	194
M 4.23 Sicherer Aufruf ausführbarer Dateien	194
M 4.24 Sicherstellung einer konsistenten Systemverwaltung	195
M 4.25 Einsatz der Protokollierung im Unix-System	195
M 4.26 Regelmäßiger Sicherheitscheck des Unix-Systems	195
M 4.27 Zugriffsschutz am Laptop	195
M 4.28 Software-Reinstallation bei Benutzerwechsel eines Laptops	196
M 4.29 Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme	196
M 4.30 Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen	196
M 4.31 Sicherstellung der Energieversorgung im mobilen Einsatz	196
M 4.32 Physikalisches Löschen der Datenträger vor und nach Verwendung	197
M 4.33 Einsatz eines Viren- Suchprogramms bei Datenträgeraustausch und Datenübertragung	197
M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	197
M 4.35 Verifizieren der zu übertragenden Daten vor Versand	197
M 4.36 Sperren bestimmter Faxempfänger-Rufnummern	198
M 4.37 Sperren bestimmter Absender-Faxnummern	198
M 4.40 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras	198
M 4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme	198
M 4.42 Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung	199
M 4.43 Faxgerät mit automatischer Eingangskuvrierung	199
M 4.47 Protokollierung der Sicherheitsgateway-Aktivitäten	199
M 4.48 Passwortschutz unter Windows-Systemen	200
M 4.49 Absicherung des Boot-Vorgangs für ein Windows-System	200
M 4.52 Geräteschutz unter NT-basierten Windows-Systemen	200
M 4.56 Sicheres Löschen unter Windows-Betriebssystemen	201
M 4.57 Deaktivieren der automatischen CD-ROM-Erkennung	201
M 4.59 Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten	201
M 4.60 Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten	201
M 4.61 Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten	202
M 4.62 Einsatz eines D-Kanal-Filters	202
M 4.63 Sicherheitstechnische Anforderungen an den Telearbeitsrechner	202
M 4.64 Verifizieren der zu übertragenden Daten vor Weitergabe/Beseitigung von Restinformationen	202
M 4.65 Test neuer Hard- und Software	203

	Seite	
M 4.67	Sperren und Löschen nicht benötigter Datenbank-Accounts	203
M 4.68	Sicherstellung einer konsistenten Datenbankverwaltung	203
M 4.69	Regelmäßiger Sicherheitscheck der Datenbank	203
M 4.70	Durchführung einer Datenbanküberwachung	204
M 4.71	Restriktive Handhabung von Datenbank-Links	204
M 4.72	Datenbank-Verschlüsselung	204
M 4.73	Festlegung von Obergrenzen für selektierbare Datensätze	204
M 4.75	Schutz der Registry unter Windows-Systemen	204
M 4.78	Sorgfältige Durchführung von Konfigurationsänderungen	205
M 4.79	Sichere Zugriffsmechanismen bei lokaler Administration	205
M 4.80	Sichere Zugriffsmechanismen bei Fernadministration	205
M 4.81	Audit und Protokollierung der Aktivitäten im Netz	206
M 4.82	Sichere Konfiguration der aktiven Netzkomponenten	206
M 4.83	Update/Upgrade von Soft- und Hardware im Netzbereich	206
M 4.84	Nutzung der BIOS-Sicherheitsmechanismen	207
M 4.85	Geeignetes Schnittstellendesign bei Kryptomodulen	207
M 4.86	Sichere Rollenteilung und Konfiguration der Kryptomodule	207
M 4.87	Physikalische Sicherheit von Kryptomodulen	207
M 4.88	Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen	208
M 4.89	Abstrahlsicherheit	208
M 4.91	Sichere Installation eines Systemmanagementsystems	208
M 4.92	Sicherer Betrieb eines Systemmanagementsystems	209
M 4.93	Regelmäßige Integritätsprüfung	209
M 4.94	Schutz der Webserver-Dateien	210
M 4.95	Minimales Betriebssystem	210
M 4.96	Abschaltung von DNS	210
M 4.97	Ein Dienst pro Server	211
M 4.98	Kommunikation durch Paketfilter auf Minimum beschränken	211
M 4.99	Schutz gegen nachträgliche Veränderungen von Informationen	211
M 4.100	Sicherheitsgateways und aktive Inhalte	211
M 4.101	Sicherheitsgateways und Verschlüsselung	211
M 4.105	Erste Maßnahmen nach einer Unix-Standardinstallation	212
M 4.106	Aktivieren der Systemprotokollierung	212
M 4.107	Nutzung von Hersteller- und Entwickler-Ressourcen	212
M 4.109	Software-Reinstallation bei Arbeitsplatzrechnern	213
M 4.113	Nutzung eines Authentisierungsservers bei Remote-Access-VPNs	213
M 4.114	Nutzung der Sicherheitsmechanismen von Mobiltelefonen	213
M 4.115	Sicherstellung der Energieversorgung von Mobiltelefonen	213
M 4.116	Sichere Installation von Lotus Notes/Domino	214
M 4.128	Sicherer Betrieb der Lotus Notes/Domino-Umgebung	214
M 4.132	Überwachung der Lotus Notes/Domino-Umgebung	215
M 4.133	Geeignete Auswahl von Authentifikationsmechanismen	215
M 4.134	Wahl geeigneter Datenformate	215
M 4.135	Restriktive Vergabe von Zugriffsrechten auf Systemdateien	216
M 4.138	Konfiguration von Windows Server als Domänen-Controller	216
M 4.146	Sicherer Betrieb von Windows Client-Betriebssystemen	216
M 4.147	Sichere Nutzung von EFS unter Windows	217
M 4.148	Überwachung eines Windows 2000/XP Systems	217
M 4.149	Datei- und Freigabeberechtigungen unter Windows	217
M 4.151	Sichere Installation von Internet-PCs	218
M 4.152	Sicherer Betrieb von Internet-PCs	218
M 4.153	Sichere Installation von Novell eDirectory	218
M 4.154	Sichere Installation der Novell eDirectory Clientsoftware	218
M 4.155	Sichere Konfiguration von Novell eDirectory	219
M 4.156	Sichere Konfiguration der Novell eDirectory Clientsoftware	219
M 4.157	Einrichten von Zugriffsberechtigungen auf Novell eDirectory	219
M 4.158	Einrichten des LDAP-Zugriffs auf Novell eDirectory	219
M 4.159	Sicherer Betrieb von Novell eDirectory	220
M 4.160	Überwachen von Novell eDirectory	220
M 4.161	Sichere Installation von Exchange-Systemen	220
M 4.162	Sichere Konfiguration von Exchange-Servern	220
M 4.163	Zugriffsrechte auf Exchange-Objekte	221
M 4.165	Sichere Konfiguration von Outlook	221
M 4.166	Sicherer Betrieb von Exchange-Systemen	221
M 4.168	Auswahl eines geeigneten Archivsystems	221
M 4.169	Verwendung geeigneter Archivmedien	222
M 4.170	Auswahl geeigneter Datenformate für die Archivierung von Dokumenten	222

	Seite	
M 4.171	Schutz der Integrität der Index-Datenbank von Archivsystemen	222
M 4.172	Protokollierung der Archivzugriffe	223
M 4.173	Regelmäßige Funktions- und Recoverytests bei der Archivierung	223
M 4.176	Auswahl einer Authentisierungsmethode für Webangebote	223
M 4.177	Sicherstellung der Integrität und Authentizität von Softwarepaketen	224
M 4.198	Installation einer Applikation in einem chroot Käfig	224
M 4.199	Vermeidung problematischer Dateiformate	224
M 4.200	Umgang mit USB-Speichermedien	224
M 4.201	Sichere lokale Grundkonfiguration von Routern und Switches	225
M 4.202	Sichere Netz-Grundkonfiguration von Routern und Switches	226
M 4.203	Konfigurations-Checkliste für Router und Switches	226
M 4.204	Sichere Administration von Routern und Switches	226
M 4.205	Protokollierung bei Routern und Switches	227
M 4.206	Sicherung von Switch-Ports	227
M 4.207	Einsatz und Sicherung systemnaher z/OS-Terminals	227
M 4.208	Absichern des Start-Vorgangs von z/OS-Systemen	228
M 4.209	Sichere Grundkonfiguration von z/OS-Systemen	228
M 4.210	Sicherer Betrieb des z/OS-Betriebssystems	229
M 4.211	Einsatz des z/OS-Sicherheitssystems RACF	229
M 4.212	Absicherung von Linux für zSeries	230
M 4.213	Absichern des Login-Vorgangs unter z/OS	230
M 4.214	Datenträgerverwaltung unter z/OS-Systemen	230
M 4.215	Absicherung sicherheitskritischer z/OS-Dienstprogramme	231
M 4.216	Festlegung der Systemgrenzen von z/OS	231
M 4.217	Workload Management für z/OS-Systeme	231
M 4.218	Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen	232
M 4.219	Lizenzschlüssel-Management für z/OS-Software	232
M 4.220	Absicherung von Unix System Services bei z/OS-Systemen	232
M 4.221	Parallel-Sysplex unter z/OS	233
M 4.222	Festlegung geeigneter Einstellungen von Sicherheitsproxies	233
M 4.223	Integration von Proxy-Servern in das Sicherheitsgateway	233
M 4.224	Integration von VPN-Komponenten in ein Sicherheitsgateway	234
M 4.225	Einsatz eines Protokollierungsservers in einem Sicherheitsgateway	234
M 4.226	Integration von Virenscannern in ein Sicherheitsgateway	234
M 4.227	Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation	234
M 4.228	Nutzung der Sicherheitsmechanismen von Smartphones, Tablets und PDAs	235
M 4.229	Sicherer Betrieb von Smartphones, Tablets und PDAs	235
M 4.230	Zentrale Administration von Smartphones, Tablets und PDAs	235
M 4.231	Einsatz zusätzlicher Sicherheitswerkzeuge für Smartphones, Tablets oder PDAs	235
M 4.232	Sichere Nutzung von Zusatzspeicherkarten	235
M 4.234	Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern	236
M 4.235	Abgleich der Datenbestände von Laptops	236
M 4.236	Zentrale Administration von Laptops	236
M 4.237	Sichere Grundkonfiguration eines IT-Systems	236
M 4.238	Einsatz eines lokalen Paketfilters	237
M 4.239	Sicherer Betrieb eines Servers	237
M 4.240	Einrichten einer Testumgebung für einen Server	237
M 4.241	Sicherer Betrieb von Clients	237
M 4.242	Einrichten einer Referenzinstallation für Clients	238
M 4.243	Verwaltungswerkzeuge unter Windows Client-Betriebssystemen	238
M 4.244	Sichere Systemkonfiguration von Windows Client-Betriebssystemen	238
M 4.245	Basiseinstellungen für Windows Group Policy Objects	239
M 4.246	Konfiguration der Systemdienste auf Clients ab Windows XP	239
M 4.247	Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista	239
M 4.248	Sichere Installation von Windows Client-Betriebssystemen	240
M 4.249	Windows Client-Systeme aktuell halten	240
M 4.250	Auswahl eines zentralen, netzbasierten Authentisierungsdienstes	240
M 4.251	Arbeiten mit fremden IT-Systemen	241
M 4.252	Sichere Konfiguration von Schulungsrechnern	241
M 4.254	Sicherer Einsatz von drahtlosen Tastaturen und Mäusen	241
M 4.255	Nutzung von IrDA-Schnittstellen	241
M 4.256	Sichere Installation von SAP Systemen	242
M 4.257	Absicherung des SAP Installationsverzeichnisses auf Betriebssystemebene	242
M 4.258	Sichere Konfiguration des SAP ABAP-Stacks	243
M 4.259	Sicherer Einsatz der ABAP-Stack Benutzerverwaltung	243
M 4.260	Berechtigungsverwaltung für SAP Systeme	244
M 4.261	Sicherer Umgang mit kritischen SAP Berechtigungen	244

	Seite	
M 4.262	Konfiguration zusätzlicher SAP Berechtigungsprüfungen	244
M 4.263	Absicherung von SAP Destinationen	245
M 4.264	Einschränkung von direkten Tabellenveränderungen in SAP Systemen	245
M 4.265	Sichere Konfiguration der Batch-Verarbeitung im SAP System	245
M 4.266	Sichere Konfiguration des SAP Java-Stacks	246
M 4.267	Sicherer Einsatz der SAP Java-Stack Benutzerverwaltung	246
M 4.268	Sichere Konfiguration der SAP Java-Stack Berechtigungen	246
M 4.269	Sichere Konfiguration der SAP System Datenbank	247
M 4.270	SAP Protokollierung	247
M 4.271	Virenschutz für SAP Systeme	247
M 4.272	Sichere Nutzung des SAP Transportsystems	248
M 4.273	Sichere Nutzung der SAP Java-Stack Software-Verteilung	248
M 4.274	Sichere Grundkonfiguration von Speichersystemen	248
M 4.275	Sicherer Betrieb einer Speicherlösung	249
M 4.276	Planung des Einsatzes von Windows Server 2003	249
M 4.277	Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows-Servern	250
M 4.278	Sichere Nutzung von EFS unter Windows Server 2003	250
M 4.279	Erweiterte Sicherheitsaspekte für Windows Server 2003	250
M 4.280	Sichere Basiskonfiguration ab Windows Server 2003	251
M 4.281	Sichere Installation und Bereitstellung von Windows Server 2003	251
M 4.282	Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003	252
M 4.283	Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003	252
M 4.284	Umgang mit Diensten ab Windows Server 2003	252
M 4.285	Deinstallation nicht benötigter Client-Funktionen von Windows Server 2003	252
M 4.286	Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003	253
M 4.287	Sichere Administration der VoIP-Middleware	253
M 4.288	Sichere Administration von VoIP-Endgeräten	254
M 4.289	Einschränkung der Erreichbarkeit über VoIP	254
M 4.290	Anforderungen an ein Sicherheitsgateway für den Einsatz von VoIP	254
M 4.291	Sichere Konfiguration der VoIP-Middleware	255
M 4.292	Protokollierung bei VoIP	255
M 4.293	Sicherer Betrieb von Hotspots	256
M 4.294	Sichere Konfiguration der Access Points	256
M 4.295	Sichere Konfiguration der WLAN-Clients	257
M 4.296	Einsatz einer geeigneten WLAN-Management-Lösung	257
M 4.297	Sicherer Betrieb der WLAN-Komponenten	258
M 4.298	Regelmäßige Audits der WLAN-Komponenten	258
M 4.299	Authentisierung bei Druckern, Kopierern und Multifunktionsgeräten	258
M 4.300	Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten	259
M 4.301	Beschränkung der Zugriffe auf Drucker, Kopierer und Multifunktionsgeräte	259
M 4.302	Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten	259
M 4.303	Einsatz von netzfähigen Dokumentenscannern	259
M 4.305	Einsatz von Speicherbeschränkungen (Quotas)	260
M 4.306	Umgang mit Passwort-Speicher-Tools	260
M 4.307	Sichere Konfiguration von Verzeichnisdiensten	260
M 4.308	Sichere Installation von Verzeichnisdiensten	260
M 4.309	Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste	261
M 4.310	Einrichtung des LDAP-Zugriffs auf Verzeichnisdienste	261
M 4.311	Sicherer Betrieb von Verzeichnisdiensten	261
M 4.312	Überwachung von Verzeichnisdiensten	261
M 4.313	Bereitstellung von sicheren Domänen-Controllern	262
M 4.314	Sichere Richtlinieneinstellungen für Domänen und Domänen-Controller	262
M 4.315	Aufrechterhaltung der Betriebssicherheit von Active Directory	262
M 4.316	Überwachung der Active Directory Infrastruktur	263
M 4.317	Sichere Migration von Windows Verzeichnisdiensten	263
M 4.318	Umsetzung sicherer Verwaltungsmethoden für Active Directory	263
M 4.319	Sichere Installation von VPN-Endgeräten	264
M 4.320	Sichere Konfiguration eines VPNs	264
M 4.321	Sicherer Betrieb eines VPNs	265
M 4.322	Sperrung nicht mehr benötigter VPN-Zugänge	265
M 4.323	Synchronisierung innerhalb des Patch- und Änderungsmanagements	265
M 4.324	Konfiguration von Autoupdate-Mechanismen beim Patch- und Änderungsmanagement	266
M 4.325	Löschen von Auslagerungsdateien	266
M 4.326	Sicherstellung der NTFS-Eigenschaften auf einem Samba-Dateiserver	266
M 4.327	Überprüfung der Integrität und Authentizität der Samba-Pakete und -Quellen	266
M 4.328	Sichere Grundkonfiguration eines Samba-Servers	267
M 4.329	Sicherer Einsatz von Kommunikationsprotokollen beim Einsatz eines Samba-Servers	267

	Seite
M 4.330 Sichere Installation eines Samba-Servers	267
M 4.331 Sichere Konfiguration des Betriebssystems für einen Samba-Server	268
M 4.332 Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server	268
M 4.333 Sichere Konfiguration von Winbind unter Samba	268
M 4.334 SMB Message Signing und Samba	269
M 4.335 Sicherer Betrieb eines Samba-Servers	269
M 4.336 Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag	269
M 4.337 Einsatz von BitLocker Drive Encryption	270
M 4.338 Einsatz von File und Registry Virtualization bei Clients ab Windows Vista	270
M 4.339 Verhindern unautorisierter Nutzung von Wechselmedien unter Windows-Clients ab Windows Vista	270
M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista	271
M 4.341 Integritätsschutz ab Windows Vista	271
M 4.342 Aktivierung des Last Access Zeitstempels ab Windows Vista	271
M 4.343 Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag	272
M 4.344 Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008	272
M 4.345 Schutz vor unerwünschten Informationsabflüssen	272
M 4.346 Sichere Konfiguration virtueller IT-Systeme	273
M 4.347 Deaktivierung von Snapshots virtueller IT-Systeme	273
M 4.348 Zeitsynchronisation in virtuellen IT-Systemen	273
M 4.349 Sicherer Betrieb von virtuellen Infrastrukturen	274
M 4.350 Sichere Grundkonfiguration eines DNS-Servers	274
M 4.351 Absicherung von Zonentransfers	274
M 4.352 Absicherung von dynamischen DNS-Updates	274
M 4.353 Einsatz von DNSSEC	275
M 4.354 Überwachung eines DNS-Servers	275
M 4.355 Berechtigungsverwaltung für Groupware-Systeme	275
M 4.356 Sichere Installation von Groupware-Systemen	275
M 4.357 Sicherer Betrieb von Groupware-Systemen	276
M 4.358 Protokollierung von Groupware-Systemen	276
M 4.359 Überblick über Komponenten eines Webservers	276
M 4.360 Sichere Konfiguration eines Webservers	276
M 4.362 Sichere Konfiguration von Bluetooth	277
M 4.363 Sicherer Betrieb von Bluetooth-Geräten	277
M 4.364 Regelungen für die Aussonderung von Bluetooth-Geräten	277
M 4.365 Nutzung eines Terminalservers als grafische Firewall	277
M 4.366 Sichere Konfiguration von beweglichen Benutzerprofilen in Terminalserver-Umgebungen	278
M 4.367 Sichere Verwendung von Client-Applikationen für Terminalserver	278
M 4.368 Regelmäßige Audits der Terminalserver-Umgebung	278
M 4.369 Sicherer Betrieb eines Anrufbeantworters	278
M 4.370 Einsatz von Anubis unter Unix	279
M 4.371 Konfiguration von Mac OS X Clients	279
M 4.372 Einsatz von FileVault unter Mac OS X	279
M 4.373 Deaktivierung nicht benötigter Hardware unter Mac OS X	280
M 4.374 Zugriffsschutz der Benutzerkonten unter Mac OS X	280
M 4.375 Einsatz der Sandbox-Funktion unter Mac OS X	280
M 4.376 Festlegung von Passwortrichtlinien unter Mac OS X	280
M 4.377 Überprüfung der Signaturen von Mac OS X Anwendungen	281
M 4.378 Einschränkung der Programmzugriffe unter Mac OS X	281
M 4.379 Sichere Datenhaltung und sicherer Transport unter Mac OS X	281
M 4.380 Einsatz von Apple-Software-Restore unter Mac OS X	281
M 4.381 Verschlüsselung von Exchange-System-Datenbanken	281
M 4.382 Auswahl und Prüfung der OpenLDAP-Installationspakete	282
M 4.383 Sichere Installation von OpenLDAP	282
M 4.384 Sichere Konfiguration von OpenLDAP	282
M 4.385 Konfiguration der durch OpenLDAP verwendeten Datenbank	282
M 4.386 Einschränkung von Attributen bei OpenLDAP	283
M 4.387 Sichere Vergabe von Zugriffsrechten auf OpenLDAP	283
M 4.388 Sichere Authentisierung gegenüber OpenLDAP	283
M 4.389 Partitionierung und Replikation bei OpenLDAP	283
M 4.390 Sichere Aktualisierung von OpenLDAP	284
M 4.391 Sicherer Betrieb von OpenLDAP	284
M 4.392 Authentisierung bei Webanwendungen	284
M 4.393 Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services	285
M 4.394 Session-Management bei Webanwendungen und Web-Services	285
M 4.395 Fehlerbehandlung durch Webanwendungen und Web-Services	286
M 4.396 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen	286
M 4.397 Protokollierung sicherheitsrelevanter Ereignisse von Webanwendungen und Web-Services	286

	Seite
M 4.398 Sichere Konfiguration von Webanwendungen	287
M 4.399 Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen	287
M 4.400 Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services	288
M 4.401 Schutz vertraulicher Daten bei Webanwendungen	288
M 4.402 Zugriffskontrolle bei Webanwendungen	289
M 4.403 Verhinderung von Cross-Site Request Forgery (CSRF, XSRF, Session Riding)	289
M 4.404 Sicherer Entwurf der Logik von Webanwendungen	289
M 4.405 Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services	290
M 4.406 Verhinderung von Clickjacking	290
M 4.407 Protokollierung beim Einsatz von OpenLDAP	290
M 4.409 Beschaffung von Windows Server 2008	290
M 4.410 Einsatz von Netzwerkzugriffsschutz unter Windows	291
M 4.411 Sichere Nutzung von DirectAccess unter Windows	291
M 4.412 Sichere Migration von Windows Server 2003 auf Server 2008	291
M 4.413 Sicherer Einsatz von Virtualisierung mit Hyper-V	292
M 4.415 Sicherer Betrieb der biometrischen Authentisierung unter Windows	292
M 4.416 Einsatz von Windows Server Core	292
M 4.417 Patch-Management mit WSUS ab Windows Server 2008	293
M 4.418 Planung des Einsatzes von Windows Server 2008	293
M 4.419 Anwendungssteuerung ab Windows 7 mit AppLocker	293
M 4.420 Sicherer Einsatz des Wartungszentrums unter Windows 7	294
M 4.421 Absicherung der Windows PowerShell	294
M 4.422 Nutzung von BitLocker To Go ab Windows 7	294
M 4.423 Verwendung der Heimnetzgruppen-Funktion ab Windows 7	295
M 4.424 Sicherer Einsatz älterer Software ab Windows 7	295
M 4.425 Verwendung der Tresor- und Cardspace-Funktion unter Windows 7	295
M 4.426 Archivierung für die Lotus Notes/Domino-Umgebung	296
M 4.427 Sicherheitsrelevante Protokollierung und Auswertung für Lotus Notes/Domino	296
M 4.428 Audit der Lotus Notes/Domino-Umgebung	296
M 4.429 Sichere Konfiguration von Lotus Notes/Domino	296
M 4.430 Analyse von Protokolldaten	297
M 4.431 Auswahl und Verarbeitung relevanter Informationen für die Protokollierung	297
M 4.432 Sichere Konfiguration von Serverdiensten	297
M 4.433 Einsatz von Datenträgerverschlüsselung	298
M 4.434 Sicherer Einsatz von Appliances	298
M 4.435 Selbstverschlüsselnde Festplatten	298
M 4.436 Planung der Ressourcen für Cloud-Dienste	299
M 4.437 Planung von Cloud-Dienstprofilen	299
M 4.438 Auswahl von Cloud-Komponenten	300
M 4.439 Virtuelle Sicherheitsgateways (Firewalls) in Clouds	300
M 4.440 Verschlüsselte Speicherung von Cloud-Anwenderdaten	300
M 4.441 Multifaktor-Authentisierung für den Cloud-Benutzerzugriff	301
M 4.442 Zentraler Schutz vor Schadprogrammen in der Cloud-Infrastruktur	301
M 4.443 Protokollierung und Monitoring von Ereignissen in der Cloud-Infrastruktur	301
M 4.444 Patchmanagement für Cloud-Komponenten	301
M 4.445 Durchgängige Mandantentrennung von Cloud-Diensten	302
M 4.447 Sicherstellung der Integrität der SAN-Fabric	302
M 4.448 Einsatz von Verschlüsselung für Speicherlösungen	302
M 4.449 Einführung eines Zonenkonzeptes	302
M 4.450 Absicherung der Kommunikation bei Web-Services	303
M 4.451 Aktuelle Web-Service Standards	303
M 4.452 Überwachung eines Web-Service	303
M 4.453 Einsatz eines Security Token Service (STS)	304
M 4.454 Schutz vor unerlaubter Nutzung von Web-Services	304
M 4.455 Autorisierung bei Web-Services	305
M 4.456 Authentisierung bei Web-Services	305
M 4.457 Sichere Mandantentrennung bei Webanwendungen und Web-Services	306
M 4.458 Planung des Einsatzes von Web-Services	306
M 4.459 Einsatz von Verschlüsselung bei Cloud-Nutzung	306
M 4.460 Einsatz von Federation Services	307
M 4.461 Portabilität von Cloud Services	307
M 4.463 Sichere Installation einer Anwendung	307
M 4.464 Aufrechterhaltung der Sicherheit im laufenden Anwendungsbetrieb	307
M 4.465 Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs	308
M 4.466 Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs	308
M 4.467 Auswahl von Applikationen für Smartphones, Tablets und PDAs	308
M 4.468 Trennung von privatem und dienstlichem Bereich auf Smartphones, Tablets und PDAs	308

	Seite	
M 4.469	Abwehr von eingeschleusten GSM-Codes auf Endgeräten mit Telefonfunktion	309
M 4.472	Datensparsamkeit bei Windows 8	309
M 4.473	Schutz und Abhören von XML-Transportcontainern in einer SOA	309
M 4.474	Schutz vor Schwachstellen in Backend-Anwendungen einer SOA	309
M 4.475	Schutz vor Spoofing-Angriffen auf Identitätsdienste	310
M 4.476	Schutz einer WS-Notification-Subscription im Broker	310
M 4.477	Schutz einer WS-Notification	310
M 4.478	Schlüsselmittelverwaltung bei SOA	310
M 4.479	Schutz von Richtlinien in einer SOA	310
M 4.480	Schutz von WS-Resource in SOA-Umgebungen	311
M 4.481	Sichere Nutzung verbindungsloser SOAP-Kommunikation	311
M 4.482	Hardware-Realisierung von Funktionen eingebetteter Systeme	311
M 4.483	Einsatz kryptographischer Prozessoren bzw. Koprozessoren (Trusted Platform Module) bei eingebetteten Systemen	311
M 4.484	Speicherschutz bei eingebetteten Systemen	312
M 4.485	Sicheres Betriebssystem für eingebettete Systeme	312
M 4.486	Widerstandsfähigkeit eingebetteter Systeme gegen Seitenkanalangriffe	312
M 4.487	Tamper-Schutz (Erkennung, Verhinderung, Abwehr) bei eingebetteten Systemen	312
M 4.488	Deaktivieren nicht benutzter Schnittstellen und Dienste bei eingebetteten Systemen	313
M 4.489	Abgesicherter und authentisierter Bootprozess bei eingebetteten Systemen	313
M 4.490	Automatische Überwachung der Baugruppenfunktion (BIST) bei eingebetteten Systemen	313
M 4.491	Verhindern von Debugging-Möglichkeiten bei eingebetteten Systemen	313
M 4.492	Sichere Konfiguration und Nutzung eines eingebetteten Webservers	314
M 4.493	Auswahl einer Entwicklungsumgebung für die Software-Entwicklung	314
M 4.494	Sicherer Einsatz einer Entwicklungsumgebung	314
M 4.495	Sicheres Systemdesign bei der Software-Entwicklung	314
M 4.496	Sichere Installation der entwickelten Software	315
M 4.497	Sichere Installation eines Netzmanagement-Systems	315
M 4.498	Sicherer Einsatz von Single-Sign-On	315
M 4.499	Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen	315
M 4.500	Sicherer Einsatz von Systemen für Identitäts- und Berechtigungsmanagement	316
M 5	Maßnahmenkatalog Kommunikation	317
M 5.1	Entfernen oder Deaktivieren nicht benötigter Leitungen	317
M 5.2	Auswahl einer geeigneten Netz-Topologie	317
M 5.3	Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht	317
M 5.4	Dokumentation und Kennzeichnung der Verkabelung	318
M 5.5	Schadensmindernde Kabelführung	318
M 5.7	Netzverwaltung	318
M 5.8	Regelmäßiger Sicherheitscheck des Netzes	318
M 5.9	Protokollierung am Server	319
M 5.10	Restriktive Rechtevergabe	319
M 5.13	Geeigneter Einsatz von Elementen zur Netzkopplung	319
M 5.14	Absicherung interner Remote-Zugänge von TK-Anlagen	319
M 5.15	Absicherung externer Remote-Zugänge von TK-Anlagen	320
M 5.16	Übersicht über Netzdienste	320
M 5.17	Einsatz der Sicherheitsmechanismen von NFS	320
M 5.18	Einsatz der Sicherheitsmechanismen von NIS	320
M 5.19	Einsatz der Sicherheitsmechanismen von sendmail	321
M 5.20	Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp	321
M 5.21	Sicherer Einsatz von telnet, ftp, tftp und rexec	321
M 5.22	Kompatibilitätsprüfung des Sender- und Empfängersystems	321
M 5.23	Auswahl einer geeigneten Versandart für Datenträger	322
M 5.24	Nutzung eines geeigneten Faxvorblattes	322
M 5.25	Nutzung von Sende- und Empfangsprotokollen	322
M 5.26	Telefonische Ankündigung einer Faxsendung	322
M 5.27	Telefonische Rückversicherung über korrekten Faxempfang	323
M 5.28	Telefonische Rückversicherung über korrekten Faxabsender	323
M 5.29	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle	323
M 5.31	Geeignete Modem-Konfiguration	323
M 5.32	Sicherer Einsatz von Kommunikationssoftware	324
M 5.33	Absicherung von Fernwartung	324
M 5.34	Einsatz von Einmalpasswörtern	324
M 5.35	Einsatz der Sicherheitsmechanismen von UUCP	324
M 5.39	Sicherer Einsatz der Protokolle und Dienste	325
M 5.44	Einseitiger Verbindungsaufbau	325
M 5.45	Sichere Nutzung von Browsern	326

	Seite	
M 5.46	Einsatz von Stand-alone-Systemen zur Nutzung des Internets	326
M 5.47	Einrichten einer Closed User Group	326
M 5.48	Authentisierung mittels CLIP/COLP	326
M 5.49	Callback basierend auf CLIP/COLP	327
M 5.50	Authentisierung mittels PAP/CHAP	327
M 5.51	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner – Institution	327
M 5.52	Sicherheitstechnische Anforderungen an den Kommunikationsrechner	327
M 5.54	Umgang mit unerwünschten E-Mails	328
M 5.56	Sicherer Betrieb eines Mailservers	328
M 5.57	Sichere Konfiguration der Groupware-/Mail-Clients	328
M 5.58	Auswahl und Installation von Datenbankschnittstellen-Treibern	329
M 5.59	Schutz vor DNS-Spoofing bei Authentisierungsmechanismen	329
M 5.60	Auswahl einer geeigneten Backbone-Technologie	329
M 5.61	Geeignete physikalische Segmentierung	329
M 5.62	Geeignete logische Segmentierung	330
M 5.63	Einsatz von GnuPG oder PGP	330
M 5.64	Secure Shell	330
M 5.66	Verwendung von SSL/TLS	331
M 5.67	Verwendung eines Zeitstempel-Dienstes	331
M 5.68	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation	331
M 5.69	Schutz vor aktiven Inhalten	331
M 5.70	Adressumsetzung – NAT (Network Address Translation)	332
M 5.71	Intrusion Detection und Intrusion Response Systeme	332
M 5.72	Deaktivieren nicht benötigter Netzdienste	332
M 5.73	Sicherer Betrieb eines Faxservers	333
M 5.74	Pflege der Faxserver-Adressbücher und der Verteillisten	333
M 5.75	Schutz vor Überlastung des Faxservers	334
M 5.76	Einsatz geeigneter Tunnel-Protokolle für die VPN-Kommunikation	334
M 5.77	Bildung von Teilnetzen	334
M 5.78	Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung	334
M 5.79	Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung	335
M 5.80	Schutz vor Abhören der Raumgespräche über Mobiltelefone	335
M 5.81	Sichere Datenübertragung über Mobiltelefone	335
M 5.87	Vereinbarung über die Anbindung an Netze Dritter	335
M 5.88	Vereinbarung über Datenaustausch mit Dritten	336
M 5.89	Konfiguration des sicheren Kanals unter Windows	336
M 5.90	Einsatz von IPSec unter Windows	336
M 5.91	Einsatz von Personal Firewalls für Clients	336
M 5.92	Sichere Internet-Anbindung von Internet-PCs	337
M 5.93	Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs	337
M 5.94	Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs	338
M 5.95	Sicherer E-Commerce bei der Nutzung von Internet-PCs	338
M 5.96	Sichere Nutzung von Webmail	338
M 5.97	Absicherung der Kommunikation mit Novell eDirectory	339
M 5.98	Schutz vor Missbrauch kostenpflichtiger Einwahlnummern	339
M 5.100	Absicherung der Kommunikation von und zu Exchange-Systemen	339
M 5.108	Kryptographische Absicherung von Groupware bzw. E-Mail	339
M 5.109	Einsatz eines E-Mail-Scanners auf dem Mailserver	340
M 5.110	Absicherung von E-Mail mit SPHINX (S/MIME)	340
M 5.111	Einrichtung von Access Control Lists auf Routern	340
M 5.112	Sicherheitsaspekte von Routing-Protokollen	341
M 5.113	Einsatz des VTAM Session Management Exit unter z/OS	341
M 5.114	Absicherung der z/OS-Tracefunktionen	341
M 5.115	Integration eines Webservers in ein Sicherheitsgateway	342
M 5.116	Integration eines E-Mail-servers in ein Sicherheitsgateway	342
M 5.117	Integration eines Datenbank-Servers in ein Sicherheitsgateway	342
M 5.118	Integration eines DNS-Servers in ein Sicherheitsgateway	343
M 5.119	Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway ..	343
M 5.120	Behandlung von ICMP am Sicherheitsgateway	344
M 5.121	Sichere Kommunikation von unterwegs	344
M 5.122	Sicherer Anschluss von Laptops an lokale Netze	344
M 5.123	Absicherung der Netzkommunikation unter Windows	345
M 5.124	Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen	345
M 5.125	Absicherung der Kommunikation von und zu SAP Systemen	345
M 5.126	Absicherung der SAP RFC-Schnittstelle	346
M 5.127	Absicherung des SAP Internet Connection Framework (ICF)	346
M 5.128	Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle	346

	Seite
M 5.129 Sichere Konfiguration der http-basierten Dienste von SAP Systemen	347
M 5.130 Absicherung des SANs durch Segmentierung	347
M 5.131 Absicherung von IP-Protokollen unter Windows Server 2003	347
M 5.132 Sicherer Einsatz von WebDAV unter Windows Server 2003	348
M 5.133 Auswahl eines VoIP-Signalisierungsprotokolls	348
M 5.134 Sichere Signalisierung bei VoIP	348
M 5.135 Sicherer Medientransport mit SRTP	348
M 5.136 Dienstgüte und Netzmanagement bei VoIP	349
M 5.137 Einsatz von NAT für VoIP	349
M 5.138 Einsatz von RADIUS-Servern	349
M 5.139 Sichere Anbindung eines WLANs an ein LAN	349
M 5.140 Aufbau eines Distribution Systems	350
M 5.141 Regelmäßige Sicherheitschecks in WLANs	350
M 5.142 Abnahme der IT-Verkabelung	350
M 5.143 Laufende Fortschreibung und Revision der Netzdokumentation	350
M 5.144 Rückbau der IT-Verkabelung	351
M 5.145 Sicherer Einsatz von CUPS	351
M 5.146 Netztrennung beim Einsatz von Multifunktionsgeräten	351
M 5.147 Absicherung der Kommunikation mit Verzeichnisdiensten	351
M 5.148 Sichere Anbindung eines externen Netzes mit OpenVPN	352
M 5.149 Sichere Anbindung eines externen Netzes mit IPSec	352
M 5.150 Durchführung von Penetrationstests	352
M 5.151 Sichere Konfiguration des Samba Web Administration Tools	353
M 5.152 Austausch von Informationen und Ressourcen über Peer-to-Peer-Dienste	353
M 5.153 Planung des Netzes für virtuelle Infrastrukturen	353
M 5.154 Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen	354
M 5.155 Datenschutz-Aspekte bei der Internet-Nutzung	354
M 5.156 Sichere Nutzung von Twitter	354
M 5.157 Sichere Nutzung von sozialen Netzwerken	354
M 5.158 Nutzung von Web-Speicherplatz	355
M 5.162 Planung der Leitungskapazitäten beim Einsatz von Terminalservern	355
M 5.163 Restriktive Rechtevergabe auf Terminalservern	355
M 5.164 Sichere Nutzung eines Terminalservers aus einem entfernten Netz	356
M 5.165 Deaktivieren nicht benötigter Mac OS X-Netzdienste	356
M 5.166 Konfiguration der Mac OS X Personal Firewall	356
M 5.167 Sicherheit beim Fernzugriff unter Mac OS X	356
M 5.168 Sichere Anbindung von Hintergrundsystemen an Webanwendungen und Web-Services	357
M 5.169 Systemarchitektur einer Webanwendung	357
M 5.170 Sichere Kommunikationsverbindungen beim Einsatz von OpenLDAP	357
M 5.171 Sichere Kommunikation zu einem zentralen Protokollierungsserver	358
M 5.172 Sichere Zeitsynchronisation bei der zentralen Protokollierung	358
M 5.173 Nutzung von Kurz-URLs und QR-Codes	358
M 5.174 Absicherung der Kommunikation zum Cloud-Zugriff	358
M 5.175 Einsatz eines XML-Gateways	359
M 5.176 Sichere Anbindung von Smartphones, Tablets und PDAs an das Netz der Institution	359
M 5.177 Serverseitige Verwendung von SSL/TLS	359
M 6 Maßnahmenkatalog Notfallvorsorge	361
M 6.1 Erstellung einer Übersicht über Verfügbarkeitsanforderungen	361
M 6.16 Abschließen von Versicherungen	361
M 6.17 Alarmierungsplan und Brandschutzübungen	361
M 6.18 Redundante Leitungsführung	361
M 6.20 Geeignete Aufbewahrung der Backup-Datenträger	362
M 6.21 Sicherungskopie der eingesetzten Software	362
M 6.22 Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen	362
M 6.23 Verhaltensregeln bei Auftreten von Schadprogrammen	363
M 6.24 Erstellen eines Notfall-Bootmediums	363
M 6.26 Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten	363
M 6.27 Sicheres Update des BIOS	364
M 6.29 TK-Basisanschluss für Notrufe	364
M 6.31 Verhaltensregeln nach Verlust der Systemintegrität	364
M 6.32 Regelmäßige Datensicherung	364
M 6.33 Entwicklung eines Datensicherungskonzepts	365
M 6.34 Erhebung der Einflussfaktoren der Datensicherung	365
M 6.35 Festlegung der Verfahrensweise für die Datensicherung	365
M 6.36 Festlegung des Minimaldatensicherungskonzeptes	365
M 6.37 Dokumentation der Datensicherung	366

	Seite
M 6.38	Sicherungskopie der übermittelten Daten 366
M 6.39	Auflistung von Händleradressen zur Fax-Wiederbeschaffung 366
M 6.41	Übungen zur Datenrekonstruktion 366
M 6.43	Einsatz redundanter Windows-Server 367
M 6.47	Datensicherung bei der Telearbeit 367
M 6.48	Verhaltensregeln nach Verlust der Datenbankintegrität 367
M 6.49	Datensicherung einer Datenbank 367
M 6.50	Archivierung von Datenbeständen 368
M 6.51	Wiederherstellung einer Datenbank 368
M 6.52	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten 368
M 6.53	Redundante Auslegung der Netzkomponenten 368
M 6.54	Verhaltensregeln nach Verlust der Netzintegrität 369
M 6.56	Datensicherung bei Einsatz kryptographischer Verfahren 369
M 6.57	Erstellen eines Notfallplans für den Ausfall des Managementsystems 369
M 6.58	Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen 369
M 6.59	Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen 370
M 6.60	Festlegung von Meldewegen für Sicherheitsvorfälle 370
M 6.61	Eskalationsstrategie für Sicherheitsvorfälle 370
M 6.62	Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen 371
M 6.64	Behebung von Sicherheitsvorfällen 371
M 6.65	Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen 371
M 6.66	Nachbereitung von Sicherheitsvorfällen 372
M 6.67	Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle 372
M 6.68	Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen 372
M 6.69	Notfallvorsorge und Ausfallsicherheit bei Faxservern 373
M 6.71	Datensicherung bei mobiler Nutzung des IT-Systems 373
M 6.72	Ausfallvorsorge bei Mobiltelefonen 373
M 6.73	Notfallplanung und Notfallübungen für die Lotus Notes/Domino-Umgebung 373
M 6.74	Notfallarchiv 374
M 6.75	Redundante Kommunikationsverbindungen 374
M 6.76	Erstellen eines Notfallplans für den Ausfall von Windows-Systemen 374
M 6.78	Datensicherung unter Windows Clients 375
M 6.79	Datensicherung beim Einsatz von Internet-PCs 375
M 6.81	Erstellen von Datensicherungen für Novell eDirectory 375
M 6.83	Notfallvorsorge beim Outsourcing 376
M 6.84	Regelmäßige Datensicherung der System- und Archivdaten 376
M 6.88	Erstellen eines Notfallplans für den Webserver 377
M 6.90	Datensicherung und Archivierung bei Groupware und E-Mail 377
M 6.91	Datensicherung und Recovery bei Routern und Switches 377
M 6.92	Notfallvorsorge bei Routern und Switches 378
M 6.93	Notfallvorsorge für z/OSSysteme 378
M 6.94	Notfallvorsorge bei Sicherheitsgateways 379
M 6.95	Ausfallvorsorge und Datensicherung bei Smartphones, Tablets und PDAs 379
M 6.96	Notfallvorsorge für einen Server 379
M 6.97	Notfallvorsorge für SAP Systeme 380
M 6.98	Notfallvorsorge und Notfallreaktion für Speichersysteme 380
M 6.99	Regelmäßige Sicherung wichtiger Systemkomponenten für Windows-Server 380
M 6.100	Erstellung eines Notfallplans für den Ausfall von VoIP 381
M 6.101	Datensicherung bei VoIP 381
M 6.102	Verhaltensregeln bei WLAN-Sicherheitsvorfällen 381
M 6.103	Redundanzen für die Primärverkabelung 381
M 6.104	Redundanzen für die Gebäudeverkabelung 382
M 6.105	Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten 382
M 6.106	Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes 382
M 6.107	Erstellung von Datensicherungen für Verzeichnisdienste 382
M 6.108	Datensicherung für Domänen-Controller 383
M 6.109	Notfallplan für den Ausfall eines VPNs 383
M 6.110	Festlegung des Geltungsbereichs und der Notfallmanagementstrategie 383
M 6.111	Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Leitungsebene 384
M 6.112	Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement 384
M 6.113	Bereitstellung angemessener Ressourcen für das Notfallmanagement 384
M 6.114	Erstellung eines Notfallkonzepts 385
M 6.115	Integration der Mitarbeiter in den Notfallmanagement-Prozess 385
M 6.116	Integration von Notfallmanagement in organisationsweite Abläufe und Prozesse 385
M 6.117	Tests und Notfallübungen 386
M 6.118	Überprüfung und Aufrechterhaltung der Notfallmaßnahmen 386
M 6.119	Dokumentation im Notfallmanagement-Prozess 386

	Seite
M 6.120 Überprüfung und Steuerung des Notfallmanagement-Systems	386
M 6.121 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen	387
M 6.122 Definition eines Sicherheitsvorfalls	387
M 6.123 Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen	387
M 6.124 Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung	388
M 6.125 Einrichtung einer zentralen Kontaktstelle für die Meldung von Sicherheitsvorfällen	388
M 6.126 Einführung in die Computer-Forensik	388
M 6.127 Etablierung von Beweissicherungsmaßnahmen bei Sicherheitsvorfällen	389
M 6.128 Schulung an Beweismittelsicherungswerkzeugen	389
M 6.129 Schulung der Mitarbeiter des Service Desk zur Behandlung von Sicherheitsvorfällen	389
M 6.130 Erkennen und Erfassen von Sicherheitsvorfällen	390
M 6.131 Qualifizieren und Bewerten von Sicherheitsvorfällen	390
M 6.132 Eindämmen der Auswirkung von Sicherheitsvorfällen	390
M 6.133 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen	390
M 6.134 Dokumentation von Sicherheitsvorfällen	391
M 6.135 Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers	391
M 6.136 Erstellen eines Notfallplans für den Ausfall eines Samba-Servers	391
M 6.137 Treuhänderische Hinterlegung (Escrow)	392
M 6.138 Erstellung eines Notfallplans für den Ausfall von Virtualisierungskomponenten	392
M 6.139 Erstellen eines Notfallplans für DNS-Server	392
M 6.140 Erstellen eines Notfallplans für den Ausfall von Groupware-Systemen	393
M 6.141 Festlegung von Ausweichverfahren bei der Internet-Nutzung	393
M 6.142 Einsatz von redundanten Terminalservern	393
M 6.143 Bereitstellung von Terminalserver-Clients aus Depot-Wartung	393
M 6.144 Konfiguration von Terminalserver-Clients für die duale Nutzung als normale Client-PCs	393
M 6.145 Notfallvorsorge für TK-Anlagen	394
M 6.146 Datensicherung und Wiederherstellung von Mac OS X Clients	394
M 6.147 Wiederherstellung von Systemparametern beim Einsatz von Mac OS X	394
M 6.148 Aussonderung eines Mac OS X Systems	394
M 6.149 Datensicherung unter Exchange	395
M 6.150 Datensicherung beim Einsatz von OpenLDAP	395
M 6.151 Alarmierungskonzept für die Protokollierung	395
M 6.152 Notfallvorsorge und regelmäßige Datensicherung im Cloud Computing	395
M 6.153 Einsatz von redundanten Cloud-Management-Komponenten	396
M 6.154 Notfallmanagement für Web-Services	396
M 6.155 Erstellung eines Notfallkonzeptes für einen Cloud Service	396
M 6.156 Durchführung eigener Datensicherungen	397
M 6.157 Entwicklung eines Redundanzkonzeptes für Anwendungen	397
M 6.158 Notfallvorsorge für Anwendungen	397
M 6.159 Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs	397
M 6.166 Notfallvorsorgekonzept für SOA-Umgebungen	398
M 6.161 Redundante Hardware-Komponenten in serviceorientierten Architekturen	398
M 6.162 Reaktion bei praktischer Schwächung eines Kryptoverfahrens	398
M 6.163 Wiederherstellung von eingebetteten Systemen	398
M 6.164 Notfallvorsorge bei der Software-Entwicklung	398
M 6.165 Erstellen eines Notfallplans für den Ausfall des lokalen Netzes	399
M 6.166 Notfallvorsorge beim Identitäts- und Berechtigungsmanagement-System	399