

Bausteine und zugeordnete Maßnahmen

| Baustein | Alt | Bausteinname | Maßnahme | Zertifikat | Zyklus | Maßnahmentitel |
|----------|-------|--------------------------|----------|------------|----------|---|
| B 1.0 | (3.0) | IT-Sicherheitsmanagement | M 2.192 | (A) | Planung | Erstellung einer IT-Sicherheitsleitlinie |
| | | | M 2.193 | (A) | Umsetzg. | Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit |
| | | | M 2.195 | (A) | Umsetzg. | Erstellung eines IT-Sicherheitskonzepts |
| | | | M 2.197 | (A) | Umsetzg. | Integration der Mitarbeiter in den Sicherheitsprozess |
| | | | M 2.199 | (A) | Betrieb | Aufrechterhaltung der IT-Sicherheit |
| | | | M 2.200 | (C) | Betrieb | Managementreporte und -bewertungen der IT-Sicherheit |
| | | | M 2.201 | (C) | Betrieb | Dokumentation des IT-Sicherheitsprozesses |
| | | | M 2.335 | (A) | Planung | Festlegung der IT-Sicherheitsziele und -strategie |
| | | | M 2.336 | (A) | Planung | Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene |
| | | | M 2.337 | (A) | Umsetzg. | Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse |
| | | | M 2.338 | (Z) | Umsetzg. | Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien |
| | | | M 2.339 | (Z) | Umsetzg. | Wirtschaftlicher Einsatz von Ressourcen für IT-Sicherheit |
| | | | M 2.340 | (A) | Betrieb | Beachtung rechtlicher Rahmenbedingungen |
| B 1.1 | (3.1) | Organisation | M 2.1 | (A) | Planung | Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz |
| | | | M 2.2 | (C) | Planung | Betriebsmittelverwaltung |
| | | | M 2.4 | (B) | Planung | Regelungen für Wartungs- und Reparaturarbeiten |
| | | | M 2.5 | (A) | Planung | Aufgabenverteilung und Funktionstrennung |
| | | | M 2.6 | (A) | Betrieb | Vergabe von Zutrittsberechtigungen |
| | | | M 2.7 | (A) | Betrieb | Vergabe von Zugangsberechtigungen |
| | | | M 2.8 | (A) | Betrieb | Vergabe von Zugriffsrechten |
| | | | M 2.13 | (A) | Aussnd. | Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln |
| | | | M 2.14 | (A) | Betrieb | Schlüsselverwaltung |
| | | | M 2.16 | (B) | Betrieb | Beaufsichtigung oder Begleitung von Fremdpersonen |
| | | | M 2.18 | (Z) | Betrieb | Kontrollgänge |
| | | | M 2.37 | (Z) | Betrieb | "Der aufgeräumte Arbeitsplatz" |
| | | | M 2.39 | (B) | Betrieb | Reaktion auf Verletzungen der Sicherheitspolitik |
| | | | M 2.40 | (A) | Planung | Rechtzeitige Beteiligung des Personal-/Betriebsrates |
| | | | M 2.177 | (Z) | Betrieb | Sicherheit bei Umzügen |
| | | | M 2.225 | (B) | Planung | Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten |
| B 1.2 | (3.2) | Personal | M 3.1 | (A) | Umsetzg. | Geregelte Einarbeitung/Einweisung neuer Mitarbeiter |
| | | | M 3.2 | (A) | Umsetzg. | Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen |
| | | | M 3.3 | (A) | Betrieb | Vertretungsregelungen |
| | | | M 3.4 | (A) | Betrieb | Schulung vor Programmnutzung |
| | | | M 3.5 | (A) | Betrieb | Schulung zu IT-Sicherheitsmaßnahmen |
| | | | M 3.6 | (A) | Aussnd. | Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern |

| | | | | | | |
|-------|-------|-----------------------------|---------|-----|-----------|--|
| | | | M 3.7 | (Z) | Betrieb | Anlaufstelle bei persönlichen Problemen |
| | | | M 3.8 | (Z) | Betrieb | Vermeidung von Störungen des Betriebsklimas |
| | | | M 3.10 | (A) | Umsetzg. | Auswahl eines vertrauenswürdigen Administrators und Vertreters |
| | | | M 3.11 | (A) | Betrieb | Schulung des Wartungs- und Administrationspersonals |
| | | | M 3.33 | (Z) | Umsetzg. | Sicherheitsüberprüfung von Mitarbeitern |
| | | | M 3.50 | (Z) | Beschaff. | Auswahl von Personal |
| | | | M 3.51 | (Z) | Planung | Geeignetes Konzept für Personaleinsatz und -qualifizierung |
| B 1.3 | (3.3) | Notfallvorsorgekonzept | | | | |
| | | | M 6.1 | (A) | Planung | Erstellung einer Übersicht über Verfügbarkeitsanforderungen |
| | | | M 6.2 | (A) | Planung | Notfall-Definition, Notfall-Verantwortlicher |
| | | | M 6.3 | (C) | Planung | Erstellung eines Notfall-Handbuches |
| | | | M 6.4 | (B) | Umsetzg. | Dokumentation der Kapazitätsanforderungen der IT-Anwendungen |
| | | | M 6.5 | (B) | Umsetzg. | Definition des eingeschränkten IT-Betriebs |
| | | | M 6.6 | (B) | Umsetzg. | Untersuchung interner und externer Ausweichmöglichkeiten |
| | | | M 6.7 | (A) | Umsetzg. | Regelung der Verantwortung im Notfall |
| | | | M 6.8 | (A) | Umsetzg. | Alarmierungsplan |
| | | | M 6.9 | (C) | Umsetzg. | Notfall-Pläne für ausgewählte Schadensereignisse |
| | | | M 6.10 | (C) | Umsetzg. | Notfall-Plan für DFÜ-Ausfall |
| | | | M 6.11 | (B) | Umsetzg. | Erstellung eines Wiederanlaufplans |
| | | | M 6.12 | (C) | Betrieb | Durchführung von Notfallübungen |
| | | | M 6.13 | (A) | Umsetzg. | Erstellung eines Datensicherungsplans |
| | | | M 6.14 | (B) | Beschaff. | Ersatzbeschaffungsplan |
| | | | M 6.15 | (Z) | Beschaff. | Lieferantenvereinbarungen |
| | | | M 6.16 | (Z) | Umsetzg. | Abschließen von Versicherungen |
| | | | M 6.75 | (Z) | Planung | Redundante Kommunikationsverbindungen |
| B 1.4 | (3.4) | Datensicherungskonzept | | | | |
| | | | M 2.41 | (A) | Umsetzg. | Verpflichtung der Mitarbeiter zur Datensicherung |
| | | | M 2.137 | (A) | Beschaff. | Beschaffung eines geeigneten Datensicherungssystems |
| | | | M 6.20 | (A) | Betrieb | Geeignete Aufbewahrung der Backup-Datenträger |
| | | | M 6.21 | (C) | Umsetzg. | Sicherungskopie der eingesetzten Software |
| | | | M 6.22 | (A) | Betrieb | Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen |
| | | | M 6.32 | (A) | Betrieb | Regelmäßige Datensicherung |
| | | | M 6.33 | (B) | Planung | Entwicklung eines Datensicherungskonzepts |
| | | | M 6.34 | (B) | Planung | Erhebung der Einflussfaktoren der Datensicherung |
| | | | M 6.35 | (B) | Planung | Festlegung der Verfahrensweise für die Datensicherung |
| | | | M 6.36 | (A) | Planung | Festlegung des Minimaldatensicherungskonzeptes |
| | | | M 6.37 | (A) | Umsetzg. | Dokumentation der Datensicherung |
| | | | M 6.41 | (A) | Notfallv. | Übungen zur Datenrekonstruktion |
| B 1.6 | (3.6) | Computer-Virenschutzkonzept | | | | |
| | | | M 2.154 | (A) | Planung | Erstellung eines Computer-Virenschutzkonzepts |
| | | | M 2.155 | (A) | Planung | Identifikation potentiell von Computer-Viren betroffener IT-Systeme |

| | | | | | | |
|-------|-------|-------------------------------------|---------|-----|-----------|---|
| B 1.7 | (3.7) | Kryptokonzept | M 2.156 | (A) | Planung | Auswahl einer geeigneten Computer-Virenschutz-Strategie |
| | | | M 2.157 | (A) | Beschaff. | Auswahl eines geeigneten Computer-Viren-Suchprogramms |
| | | | M 2.158 | (A) | Betrieb | Meldung von Computer-Virusinfektionen |
| | | | M 2.159 | (A) | Betrieb | Aktualisierung der eingesetzten Computer-Viren-Suchprogramme |
| | | | M 2.160 | (A) | Planung | Regelungen zum Computer-Virenschutz |
| | | | M 2.224 | (A) | Betrieb | Vorbeugung gegen Trojanische Pferde |
| | | | M 4.3 | (A) | Betrieb | Regelmäßiger Einsatz eines Anti-Viren-Programms |
| | | | M 4.33 | (A) | Betrieb | Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung |
| | | | M 4.84 | (A) | Umsetzg. | Nutzung der BIOS-Sicherheitsmechanismen |
| | | | M 4.253 | (A) | Planung | Schutz vor Spyware |
| | | | M 6.23 | (A) | Notfallv. | Verhaltensregeln bei Auftreten eines Computer-Virus |
| | | | M 2.46 | (A) | Umsetzg. | Geeignetes Schlüsselmanagement |
| | | | M 2.161 | (A) | Planung | Entwicklung eines Kryptokonzepts |
| | | | M 2.162 | (A) | Planung | Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte |
| | | | M 2.163 | (A) | Planung | Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte |
| | | | M 2.164 | (A) | Planung | Auswahl eines geeigneten kryptographischen Verfahrens |
| | | | M 2.165 | (A) | Beschaff. | Auswahl eines geeigneten kryptographischen Produktes |
| | | | M 2.166 | (A) | Planung | Regelung des Einsatzes von Kryptomodulen |
| | | | M 3.23 | (A) | Planung | Einführung in kryptographische Grundbegriffe |
| B 1.8 | (3.8) | Behandlung von Sicherheitsvorfällen | M 4.85 | (Z) | Beschaff. | Geeignetes Schnittstellendesign bei Kryptomodulen |
| | | | M 4.86 | (A) | Umsetzg. | Sichere Rollenteilung und Konfiguration der Kryptomodule |
| | | | M 4.87 | (Z) | Umsetzg. | Physikalische Sicherheit von Kryptomodulen |
| | | | M 4.88 | (A) | Beschaff. | Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen |
| | | | M 4.89 | (Z) | Umsetzg. | Abstrahlsicherheit |
| | | | M 4.90 | (A) | Planung | Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells |
| | | | M 6.56 | (A) | Notfallv. | Datensicherung bei Einsatz kryptographischer Verfahren |
| | | | M 6.58 | (A) | Planung | Etablierung eines Managementsystems zur Behandlung von Sicherheitsvorfällen |
| | | | M 6.59 | (A) | Planung | Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen |
| | | | M 6.60 | (A) | Planung | Verhaltensregeln und Meldewege bei Sicherheitsvorfällen |
| | | | M 6.61 | (C) | Planung | Eskalationsstrategie für Sicherheitsvorfälle |
| | | | M 6.62 | (B) | Planung | Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen |
| | | | M 6.63 | (A) | Betrieb | Untersuchung und Bewertung eines Sicherheitsvorfalls |
| | | | M 6.64 | (A) | Betrieb | Behebung von Sicherheitsvorfällen |
| | | | M 6.65 | (A) | Betrieb | Benachrichtigung betroffener Stellen |
| | | | M 6.66 | (B) | Betrieb | Nachbereitung von Sicherheitsvorfällen |
| | | | M 6.67 | (Z) | Planung | Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle |
| | | | M 6.68 | (C) | Betrieb | Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen |
| B 1.9 | (3.9) | Hard- und Software-Management | | | | |

| | | | |
|---------|-----|-----------|---|
| M 1.29 | (Z) | Umsetzg. | Geeignete Aufstellung eines IT-Systems |
| M 1.46 | (Z) | Betrieb | Einsatz von Diebstahl-Sicherungen |
| M 2.3 | (B) | Planung | Datenträgerverwaltung |
| M 2.9 | (A) | Planung | Nutzungsverbot nicht freigegebener Hard- und Software |
| M 2.10 | (C) | Betrieb | Überprüfung des Hard- und Software-Bestandes |
| M 2.11 | (A) | Planung | Regelung des Passwortgebrauchs |
| M 2.12 | (C) | Planung | Betreuung und Beratung von IT-Benutzern |
| M 2.22 | (Z) | Betrieb | Hinterlegen des Passwortes |
| M 2.25 | (A) | Umsetzg. | Dokumentation der Systemkonfiguration |
| M 2.26 | (A) | Umsetzg. | Ernennung eines Administrators und eines Vertreters |
| M 2.30 | (A) | Planung | Regelung für die Einrichtung von Benutzern / Benutzergruppen |
| M 2.34 | (A) | Betrieb | Dokumentation der Veränderungen an einem bestehenden System |
| M 2.35 | (B) | Betrieb | Informationsbeschaffung über Sicherheitslücken des Systems |
| M 2.38 | (B) | Umsetzg. | Aufteilung der Administrationstätigkeiten |
| M 2.62 | (B) | Beschaff. | Software-Abnahme- und Freigabe-Verfahren |
| M 2.64 | (A) | Betrieb | Kontrolle der Protokolldateien |
| M 2.65 | (C) | Betrieb | Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System |
| M 2.69 | (B) | Umsetzg. | Einrichtung von Standardarbeitsplätzen |
| M 2.110 | (A) | Betrieb | Datenschutzaspekte bei der Protokollierung |
| M 2.111 | (A) | Umsetzg. | Bereithalten von Handbüchern |
| M 2.138 | (B) | Umsetzg. | Strukturierte Datenhaltung |
| M 2.167 | (B) | Aussnd. | Sicheres Löschen von Datenträgern |
| M 2.182 | (A) | Betrieb | Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen |
| M 2.204 | (A) | Umsetzg. | Verhinderung ungesicherter Netzzugänge |
| M 2.214 | (A) | Planung | Konzeption des IT-Betriebs |
| M 2.215 | (B) | Betrieb | Fehlerbehandlung |
| M 2.216 | (C) | Planung | Genehmigungsverfahren für IT-Komponenten |
| M 2.217 | (B) | Planung | Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen |
| M 2.218 | (C) | Planung | Regelung der Mitnahme von Datenträgern und IT-Komponenten |
| M 2.219 | (A) | Betrieb | Kontinuierliche Dokumentation der Informationsverarbeitung |
| M 2.220 | (A) | Planung | Richtlinien für die Zugriffs- bzw. Zugangskontrolle |
| M 2.221 | (B) | Planung | Änderungsmanagement |
| M 2.223 | (B) | Planung | Sicherheitsvorgaben für die Nutzung von Standardsoftware |
| M 2.226 | (A) | Planung | Regelungen für den Einsatz von Fremdpersonal |
| M 3.26 | (A) | Betrieb | Einweisung des Personals in den sicheren Umgang mit IT |
| M 4.1 | (A) | Umsetzg. | Passwortschutz für IT-Systeme |
| M 4.7 | (A) | Umsetzg. | Änderung voreingestellter Passwörter |
| M 4.65 | (C) | Umsetzg. | Test neuer Hard- und Software |
| M 4.78 | (A) | Betrieb | Sorgfältige Durchführung von Konfigurationsänderungen |
| M 4.84 | (A) | Umsetzg. | Nutzung der BIOS-Sicherheitsmechanismen |
| M 4.107 | (B) | Betrieb | Nutzung von Hersteller-Ressourcen |

| | | | | | | |
|--------|--------|------------------|---------|-----|-----------|--|
| B 1.10 | (9.1) | Standardsoftware | M 4.109 | (Z) | Betrieb | Software-Reinstallation bei Arbeitsplatzrechnern |
| | | | M 4.133 | (Z) | Planung | Geeignete Auswahl von Authentikationsmechanismen |
| | | | M 4.134 | (C) | Planung | Wahl geeigneter Datenformate |
| | | | M 4.135 | (A) | Umsetzg. | Restriktive Vergabe von Zugriffsrechten auf Systemdateien |
| | | | M 4.234 | (B) | Aussnd. | Aussonderung von IT-Systemen |
| | | | M 4.254 | (Z) | Betrieb | Sicherer Einsatz von drahtlosen Tastaturen und Mäusen |
| | | | M 5.68 | (Z) | Planung | Einsatz von Verschlüsselungsverfahren zur Netzkommunikation |
| | | | M 5.77 | (Z) | Planung | Bildung von Teilnetzen |
| | | | M 5.87 | (C) | Planung | Vereinbarung über die Anbindung an Netze Dritter |
| | | | M 5.88 | (C) | Planung | Vereinbarung über Datenaustausch mit Dritten |
| | | | M 6.21 | (C) | Notfallv. | Sicherungskopie der eingesetzten Software |
| | | | M 6.27 | (C) | Notfallv. | Sicheres Update des BIOS |
| | | | M 2.66 | (Z) | Beschaff. | Beachtung des Beitrags der Zertifizierung für die Beschaffung |
| | | | M 2.79 | (A) | Planung | Festlegung der Verantwortlichkeiten im Bereich Standardsoftware |
| | | | M 2.80 | (A) | Planung | Erstellung eines Anforderungskatalogs für Standardsoftware |
| | | | M 2.81 | (A) | Beschaff. | Vorauswahl eines geeigneten Standardsoftwareproduktes |
| | | | M 2.82 | (B) | Planung | Entwicklung eines Testplans für Standardsoftware |
| | | | M 2.83 | (B) | Umsetzg. | Testen von Standardsoftware |
| | | | M 2.84 | (A) | Umsetzg. | Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware |
| B 1.11 | (3.10) | Outsourcing | M 2.85 | (A) | Umsetzg. | Freigabe von Standardsoftware |
| | | | M 2.86 | (B) | Umsetzg. | Sicherstellen der Integrität von Standardsoftware |
| | | | M 2.87 | (A) | Umsetzg. | Installation und Konfiguration von Standardsoftware |
| | | | M 2.88 | (A) | Betrieb | Lizenzverwaltung und Versionskontrolle von Standardsoftware |
| | | | M 2.89 | (C) | Aussnd. | Deinstallation von Standardsoftware |
| | | | M 2.90 | (A) | Umsetzg. | Überprüfung der Lieferung |
| | | | M 4.34 | (Z) | Planung | Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen |
| | | | M 4.42 | (Z) | Umsetzg. | Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung |
| | | | M 2.40 | (Z) | Planung | Rechtzeitige Beteiligung des Personal-/Betriebsrates |
| | | | M 2.42 | (A) | Planung | Festlegung der möglichen Kommunikationspartner |
| | | | M 2.221 | (A) | Betrieb | Änderungsmanagement |
| | | | M 2.226 | (A) | Planung | Regelungen für den Einsatz von Fremdpersonal |
| | | | M 2.250 | (A) | Planung | Festlegung einer Outsourcing-Strategie |
| | | | M 2.251 | (A) | Planung | Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben |
| | | | M 2.252 | (A) | Beschaff. | Wahl eines geeigneten Outsourcing-Dienstleisters |
| | | | M 2.253 | (A) | Umsetzg. | Vertragsgestaltung mit dem Outsourcing-Dienstleister |
| | | | M 2.254 | (A) | Planung | Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben |
| | | | M 2.255 | (A) | Umsetzg. | Sichere Migration bei Outsourcing-Vorhaben |
| | | | M 2.256 | (A) | Betrieb | Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb |
| | | | M 2.307 | (A) | Aussnd. | Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses |

| | | | | | | |
|--------|--------|--|---------|-----|-----------|---|
| B 1.12 | (9.5) | Archivierung | M 3.33 | (Z) | Betrieb | Sicherheitsüberprüfung von Mitarbeitern |
| | | | M 5.87 | (A) | Umsetzg. | Vereinbarung über die Anbindung an Netze Dritter |
| | | | M 5.88 | (A) | Umsetzg. | Vereinbarung über Datenaustausch mit Dritten |
| | | | M 6.70 | (A) | Notfallv. | Erstellen eines Notfallplans für den Ausfall des RAS-Systems |
| | | | M 6.83 | (A) | Notfallv. | Notfallvorsorge beim Outsourcing |
| | | | M 1.59 | (B) | Umsetzg. | Geeignete Aufstellung von Archivsystemen |
| | | | M 1.60 | (A) | Betrieb | Geeignete Lagerung von Archivmedien |
| | | | M 2.242 | (A) | Planung | Zielsetzung der elektronischen Archivierung |
| | | | M 2.243 | (A) | Planung | Entwicklung des Archivierungskonzepts |
| | | | M 2.244 | (A) | Planung | Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung |
| | | | M 2.245 | (A) | Planung | Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung |
| | | | M 2.246 | (A) | Planung | Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung |
| | | | M 2.257 | (C) | Betrieb | Überwachung der Speicherressourcen von Archivmedien |
| | | | M 2.258 | (A) | Betrieb | Konsistente Indizierung von Dokumenten bei der Archivierung |
| | | | M 2.259 | (Z) | Planung | Einführung eines übergeordneten Dokumentenmanagements |
| | | | M 2.260 | (B) | Betrieb | Regelmäßige Revision des Archivierungsprozesses |
| | | | M 2.261 | (B) | Betrieb | Regelmäßige Marktbeobachtung von Archivsystemen |
| | | | M 2.262 | (A) | Planung | Regelung der Nutzung von Archivsystemen |
| | | | M 2.263 | (A) | Betrieb | Regelmäßige Aufbereitung von archivierten Datenbeständen |
| | | | M 2.264 | (B) | Betrieb | Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung |
| B 1.13 | (3.11) | IT-Sicherheitssensibilisierung und -schulung | M 2.265 | (Z) | Planung | Geeigneter Einsatz digitaler Signaturen bei der Archivierung |
| | | | M 2.266 | (C) | Umsetzg. | Regelmäßige Erneuerung technischer Archivsystem-Komponenten |
| | | | M 3.2 | (A) | Umsetzg. | Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen |
| | | | M 3.34 | (A) | Umsetzg. | Einweisung in die Administration des Archivsystems |
| | | | M 3.35 | (A) | Umsetzg. | Einweisung der Benutzer in die Bedienung des Archivsystems |
| | | | M 4.168 | (A) | Beschaff. | Auswahl eines geeigneten Archivsystems |
| | | | M 4.169 | (A) | Beschaff. | Verwendung geeigneter Archivmedien |
| | | | M 4.170 | (A) | Beschaff. | Auswahl geeigneter Datenformate für die Archivierung von Dokumenten |
| | | | M 4.171 | (A) | Betrieb | Schutz der Integrität der Index-Datenbank von Archivsystemen |
| | | | M 4.172 | (C) | Betrieb | Protokollierung der Archivzugriffe |
| | | | M 4.173 | (B) | Betrieb | Regelmäßige Funktions- und Recoverytests bei der Archivierung |
| | | | M 6.84 | (A) | Notfallv. | Regelmäßige Datensicherung der System- und Archivdaten |
| | | | M 2.198 | (A) | Betrieb | Sensibilisierung der Mitarbeiter für IT-Sicherheit |
| | | | M 2.312 | (A) | Planung | Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit |
| | | | M 3.4 | (A) | Betrieb | Schulung vor Programmnutzung |
| | | | M 3.5 | (A) | Umsetzg. | Schulung zu IT-Sicherheitsmaßnahmen |
| | | | M 3.11 | (A) | Betrieb | Schulung des Wartungs- und Administrationspersonals |

| | | | | | | |
|-------|-------|-------------|---------|-----|-----------|---|
| B 2.1 | (4.1) | Gebäude | M 3.26 | (A) | Betrieb | Einweisung des Personals in den sicheren Umgang mit IT |
| | | | M 3.44 | (A) | Planung | Sensibilisierung des Managements für IT-Sicherheit |
| | | | M 3.45 | (A) | Umsetzg. | Planung von Schulungsinhalten zur IT-Sicherheit |
| | | | M 3.46 | (A) | Umsetzg. | Ansprechpartner zu Sicherheitsfragen |
| | | | M 3.47 | (Z) | Betrieb | Durchführung von Planspielen zur IT-Sicherheit |
| | | | M 3.48 | (A) | Beschaff. | Auswahl von Trainern oder Schulungsanbietern |
| | | | M 3.49 | (B) | Umsetzg. | Schulung zur Vorgehensweise nach IT-Grundschutz |
| | | | M 1.1 | (A) | Umsetzg. | Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften |
| | | | M 1.2 | (A) | Umsetzg. | Regelungen für Zutritt zu Verteilern |
| | | | M 1.3 | (A) | Planung | Angepasste Aufteilung der Stromkreise |
| | | | M 1.4 | (B) | Planung | Blitzschutzeinrichtungen |
| | | | M 1.5 | (Z) | Planung | Galvanische Trennung von Außenleitungen |
| | | | M 1.6 | (A) | Umsetzg. | Einhaltung von Brandschutzvorschriften |
| | | | M 1.7 | (A) | Planung | Handfeuerlöscher |
| | | | M 1.8 | (A) | Planung | Raumbelegung unter Berücksichtigung von Brandlasten |
| | | | M 1.10 | (Z) | Planung | Verwendung von Sicherheitstüren und -fenstern |
| | | | M 1.11 | (A) | Planung | Lagepläne der Versorgungsleitungen |
| | | | M 1.12 | (A) | Planung | Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile |
| | | | M 1.13 | (Z) | Planung | Anordnung schützenswerter Gebäudeteile |
| B 2.2 | (4.2) | Verkabelung | M 1.14 | (Z) | Planung | Selbsttätige Entwässerung |
| | | | M 1.15 | (A) | Betrieb | Geschlossene Fenster und Türen |
| | | | M 1.16 | (Z) | Planung | Geeignete Standortauswahl |
| | | | M 1.17 | (Z) | Umsetzg. | Pförtnerdienst |
| | | | M 1.18 | (Z) | Planung | Gefahrenmeldeanlage |
| | | | M 1.19 | (Z) | Planung | Einbruchsschutz |
| | | | M 2.14 | (A) | Betrieb | Schlüsselverwaltung |
| | | | M 2.15 | (B) | Betrieb | Brandschutzbegehungen |
| | | | M 2.17 | (A) | Umsetzg. | Zutrittsregelung und -kontrolle |
| | | | M 2.308 | (Z) | Aussnd. | Auszug aus Gebäuden |
| | | | M 2.334 | (Z) | Planung | Auswahl eines geeigneten Gebäudes |
| | | | M 6.17 | (A) | Notfallv. | Alarmierungsplan und Brandschutzübungen |
| | | | M 1.9 | (A) | Umsetzg. | Brandabschottung von Trassen |
| | | | M 1.20 | (A) | Planung | Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht |
| | | | M 1.21 | (A) | Planung | Ausreichende Trassendimensionierung |
| | | | M 1.22 | (Z) | Planung | Materielle Sicherung von Leitungen und Verteilern |
| | | | M 1.39 | (Z) | Umsetzg. | Verhinderung von Ausgleichsströmen auf Schirmungen |
| | | | M 2.19 | (B) | Umsetzg. | Neutrale Dokumentation in den Verteilern |
| | | | M 2.20 | (Z) | Betrieb | Kontrolle bestehender Verbindungen |
| | | | M 5.1 | (B) | Betrieb | Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen |

| | | | | | |
|-------|---|--------|-----|-----------|---|
| B 2.3 | (4.3.1) Büroraum | M 5.2 | (A) | Planung | Auswahl einer geeigneten Netz-Topographie |
| | | M 5.3 | (A) | Planung | Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht |
| | | M 5.4 | (A) | Umsetzg. | Dokumentation und Kennzeichnung der Verkabelung |
| | | M 5.5 | (A) | Umsetzg. | Schadensmindernde Kabelführung |
| | | M 6.18 | (Z) | Notfallv. | Redundante Leitungsführung |
| B 2.4 | (4.3.2) Serverraum | M 1.15 | (A) | Betrieb | Geschlossene Fenster und Türen |
| | | M 1.23 | (A) | Betrieb | Abgeschlossene Türen |
| | | M 1.46 | (Z) | Betrieb | Einsatz von Diebstahl-Sicherungen |
| | | M 2.17 | (A) | Umsetzg. | Zutrittsregelung und -kontrolle |
| | | M 3.9 | (Z) | Planung | Ergonomischer Arbeitsplatz |
| B 2.5 | (4.3.3) Datenträgerarchiv | M 1.3 | (A) | Planung | Angepasste Aufteilung der Stromkreise |
| | | M 1.7 | (A) | Planung | Handfeuerlöscher |
| | | M 1.10 | (C) | Planung | Verwendung von Sicherheitstüren und -fenstern |
| | | M 1.15 | (A) | Betrieb | Geschlossene Fenster und Türen |
| | | M 1.18 | (Z) | Planung | Gefahrenmeldeanlage |
| | | M 1.23 | (A) | Betrieb | Abgeschlossene Türen |
| | | M 1.24 | (C) | Planung | Vermeidung von wasserführenden Leitungen |
| | | M 1.25 | (B) | Planung | Überspannungsschutz |
| | | M 1.26 | (Z) | Planung | Not-Aus-Schalter |
| | | M 1.27 | (B) | Planung | Klimatisierung |
| | | M 1.28 | (B) | Planung | Lokale unterbrechungsfreie Stromversorgung |
| | | M 1.31 | (Z) | Planung | Fernanzeige von Störungen |
| | | M 1.52 | (Z) | Planung | Redundanzen in der technischen Infrastruktur |
| | | M 1.58 | (A) | Planung | Technische und organisatorische Vorgaben für Serverräume |
| | | M 1.62 | (C) | Planung | Brandschutz von Patchfeldern |
| B 2.6 | (4.3.4) Raum für technische Infrastruktur | M 2.17 | (A) | Umsetzg. | Zutrittsregelung und -kontrolle |
| | | M 2.21 | (A) | Umsetzg. | Rauchverbot |
| | | M 1.7 | (A) | Planung | Handfeuerlöscher |
| | | M 1.10 | (C) | Planung | Verwendung von Sicherheitstüren und -fenstern |
| | | M 1.15 | (A) | Betrieb | Geschlossene Fenster und Türen |
| | | M 1.18 | (Z) | Planung | Gefahrenmeldeanlage |
| | | M 1.23 | (A) | Betrieb | Abgeschlossene Türen |
| | | M 1.24 | (Z) | Planung | Vermeidung von wasserführenden Leitungen |
| | | M 1.27 | (Z) | Planung | Klimatisierung |
| | | M 2.17 | (A) | Umsetzg. | Zutrittsregelung und -kontrolle |
| | | M 2.21 | (A) | Umsetzg. | Rauchverbot |
| | | M 1.3 | (A) | Planung | Angepasste Aufteilung der Stromkreise |

| | | | | | | |
|-------|-------|-------------------------|---------|-----|-----------|--|
| B 2.7 | (4.4) | Schutzschrank | M 1.7 | (A) | Planung | Handfeuerlöscher |
| | | | M 1.10 | (Z) | Planung | Verwendung von Sicherheitstüren und -fenstern |
| | | | M 1.15 | (A) | Betrieb | Geschlossene Fenster und Türen |
| | | | M 1.18 | (Z) | Planung | Gefahrenmeldeanlage |
| | | | M 1.23 | (A) | Betrieb | Abgeschlossene Türen |
| | | | M 1.24 | (Z) | Planung | Vermeidung von wasserführenden Leitungen |
| | | | M 1.25 | (A) | Planung | Überspannungsschutz |
| | | | M 1.26 | (Z) | Planung | Not-Aus-Schalter |
| | | | M 1.27 | (B) | Planung | Klimatisierung |
| | | | M 1.31 | (Z) | Planung | Fernanzeige von Störungen |
| | | | M 2.17 | (A) | Umsetzg. | Zutrittsregelung und -kontrolle |
| | | | M 2.21 | (A) | Umsetzg. | Rauchverbot |
| | | | M 1.7 | (B) | Planung | Handfeuerlöscher |
| B 2.8 | (4.5) | Häuslicher Arbeitsplatz | M 1.15 | (A) | Betrieb | Geschlossene Fenster und Türen |
| | | | M 1.18 | (Z) | Planung | Gefahrenmeldeanlage |
| | | | M 1.24 | (Z) | Planung | Vermeidung von wasserführenden Leitungen |
| | | | M 1.25 | (B) | Planung | Überspannungsschutz |
| | | | M 1.26 | (A) | Planung | Not-Aus-Schalter |
| | | | M 1.27 | (B) | Planung | Klimatisierung |
| | | | M 1.28 | (B) | Planung | Lokale unterbrechungsfreie Stromversorgung |
| | | | M 1.31 | (Z) | Planung | Fernanzeige von Störungen |
| | | | M 1.40 | (A) | Umsetzg. | Geeignete Aufstellung von Schutzschranken |
| | | | M 1.41 | (Z) | Planung | Schutz gegen elektromagnetische Einstrahlung |
| | | | M 2.17 | (C) | Umsetzg. | Zutrittsregelung und -kontrolle |
| | | | M 2.21 | (A) | Umsetzg. | Rauchverbot |
| | | | M 2.95 | (A) | Beschaff. | Beschaffung geeigneter Schutzschränke |
| | | | M 2.96 | (A) | Betrieb | Verschluss von Schutzschranken |
| | | | M 2.97 | (A) | Betrieb | Korrektur Umgang mit Codeschlössern |
| | | | M 2.311 | (A) | Planung | Planung von Schutzschranken |
| | | | M 3.20 | (A) | Umsetzg. | Einweisung in die Bedienung von Schutzschranken |
| | | | M 1.15 | (A) | Betrieb | Geschlossene Fenster und Türen |
| | | | M 1.19 | (Z) | Planung | Einbruchsschutz |
| | | | M 1.23 | (A) | Betrieb | Abgeschlossene Türen |
| | | | M 1.44 | (A) | Planung | Geeignete Einrichtung eines häuslichen Arbeitsplatzes |
| | | | M 1.45 | (A) | Betrieb | Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger |
| | | | M 2.13 | (A) | Aussnd. | Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln |
| | | | M 2.37 | (C) | Betrieb | "Der aufgeräumte Arbeitsplatz" |
| | | | M 2.112 | (A) | Umsetzg. | Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution |

| | | | | | | |
|--------|-------|----------------------|---------|-----|-----------|--|
| B 2.9 | (4.6) | Rechenzentrum | M 2.136 | (A) | Betrieb | Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung |
| | | | M 3.9 | (Z) | Planung | Ergonomischer Arbeitsplatz |
| B 2.10 | (4.7) | Mobiler Arbeitsplatz | M 1.3 | (A) | Planung | Angepasste Aufteilung der Stromkreise |
| | | | M 1.7 | (A) | Planung | Handfeuerlöscher |
| | | | M 1.10 | (C) | Planung | Verwendung von Sicherheitstüren und -fenstern |
| | | | M 1.12 | (A) | Planung | Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile |
| | | | M 1.13 | (Z) | Planung | Anordnung schützenswerter Gebäudeteile |
| | | | M 1.15 | (A) | Betrieb | Geschlossene Fenster und Türen |
| | | | M 1.18 | (B) | Planung | Gefahrenmeldeanlage |
| | | | M 1.23 | (A) | Betrieb | Abgeschlossene Türen |
| | | | M 1.24 | (C) | Planung | Vermeidung von wasserführenden Leitungen |
| | | | M 1.25 | (A) | Planung | Überspannungsschutz |
| | | | M 1.26 | (B) | Planung | Not-Aus-Schalter |
| | | | M 1.27 | (B) | Planung | Klimatisierung |
| | | | M 1.31 | (Z) | Planung | Fernanzeige von Störungen |
| | | | M 1.47 | (B) | Planung | Eigener Brandabschnitt |
| | | | M 1.48 | (B) | Planung | Brandmeldeanlage |
| | | | M 1.49 | (A) | Planung | Technische und organisatorische Vorgaben für das Rechenzentrum |
| | | | M 1.50 | (C) | Planung | Rauchschutz |
| | | | M 1.51 | (A) | Umsetzg. | Brandlastreduzierung |
| | | | M 1.52 | (Z) | Planung | Redundanzen in der technischen Infrastruktur |
| | | | M 1.53 | (Z) | Planung | Videoüberwachung |
| | | | M 1.54 | (Z) | Planung | Brandfrüherkennung / Löschtechnik |
| | | | M 1.55 | (Z) | Planung | Perimeterschutz |
| | | | M 1.56 | (A) | Planung | Sekundär-Energieversorgung |
| | | | M 1.57 | (A) | Umsetzg. | Aktuelle Infrastruktur- und Baupläne |
| | | | M 1.62 | (C) | Planung | Brandschutz von Patchfeldern |
| | | | M 2.17 | (A) | Umsetzg. | Zutrittsregelung und -kontrolle |
| | | | M 2.21 | (A) | Umsetzg. | Rauchverbot |
| | | | M 2.212 | (B) | Umsetzg. | Organisatorische Vorgaben für die Gebäudereinigung |
| | | | M 2.213 | (A) | Umsetzg. | Wartung der technischen Infrastruktur |
| | | | M 6.16 | (Z) | Notfallv. | Abschließen von Versicherungen |
| | | | M 6.17 | (A) | Notfallv. | Alarmierungsplan und Brandschutzübungen |
| | | | M 6.74 | (Z) | Notfallv. | Notfallarchiv |
| | | | M 1.15 | (A) | Betrieb | Geschlossene Fenster und Türen |
| | | | M 1.23 | (A) | Betrieb | Abgeschlossene Türen |
| | | | M 1.45 | (A) | Betrieb | Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger |
| | | | M 1.46 | (Z) | Betrieb | Einsatz von Diebstahl-Sicherungen |
| | | | M 1.61 | (A) | Planung | Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes |

| | | | | | | |
|---------|-------|---|---------|-----|-----------|--|
| B 2.11 | (4.8) | Besprechungs-, Veranstaltungs- und Schulungsräume | M 2.13 | (A) | Aussnd. | Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln |
| | | | M 2.37 | (C) | Betrieb | "Der aufgeräumte Arbeitsplatz" |
| | | | M 2.136 | (A) | Betrieb | Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung |
| | | | M 2.218 | (A) | Planung | Regelung der Mitnahme von Datenträgern und IT-Komponenten |
| | | | M 2.309 | (C) | Planung | Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung |
| | | | M 4.251 | (A) | Betrieb | Arbeiten mit fremden IT-Systemen |
| | | | M 1.6 | (A) | Umsetzg. | Einhaltung von Brandschutzvorschriften |
| | | | M 1.15 | (A) | Betrieb | Geschlossene Fenster und Türen |
| | | | M 2.16 | (B) | Betrieb | Beaufsichtigung oder Begleitung von Fremdpersonen |
| | | | M 2.69 | (B) | Umsetzg. | Einrichtung von Standardarbeitsplätzen |
| B 3.101 | (6.1) | Allgemeiner Server | M 2.204 | (A) | Umsetzg. | Verhinderung ungesicherter Netzzugänge |
| | | | M 2.331 | (A) | Planung | Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen |
| | | | M 2.332 | (B) | Planung | Einrichtung von Besprechungs-, Vortrags- und Schulungsräumen |
| | | | M 2.333 | (A) | Umsetzg. | Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen |
| | | | M 3.9 | (Z) | Planung | Ergonomischer Arbeitsplatz |
| | | | M 4.109 | (C) | Betrieb | Software-Reinstallation bei Arbeitsplatzrechnern |
| | | | M 4.252 | (C) | Umsetzg. | Sichere Konfiguration von Schulungsrechnern |
| | | | M 5.77 | (Z) | Planung | Bildung von Teilnetzen |
| | | | M 5.124 | (C) | Planung | Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen |
| | | | M 1.28 | (B) | Planung | Lokale unterbrechungsfreie Stromversorgung |
| | | | M 2.22 | (A) | Betrieb | Hinterlegen des Passwortes |
| | | | M 2.31 | (A) | Betrieb | Dokumentation der zugelassenen Benutzer und Rechteprofile |
| | | | M 2.32 | (Z) | Umsetzg. | Einrichtung einer eingeschränkten Benutzerumgebung |
| | | | M 2.35 | (B) | Betrieb | Informationsbeschaffung über Sicherheitslücken des Systems |
| | | | M 2.138 | (B) | Umsetzg. | Strukturierte Datenhaltung |
| | | | M 2.204 | (A) | Betrieb | Verhinderung ungesicherter Netzzugänge |
| | | | M 2.273 | (A) | Betrieb | Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates |
| | | | M 2.314 | (Z) | Planung | Verwendung von hochverfügbaren Architekturen für Server |
| | | | M 2.315 | (A) | Planung | Planung des Servereinsatzes |
| | | | M 2.316 | (A) | Planung | Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server |
| | | | M 2.317 | (C) | Beschaff. | Beschaffungskriterien für einen Server |
| | | | M 2.318 | (A) | Umsetzg. | Sichere Installation eines Servers |
| | | | M 2.319 | (C) | Aussnd. | Migration eines Servers |
| | | | M 2.320 | (A) | Aussnd. | Geregelte Außerbetriebnahme eines Servers |
| | | | M 4.7 | (A) | Umsetzg. | Änderung voreingestellter Passwörter |
| | | | M 4.15 | (A) | Umsetzg. | Gesichertes Login |
| | | | M 4.16 | (A) | Umsetzg. | Zugangsbeschränkungen für Accounts und / oder Terminals |
| | | | M 4.17 | (A) | Umsetzg. | Sperren und Löschen nicht benötigter Accounts und Terminals |

B 3.102 (6.2) Server unter Unix

| | | | |
|---------|-----|-----------|--|
| M 4.24 | (A) | Betrieb | Sicherstellung einer konsistenten Systemverwaltung |
| M 4.40 | (C) | Umsetzg. | Verhinderung der unautorisierten Nutzung des Rechnermikrofons |
| M 4.93 | (B) | Betrieb | Regelmäßige Integritätsprüfung |
| M 4.237 | (A) | Umsetzg. | Sichere Grundkonfiguration eines IT-Systems |
| M 4.238 | (A) | Betrieb | Einsatz eines lokalen Paketfilters |
| M 4.239 | (A) | Betrieb | Sicherer Betrieb eines Servers |
| M 4.240 | (Z) | Betrieb | Einrichten einer Testumgebung für einen Server |
| M 5.8 | (B) | Betrieb | Regelmäßiger Sicherheitscheck des Netzes |
| M 5.9 | (A) | Betrieb | Protokollierung am Server |
| M 5.10 | (A) | Planung | Restriktive Rechtevergabe |
| M 5.37 | (B) | Planung | Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz |
| M 6.24 | (A) | Notfallv. | Erstellen eines Notfall-Bootmediums |
| M 6.96 | (A) | Notfallv. | Notfallvorsorge für einen Server |
| M 2.33 | (C) | Planung | Aufteilung der Administrationstätigkeiten unter Unix |
| M 4.9 | (A) | Umsetzg. | Einsatz der Sicherheitsmechanismen von X-Windows |
| M 4.13 | (A) | Planung | Sorgfältige Vergabe von IDs |
| M 4.14 | (A) | Umsetzg. | Obligatorischer Passwortschutz unter Unix |
| M 4.18 | (A) | Planung | Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus |
| M 4.19 | (A) | Umsetzg. | Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen |
| M 4.20 | (B) | Umsetzg. | Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen |
| M 4.21 | (A) | Umsetzg. | Verhinderung des unautorisierten Erlangens von Administratorrechten |
| M 4.22 | (C) | Umsetzg. | Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System |
| M 4.23 | (A) | Umsetzg. | Sicherer Aufruf ausführbarer Dateien |
| M 4.25 | (A) | Betrieb | Einsatz der Protokollierung im Unix-System |
| M 4.26 | (B) | Betrieb | Regelmäßiger Sicherheitscheck des Unix-Systems |
| M 4.105 | (A) | Umsetzg. | Erste Maßnahmen nach einer Unix-Standardinstallation |
| M 4.106 | (A) | Umsetzg. | Aktivieren der Systemprotokollierung |
| M 5.16 | (B) | Planung | Übersicht über Netzdienste |
| M 5.17 | (A) | Umsetzg. | Einsatz der Sicherheitsmechanismen von NFS |
| M 5.18 | (A) | Umsetzg. | Einsatz der Sicherheitsmechanismen von NIS |
| M 5.19 | (A) | Umsetzg. | Einsatz der Sicherheitsmechanismen von sendmail |
| M 5.20 | (A) | Umsetzg. | Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp |
| M 5.21 | (A) | Umsetzg. | Sicherer Einsatz von telnet, ftp, tftp und rexec |
| M 5.34 | (Z) | Planung | Einsatz von Einmalpasswörtern |
| M 5.35 | (A) | Umsetzg. | Einsatz der Sicherheitsmechanismen von UUCP |
| M 5.36 | (Z) | Planung | Verschlüsselung unter Unix und Windows NT |
| M 5.38 | (B) | Planung | Sichere Einbindung von DOS-PCs in ein Unix-Netz |
| M 5.64 | (Z) | Planung | Secure Shell |
| M 5.72 | (A) | Umsetzg. | Deaktivieren nicht benötigter Netzdienste |

| | | | | | | |
|---------|-------|---------------------------------|---------|-----|-----------|--|
| B 3.103 | (6.4) | Server unter Windows NT | M 5.82 | (A) | Planung | Sicherer Einsatz von SAMBA |
| | | | M 5.83 | (Z) | Planung | Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN |
| | | | M 6.31 | (A) | Notfallv. | Verhaltensregeln nach Verlust der Systemintegrität |
| B 3.103 | (6.4) | Server unter Windows NT | M 2.91 | (A) | Planung | Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz |
| | | | M 2.92 | (B) | Betrieb | Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz |
| | | | M 2.93 | (A) | Planung | Planung des Windows NT Netzes |
| | | | M 2.94 | (B) | Umsetzg. | Freigabe von Verzeichnissen unter Windows NT |
| | | | M 4.48 | (A) | Umsetzg. | Passwortschutz unter Windows NT/2000/XP |
| | | | M 4.49 | (A) | Umsetzg. | Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System |
| | | | M 4.50 | (Z) | Planung | Strukturierte Systemverwaltung unter Windows NT |
| | | | M 4.51 | (Z) | Planung | Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT |
| | | | M 4.52 | (A) | Umsetzg. | Geräteschutz unter Windows NT/2000/XP |
| | | | M 4.53 | (A) | Umsetzg. | Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT |
| | | | M 4.54 | (A) | Betrieb | Protokollierung unter Windows NT |
| | | | M 4.55 | (A) | Umsetzg. | Sichere Installation von Windows NT |
| | | | M 4.56 | (B) | Betrieb | Sicheres Löschen unter Windows-Betriebssystemen |
| | | | M 4.57 | (A) | Umsetzg. | Deaktivieren der automatischen CD-ROM-Erkennung |
| | | | M 4.75 | (A) | Umsetzg. | Schutz der Registrierung unter Windows NT/2000/XP |
| | | | M 4.76 | (B) | Planung | Sichere Systemversion von Windows NT |
| | | | M 4.77 | (A) | Umsetzg. | Schutz der Administratorkonten unter Windows NT |
| | | | M 5.36 | (Z) | Planung | Verschlüsselung unter Unix und Windows NT |
| | | | M 5.40 | (B) | Planung | Sichere Einbindung von DOS-PCs in ein Windows NT Netz |
| | | | M 5.41 | (C) | Planung | Sichere Konfiguration des Fernzugriffs unter Windows NT |
| | | | M 5.42 | (C) | Planung | Sichere Konfiguration der TCP/IP-Netzverwaltung unter Windows NT |
| | | | M 5.43 | (B) | Planung | Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT |
| | | | M 6.42 | (A) | Notfallv. | Erstellung von Rettungsdisketten für Windows NT |
| | | | M 6.43 | (Z) | Notfallv. | Einsatz redundanter Windows NT/2000 Server |
| | | | M 6.44 | (A) | Notfallv. | Datensicherung unter Windows NT |
| B 3.104 | (6.5) | Server unter Novell Netware 3.x | M 1.42 | (A) | Umsetzg. | Gesicherte Aufstellung von Novell Netware Servern |
| | | | M 2.98 | (A) | Umsetzg. | Sichere Installation von Novell Netware Servern |
| | | | M 2.99 | (A) | Planung | Sichere Einrichtung von Novell Netware Servern |
| | | | M 2.100 | (A) | Betrieb | Sicherer Betrieb von Novell Netware Servern |
| | | | M 2.101 | (B) | Betrieb | Revision von Novell Netware Servern |
| | | | M 2.102 | (Z) | Umsetzg. | Verzicht auf die Aktivierung der Remote Console |
| B 3.105 | (6.6) | Server unter Novell Netware 4.x | M 1.42 | (A) | Umsetzg. | Gesicherte Aufstellung von Novell Netware Servern |
| | | | M 2.102 | (Z) | Umsetzg. | Verzicht auf die Aktivierung der Remote Console |
| | | | M 2.147 | (A) | Umsetzg. | Sichere Migration von Novell Netware 3.x Servern in Novell Netware 4.x Netze |

| | | | | | | |
|---------|-------|---------------------------|---------|-----|-----------|--|
| B 3.106 | (6.9) | Server unter Windows 2000 | M 2.148 | (A) | Planung | Sichere Einrichtung von Novell Netware 4.x Netzen |
| | | | M 2.149 | (A) | Betrieb | Sicherer Betrieb von Novell Netware 4.x Netzen |
| | | | M 2.150 | (B) | Betrieb | Revision von Novell Netware 4.x Netzen |
| | | | M 2.151 | (A) | Planung | Entwurf eines NDS-Konzeptes |
| | | | M 2.152 | (B) | Planung | Entwurf eines Zeitsynchronisations-Konzeptes |
| | | | M 2.153 | (A) | Planung | Dokumentation von Novell Netware 4.x Netzen |
| | | | M 4.102 | (Z) | Umsetzg. | C2-Sicherheit unter Novell 4.11 |
| | | | M 4.103 | (Z) | Umsetzg. | DHCP-Server unter Novell Netware 4.x |
| | | | M 4.104 | (Z) | Umsetzg. | LDAP Services for NDS |
| | | | M 4.108 | (Z) | Betrieb | Vereinfachtes und sicheres Netzmanagement mit DNS Services unter Novell NetWare 4.11 |
| | | | M 6.55 | (C) | Notfallv. | Reduzierung der Wiederanlaufzeit für Novell Netware Server |
| | | | M 2.227 | (A) | Planung | Planung des Windows 2000 Einsatzes |
| | | | M 2.228 | (A) | Planung | Festlegen einer Windows 2000 Sicherheitsrichtlinie |
| | | | M 2.229 | (A) | Planung | Planung des Active Directory |
| | | | M 2.230 | (A) | Planung | Planung der Active Directory-Administration |
| | | | M 2.231 | (A) | Planung | Planung der Gruppenrichtlinien unter Windows 2000 |
| | | | M 2.232 | (B) | Planung | Planung der Windows 2000 CA-Struktur |
| | | | M 2.233 | (B) | Planung | Planung der Migration von Windows NT auf Windows 2000 |
| | | | M 3.27 | (A) | Umsetzg. | Schulung zur Active Directory-Verwaltung |
| | | | M 4.48 | (A) | Umsetzg. | Passwortschutz unter Windows NT/2000/XP |
| | | | M 4.56 | (C) | Betrieb | Sicheres Löschen unter Windows-Betriebssystemen |
| | | | M 4.75 | (A) | Umsetzg. | Schutz der Registrierung unter Windows NT/2000/XP |
| | | | M 4.136 | (A) | Umsetzg. | Sichere Installation von Windows 2000 |
| | | | M 4.137 | (A) | Umsetzg. | Sichere Konfiguration von Windows 2000 |
| | | | M 4.138 | (A) | Umsetzg. | Konfiguration von Windows 2000 als Domänen-Controller |
| | | | M 4.139 | (A) | Umsetzg. | Konfiguration von Windows 2000 als Server |
| | | | M 4.140 | (A) | Umsetzg. | Sichere Konfiguration wichtiger Windows 2000 Dienste |
| | | | M 4.141 | (A) | Umsetzg. | Sichere Konfiguration des DDNS unter Windows 2000 |
| | | | M 4.142 | (B) | Umsetzg. | Sichere Konfiguration des WINS unter Windows 2000 |
| | | | M 4.143 | (B) | Umsetzg. | Sichere Konfiguration des DHCP unter Windows 2000 |
| | | | M 4.144 | (B) | Umsetzg. | Nutzung der Windows 2000 CA |
| | | | M 4.145 | (A) | Umsetzg. | Sichere Konfiguration von RRAS unter Windows 2000 |
| | | | M 4.146 | (A) | Betrieb | Sicherer Betrieb von Windows 2000/XP |
| | | | M 4.147 | (Z) | Planung | Sichere Nutzung von EFS unter Windows 2000/XP |
| | | | M 4.148 | (B) | Betrieb | Überwachung eines Windows 2000/XP Systems |
| | | | M 4.149 | (A) | Umsetzg. | Datei- und Freigabeberechtigungen unter Windows 2000/XP |
| | | | M 5.89 | (A) | Umsetzg. | Konfiguration des sicheren Kanals unter Windows 2000/XP |
| | | | M 5.90 | (Z) | Umsetzg. | Einsatz von IPSec unter Windows 2000/XP |
| | | | M 6.43 | (Z) | Notfallv. | Einsatz redundanter Windows NT/2000 Server |

| | | | | | | |
|---------|--------|------------------------------|---------|-----|-----------|---|
| B 3.107 | (6.10) | S/390- und zSeries-Mainframe | M 6.76 | (C) | Notfallv. | Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes |
| | | | M 6.77 | (A) | Notfallv. | Erstellung von Rettungsdisketten für Windows 2000 |
| | | | M 6.78 | (A) | Notfallv. | Datensicherung unter Windows 2000/XP |
| B 3.107 | (6.10) | S/390- und zSeries-Mainframe | M 2.31 | (B) | Planung | Dokumentation der zugelassenen Benutzer und Rechteprofile |
| | | | M 2.285 | (Z) | Planung | Festlegung von Standards für z/OS-Systemdefinitionen |
| | | | M 2.286 | (Z) | Planung | Planung und Einsatz von zSeries-Systemen |
| | | | M 2.287 | (Z) | Planung | Batch-Job-Planung für z/OS-Systeme |
| | | | M 2.288 | (B) | Planung | Erstellung von Sicherheitsrichtlinien für z/OS-Systeme |
| | | | M 2.289 | (A) | Umsetzg. | Einsatz restriktiver z/OS-Kennungen |
| | | | M 2.290 | (Z) | Umsetzg. | Einsatz von RACF-Exits |
| | | | M 2.291 | (C) | Betrieb | Sicherheits-Berichtswesen und -Audits unter z/OS |
| | | | M 2.292 | (B) | Betrieb | Überwachung von z/OS-Systemen |
| | | | M 2.293 | (C) | Betrieb | Wartung von zSeries-Systemen |
| | | | M 2.294 | (Z) | Betrieb | Synchronisierung von z/OS-Passwörtern und RACF-Kommandos |
| | | | M 2.295 | (A) | Planung | Systemverwaltung von z/OS-Systemen |
| | | | M 2.296 | (Z) | Planung | Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren |
| | | | M 2.297 | (B) | Aussnd. | Deinstallation von z/OS-Systemen |
| | | | M 3.39 | (A) | Planung | Einführung in die zSeries-Plattform |
| | | | M 3.40 | (A) | Planung | Einführung in das z/OS-Betriebssystem |
| | | | M 3.41 | (A) | Planung | Einführung in Linux und z/VM für zSeries-Systeme |
| | | | M 3.42 | (A) | Umsetzg. | Schulung des z/OS-Bedienungspersonals |
| | | | M 4.207 | (A) | Umsetzg. | Einsatz und Sicherung systemnaher z/OS-Terminals |
| | | | M 4.208 | (B) | Umsetzg. | Absichern des Start-Vorgangs von z/OS-Systemen |
| | | | M 4.209 | (A) | Umsetzg. | Sichere Grundkonfiguration von z/OS-Systemen |
| | | | M 4.210 | (B) | Betrieb | Sicherer Betrieb des z/OS-Betriebssystems |
| | | | M 4.211 | (A) | Umsetzg. | Einsatz des z/OS-Sicherheitssystems RACF |
| | | | M 4.212 | (Z) | Umsetzg. | Absicherung von Linux für zSeries |
| | | | M 4.213 | (A) | Umsetzg. | Absichern des Login-Vorgangs unter z/OS |
| | | | M 4.214 | (B) | Betrieb | Datenträgerverwaltung unter z/OS-Systemen |
| | | | M 4.215 | (B) | Betrieb | Absicherung sicherheitskritischer z/OS-Dienstprogramme |
| | | | M 4.216 | (C) | Umsetzg. | Festlegung der Systemgrenzen von z/OS |
| | | | M 4.217 | (C) | Umsetzg. | Workload Management für z/OS-Systeme |
| | | | M 4.218 | (Z) | Betrieb | Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen |
| | | | M 4.219 | (C) | Umsetzg. | Lizenzschlüssel-Management für z/OS-Software |
| | | | M 4.220 | (B) | Umsetzg. | Absicherung von Unix System Services bei z/OS-Systemen |
| | | | M 4.221 | (C) | Planung | Parallel-Sysplex unter z/OS |
| | | | M 5.113 | (Z) | Umsetzg. | Einsatz des VTAM Session Management Exit unter z/OS |
| | | | M 5.114 | (B) | Umsetzg. | Absicherung der z/OS-Tracefunktionen |
| | | | M 6.67 | (A) | Notfallv. | Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle |
| | | | M 6.93 | (A) | Notfallv. | Notfallvorsorge für z/OS-Systeme |

B 3.201 (5.99) Allgemeiner Client

| | | | |
|---------|-----|-----------|--|
| M 2.22 | (A) | Betrieb | Hinterlegen des Passwortes |
| M 2.23 | (Z) | Planung | Herausgabe einer PC-Richtlinie |
| M 2.25 | (A) | Umsetzg. | Dokumentation der Systemkonfiguration |
| M 2.204 | (A) | Betrieb | Verhinderung ungesicherter Netzzugänge |
| M 2.273 | (A) | Betrieb | Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates |
| M 2.321 | (A) | Planung | Planung des Einsatzes von Client-Server-Netzen |
| M 2.322 | (A) | Planung | Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz |
| M 2.323 | (A) | Aussnd. | Geregelte Außerbetriebnahme eines Clients |
| M 3.18 | (A) | Betrieb | Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung |
| M 4.2 | (A) | Umsetzg. | Bildschirmsperre |
| M 4.3 | (A) | Betrieb | Regelmäßiger Einsatz eines Anti-Viren-Programms |
| M 4.4 | (C) | Betrieb | Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern |
| M 4.40 | (A) | Umsetzg. | Verhinderung der unautorisierten Nutzung des Rechnermikrofons |
| M 4.41 | (C) | Betrieb | Einsatz angemessener Sicherheitsprodukte für IT-Systeme |
| M 4.93 | (B) | Betrieb | Regelmäßige Integritätsprüfung |
| M 4.200 | (Z) | Betrieb | Umgang mit USB-Speichermedien |
| M 4.234 | (A) | Aussnd. | Aussonderung von IT-Systemen |
| M 4.236 | (Z) | Betrieb | Zentrale Administration von Laptops |
| M 4.237 | (A) | Umsetzg. | Sichere Grundkonfiguration eines IT-Systems |
| M 4.238 | (A) | Betrieb | Einsatz eines lokalen Paketfilters |
| M 4.241 | (A) | Betrieb | Sicherer Betrieb von Clients |
| M 4.242 | (Z) | Umsetzg. | Einrichten einer Referenzinstallation für Clients |
| M 5.37 | (B) | Planung | Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz |
| M 5.45 | (B) | Betrieb | Sicherheit von WWW-Browsern |
| M 6.24 | (A) | Notfallv. | Erstellen eines Notfall-Bootmediums |
| M 6.32 | (A) | Notfallv. | Regelmäßige Datensicherung |

B 3.202 (5.99) Allgemeines nicht vernetztes IT-System

| | | | |
|--------|-----|-----------|--|
| M 2.22 | (Z) | Betrieb | Hinterlegen des Passwortes |
| M 2.23 | (Z) | Planung | Herausgabe einer PC-Richtlinie |
| M 2.63 | (A) | Planung | Einrichten der Zugriffsrechte |
| M 3.18 | (A) | Betrieb | Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung |
| M 4.2 | (A) | Umsetzg. | Bildschirmsperre |
| M 4.4 | (Z) | Betrieb | Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern |
| M 4.7 | (A) | Umsetzg. | Änderung voreingestellter Passwörter |
| M 4.15 | (A) | Umsetzg. | Gesichertes Login |
| M 4.30 | (A) | Betrieb | Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen |
| M 4.40 | (C) | Betrieb | Verhinderung der unautorisierten Nutzung des Rechnermikrofons |
| M 4.41 | (Z) | Planung | Einsatz angemessener Sicherheitsprodukte für IT-Systeme |
| M 6.20 | (A) | Notfallv. | Geeignete Aufbewahrung der Backup-Datenträger |

| | | | | | | |
|---------|-------|-------------------|---------|-----|-----------|--|
| B 3.203 | (5.3) | Laptop | M 6.22 | (A) | Notfallv. | Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen |
| | | | M 6.32 | (A) | Notfallv. | Regelmäßige Datensicherung |
| B 3.203 | (5.3) | Laptop | M 1.33 | (A) | Betrieb | Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz |
| | | | M 1.34 | (A) | Betrieb | Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz |
| | | | M 1.35 | (Z) | Betrieb | Sammelaufbewahrung tragbarer IT-Systeme |
| | | | M 1.46 | (Z) | Betrieb | Einsatz von Diebstahl-Sicherungen |
| | | | M 2.36 | (B) | Betrieb | Geregelte Übergabe und Rücknahme eines tragbaren PC |
| | | | M 2.218 | (B) | Planung | Regelung der Mitnahme von Datenträgern und IT-Komponenten |
| | | | M 2.306 | (B) | Aussnd. | Verlustmeldung |
| | | | M 2.309 | (A) | Planung | Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung |
| | | | M 2.310 | (A) | Beschaff. | Geeignete Auswahl von Laptops |
| | | | M 4.3 | (A) | Betrieb | Regelmäßiger Einsatz eines Anti-Viren-Programms |
| | | | M 4.27 | (A) | Betrieb | Zugriffsschutz am Laptop |
| | | | M 4.28 | (Z) | Betrieb | Software-Reinstallation bei Benutzerwechsel eines Laptops |
| | | | M 4.29 | (Z) | Planung | Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme |
| | | | M 4.31 | (A) | Betrieb | Sicherstellung der Energieversorgung im mobilen Einsatz |
| | | | M 4.40 | (A) | Umsetzg. | Verhinderung der unautorisierten Nutzung des Rechnermikrofons |
| | | | M 4.235 | (B) | Betrieb | Abgleich der Datenbestände von Laptops |
| | | | M 4.236 | (Z) | Betrieb | Zentrale Administration von Laptops |
| | | | M 4.255 | (A) | Betrieb | Nutzung von IrDA-Schnittstellen |
| | | | M 5.91 | (A) | Betrieb | Einsatz von Personal Firewalls für Internet-PCs |
| | | | M 5.121 | (A) | Betrieb | Sichere Kommunikation von unterwegs |
| | | | M 5.122 | (A) | Betrieb | Sicherer Anschluss von Laptops an lokale Netze |
| | | | M 6.71 | (A) | Notfallv. | Datensicherung bei mobiler Nutzung des IT-Systems |
| B 3.204 | (5.2) | Client unter Unix | M 2.31 | (A) | Betrieb | Dokumentation der zugelassenen Benutzer und Rechteprofile |
| | | | M 2.32 | (Z) | Umsetzg. | Einrichtung einer eingeschränkten Benutzerumgebung |
| | | | M 2.33 | (Z) | Planung | Aufteilung der Administrationstätigkeiten unter Unix |
| | | | M 4.9 | (A) | Umsetzg. | Einsatz der Sicherheitsmechanismen von X-Windows |
| | | | M 4.13 | (A) | Planung | Sorgfältige Vergabe von IDs |
| | | | M 4.14 | (A) | Umsetzg. | Obligatorischer Passwortschutz unter Unix |
| | | | M 4.16 | (C) | Umsetzg. | Zugangsbeschränkungen für Accounts und / oder Terminals |
| | | | M 4.17 | (A) | Umsetzg. | Sperren und Löschen nicht benötigter Accounts und Terminals |
| | | | M 4.18 | (A) | Planung | Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus |
| | | | M 4.19 | (A) | Umsetzg. | Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen |
| | | | M 4.20 | (B) | Umsetzg. | Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen |
| | | | M 4.21 | (A) | Umsetzg. | Verhinderung des unautorisierten Erlangens von Administratorrechten |
| | | | M 4.22 | (Z) | Umsetzg. | Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System |
| | | | M 4.23 | (B) | Umsetzg. | Sicherer Aufruf ausführbarer Dateien |

| | | | | | | |
|---------|-------|-------------------------|---------|-----|-----------|--|
| B 3.205 | (5.5) | Client unter Windows NT | M 4.25 | (A) | Betrieb | Einsatz der Protokollierung im Unix-System |
| | | | M 4.26 | (C) | Betrieb | Regelmäßiger Sicherheitscheck des Unix-Systems |
| | | | M 4.105 | (A) | Umsetzg. | Erste Maßnahmen nach einer Unix-Standardinstallation |
| | | | M 4.106 | (B) | Umsetzg. | Aktivieren der Systemprotokollierung |
| | | | M 5.17 | (A) | Umsetzg. | Einsatz der Sicherheitsmechanismen von NFS |
| | | | M 5.18 | (A) | Umsetzg. | Einsatz der Sicherheitsmechanismen von NIS |
| | | | M 5.19 | (A) | Umsetzg. | Einsatz der Sicherheitsmechanismen von sendmail |
| | | | M 5.20 | (A) | Umsetzg. | Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp |
| | | | M 5.21 | (A) | Umsetzg. | Sicherer Einsatz von telnet, ftp, tftp und rexec |
| | | | M 5.34 | (Z) | Planung | Einsatz von Einmalpasswörtern |
| | | | M 5.35 | (A) | Umsetzg. | Einsatz der Sicherheitsmechanismen von UUCP |
| | | | M 5.36 | (Z) | Planung | Verschlüsselung unter Unix und Windows NT |
| | | | M 5.64 | (Z) | Planung | Secure Shell |
| | | | M 5.72 | (A) | Umsetzg. | Deaktivieren nicht benötigter Netzdienste |
| | | | M 6.31 | (A) | Notfallv. | Verhaltensregeln nach Verlust der Systemintegrität |
| | | | M 2.31 | (B) | Betrieb | Dokumentation der zugelassenen Benutzer und Rechteprofile |
| | | | M 2.32 | (Z) | Umsetzg. | Einrichtung einer eingeschränkten Benutzerumgebung |
| | | | M 4.17 | (B) | Umsetzg. | Sperren und Löschen nicht benötigter Accounts und Terminals |
| B 3.206 | (5.6) | Client unter Windows 95 | M 4.48 | (A) | Planung | Passwortschutz unter Windows NT/2000/XP |
| | | | M 4.49 | (A) | Planung | Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System |
| | | | M 4.50 | (Z) | Planung | Strukturierte Systemverwaltung unter Windows NT |
| | | | M 4.51 | (Z) | Planung | Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT |
| | | | M 4.52 | (B) | Umsetzg. | Geräteschutz unter Windows NT/2000/XP |
| | | | M 4.53 | (A) | Planung | Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT |
| | | | M 4.54 | (Z) | Umsetzg. | Protokollierung unter Windows NT |
| | | | M 4.55 | (B) | Umsetzg. | Sichere Installation von Windows NT |
| | | | M 4.56 | (B) | Betrieb | Sicheres Löschen unter Windows-Betriebssystemen |
| | | | M 4.57 | (A) | Umsetzg. | Deaktivieren der automatischen CD-ROM-Erkennung |
| | | | M 4.75 | (A) | Umsetzg. | Schutz der Registrierung unter Windows NT/2000/XP |
| | | | M 4.76 | (C) | Planung | Sichere Systemversion von Windows NT |
| | | | M 4.77 | (A) | Umsetzg. | Schutz der Administratorkonten unter Windows NT |
| | | | M 6.42 | (A) | Notfallv. | Erstellung von Rettungsdisketten für Windows NT |
| | | | M 6.44 | (A) | Notfallv. | Datensicherung unter Windows NT |
| | | | M 2.63 | (A) | Planung | Einrichten der Zugriffsrechte |
| | | | M 2.65 | (Z) | Betrieb | Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System |
| | | | M 2.103 | (A) | Planung | Einrichten von Benutzerprofilen unter Windows 95 |
| | | | M 2.104 | (Z) | Planung | Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95 |
| | | | M 3.18 | (A) | Betrieb | Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung |

| | | | | | | |
|---------|-------|---------------------------|---------|-----|-----------|---|
| B 3.207 | (5.7) | Client unter Windows 2000 | M 4.41 | (Z) | Planung | Einsatz angemessener Sicherheitsprodukte für IT-Systeme |
| | | | M 4.56 | (B) | Betrieb | Sicheres Löschen unter Windows-Betriebssystemen |
| | | | M 4.57 | (A) | Umsetzg. | Deaktivieren der automatischen CD-ROM-Erkennung |
| | | | M 4.74 | (A) | Planung | Vernetzte Windows 95 Rechner |
| | | | M 6.45 | (A) | Notfallv. | Datensicherung unter Windows 95 |
| | | | M 6.46 | (A) | Notfallv. | Erstellung von Rettungsdisketten für Windows 95 |
| B 3.208 | (5.8) | Internet-PC | M 2.31 | (B) | Betrieb | Dokumentation der zugelassenen Benutzer und Rechteprofile |
| | | | M 2.32 | (Z) | Umsetzg. | Einrichtung einer eingeschränkten Benutzerumgebung |
| | | | M 2.227 | (A) | Planung | Planung des Windows 2000 Einsatzes |
| | | | M 2.228 | (A) | Planung | Festlegen einer Windows 2000 Sicherheitsrichtlinie |
| | | | M 2.231 | (A) | Planung | Planung der Gruppenrichtlinien unter Windows 2000 |
| | | | M 3.28 | (A) | Umsetzg. | Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer |
| | | | M 4.17 | (A) | Umsetzg. | Sperren und Löschen nicht benötigter Accounts und Terminals |
| | | | M 4.48 | (A) | Umsetzg. | Passwortschutz unter Windows NT/2000/XP |
| | | | M 4.49 | (A) | Umsetzg. | Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System |
| | | | M 4.52 | (A) | Umsetzg. | Geräteschutz unter Windows NT/2000/XP |
| | | | M 4.57 | (A) | Umsetzg. | Deaktivieren der automatischen CD-ROM-Erkennung |
| | | | M 4.75 | (A) | Umsetzg. | Schutz der Registrierung unter Windows NT/2000/XP |
| | | | M 4.136 | (A) | Umsetzg. | Sichere Installation von Windows 2000 |
| | | | M 4.147 | (Z) | Betrieb | Sichere Nutzung von EFS unter Windows 2000/XP |
| | | | M 4.148 | (B) | Betrieb | Überwachung eines Windows 2000/XP Systems |
| | | | M 4.149 | (A) | Umsetzg. | Datei- und Freigabeberechtigungen unter Windows 2000/XP |
| | | | M 4.150 | (A) | Umsetzg. | Konfiguration von Windows 2000 als Workstation |
| | | | M 6.77 | (A) | Notfallv. | Erstellung von Rettungsdisketten für Windows 2000 |
| | | | M 6.78 | (A) | Notfallv. | Datensicherung unter Windows 2000/XP |
| | | | M 2.234 | (A) | Planung | Konzeption von Internet-PCs |
| | | | M 2.235 | (A) | Planung | Richtlinien für die Nutzung von Internet-PCs |
| | | | M 2.313 | (A) | Betrieb | Sichere Anmeldung bei Internet-Diensten |
| | | | M 4.3 | (A) | Betrieb | Regelmäßiger Einsatz eines Anti-Viren-Programms |
| | | | M 4.41 | (Z) | Planung | Einsatz angemessener Sicherheitsprodukte für IT-Systeme |
| | | | M 4.44 | (A) | Betrieb | Prüfung eingehender Dateien auf Makro-Viren |
| | | | M 4.151 | (B) | Umsetzg. | Sichere Installation von Internet-PCs |
| | | | M 4.152 | (B) | Betrieb | Sicherer Betrieb von Internet-PCs |
| | | | M 5.59 | (C) | Umsetzg. | Schutz vor DNS-Spoofing |
| | | | M 5.66 | (B) | Planung | Verwendung von SSL |
| | | | M 5.91 | (Z) | Planung | Einsatz von Personal Firewalls für Internet-PCs |
| | | | M 5.92 | (B) | Planung | Sichere Internet-Anbindung von Internet-PCs |
| | | | M 5.93 | (A) | Betrieb | Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs |
| | | | M 5.94 | (A) | Betrieb | Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs |

| | | | | | | |
|---------|-------|------------------------------|---------|-----|-----------|---|
| B 3.209 | (5.9) | Client unter Windows XP | M 5.95 | (B) | Betrieb | Sicherer E-Commerce bei der Nutzung von Internet-PCs |
| | | | M 5.96 | (A) | Betrieb | Sichere Nutzung von Webmail |
| | | | M 5.98 | (C) | Umsetzg. | Schutz vor Missbrauch kostenpflichtiger Einwahlnummern |
| | | | M 6.79 | (A) | Notfallv. | Datensicherung beim Einsatz von Internet-PCs |
| B 3.301 | (7.3) | Sicherheitgateway (Firewall) | M 2.32 | (Z) | Umsetzg. | Einrichtung einer eingeschränkten Benutzerumgebung |
| | | | M 2.324 | (A) | Planung | Einführung von Windows XP planen |
| | | | M 2.325 | (A) | Planung | Planung der Windows XP Sicherheitsrichtlinie |
| | | | M 2.326 | (A) | Planung | Planung der Windows XP Gruppenrichtlinien |
| | | | M 2.327 | (B) | Planung | Sicherheit beim Fernzugriff unter Windows XP |
| | | | M 2.328 | (B) | Planung | Einsatz von Windows XP auf mobilen Rechnern |
| | | | M 2.329 | (A) | Betrieb | Einführung von Windows XP SP2 |
| | | | M 2.330 | (B) | Betrieb | Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung |
| | | | M 3.28 | (A) | Planung | Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer |
| | | | M 4.48 | (A) | Planung | Passwortschutz unter Windows NT/2000/XP |
| | | | M 4.49 | (A) | Betrieb | Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System |
| | | | M 4.52 | (A) | Betrieb | Geräteschutz unter Windows NT/2000/XP |
| | | | M 4.56 | (C) | Betrieb | Sicheres Löschen unter Windows-Betriebssystemen |
| | | | M 4.57 | (A) | Planung | Deaktivieren der automatischen CD-ROM-Erkennung |
| | | | M 4.75 | (A) | Planung | Schutz der Registrierung unter Windows NT/2000/XP |
| | | | M 4.146 | (A) | Betrieb | Sicherer Betrieb von Windows 2000/XP |
| | | | M 4.147 | (Z) | Planung | Sichere Nutzung von EFS unter Windows 2000/XP |
| | | | M 4.148 | (B) | Betrieb | Überwachung eines Windows 2000/XP Systems |
| | | | M 4.149 | (A) | Planung | Datei- und Freigabeberechtigungen unter Windows 2000/XP |
| | | | M 4.243 | (Z) | Planung | Windows XP Verwaltungswerkzeuge |
| | | | M 4.244 | (A) | Planung | Sichere Windows XP Systemkonfiguration |
| | | | M 4.245 | (A) | Planung | Basiseinstellungen für Windows XP GPOs |
| | | | M 4.246 | (A) | Planung | Konfiguration der Systemdienste unter Windows XP |
| | | | M 4.247 | (A) | Planung | Restriktive Berechtigungsvergabe unter Windows XP |
| | | | M 4.248 | (A) | Umsetzg. | Sichere Installation von Windows XP |
| | | | M 4.249 | (A) | Betrieb | Windows XP Systeme aktuell halten |
| | | | M 5.37 | (B) | Planung | Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz |
| | | | M 5.89 | (A) | Umsetzg. | Konfiguration des sicheren Kanals unter Windows 2000/XP |
| | | | M 5.90 | (Z) | Umsetzg. | Einsatz von IPSec unter Windows 2000/XP |
| | | | M 5.123 | (B) | Planung | Absicherung der Netzwerkkommunikation unter Windows XP |
| | | | M 6.76 | (C) | Notfallv. | Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes |
| | | | M 6.78 | (A) | Notfallv. | Datensicherung unter Windows 2000/XP |
| | | | M 2.70 | (A) | Planung | Entwicklung eines Konzepts für Sicherheitgateways |
| | | | M 2.71 | (A) | Planung | Festlegung einer Policy für ein Sicherheitgateway |
| | | | M 2.73 | (A) | Beschaff. | Auswahl geeigneter Grundstrukturen für Sicherheitgateways |

| | | | |
|------------------------------------|-----|-----------|--|
| M 2.74 | (A) | Beschaff. | Geeignete Auswahl eines Paketfilters |
| M 2.75 | (A) | Beschaff. | Geeignete Auswahl eines Application-Level-Gateways |
| M 2.76 | (A) | Umsetzg. | Auswahl und Einrichtung geeigneter Filterregeln |
| M 2.77 | (A) | Umsetzg. | Integration von Servern in das Sicherheitsgateway |
| M 2.78 | (A) | Betrieb | Sicherer Betrieb eines Sicherheitsgateways |
| M 2.299 | (A) | Beschaff. | Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway |
| M 2.300 | (C) | Aussnd. | Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways |
| M 2.301 | (Z) | Planung | Outsourcing des Sicherheitsgateway |
| M 2.302 | (Z) | Betrieb | Sicherheitsgateways und Hochverfügbarkeit |
| M 3.43 | (C) | Umsetzg. | Schulung der Administratoren des Sicherheitsgateways |
| M 4.47 | (A) | Betrieb | Protokollierung der Sicherheitsgateway-Aktivitäten |
| M 4.93 | (B) | Betrieb | Regelmäßige Integritätsprüfung |
| M 4.100 | (C) | Betrieb | Sicherheitsgateways und aktive Inhalte |
| M 4.101 | (C) | Betrieb | Sicherheitsgateways und Verschlüsselung |
| M 4.222 | (B) | Betrieb | Festlegung geeigneter Einstellungen von Sicherheitsproxies |
| M 4.223 | (B) | Betrieb | Integration von Proxy-Servern in das Sicherheitsgateway |
| M 4.224 | (Z) | Betrieb | Integration von Virtual Private Networks in ein Sicherheitsgateway |
| M 4.225 | (Z) | Betrieb | Einsatz eines Protokollierungsservers in einem Sicherheitsgateway |
| M 4.226 | (Z) | Betrieb | Integration von Virensclannern in ein Sicherheitsgateway |
| M 4.227 | (C) | Betrieb | Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation |
| M 5.39 | (A) | Betrieb | Sicherer Einsatz der Protokolle und Dienste |
| M 5.46 | (A) | Betrieb | Einsatz von Stand-alone-Systemen zur Nutzung des Internets |
| M 5.59 | (A) | Betrieb | Schutz vor DNS-Spoofing |
| M 5.70 | (A) | Betrieb | Adreßumsetzung - NAT (Network Address Translation) |
| M 5.71 | (Z) | Betrieb | Intrusion Detection und Intrusion Response Systeme |
| M 5.115 | (Z) | Betrieb | Integration eines Webserver in ein Sicherheitsgateway |
| M 5.116 | (Z) | Betrieb | Integration eines E-Mailserver in ein Sicherheitsgateway |
| M 5.117 | (Z) | Betrieb | Integration eines Datenbank-Servers in ein Sicherheitsgateway |
| M 5.118 | (Z) | Betrieb | Integration eines DNS-Servers in ein Sicherheitsgateway |
| M 5.119 | (Z) | Betrieb | Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway |
| M 5.120 | (A) | Betrieb | Behandlung von ICMP am Sicherheitsgateway |
| M 6.94 | (C) | Notfallv. | Notfallvorsorge bei Sicherheitsgateways |
| B 3.302 (7.11) Router und Switches | | | |
| M 1.43 | (A) | Umsetzg. | Gesicherte Aufstellung aktiver Netzkomponenten |
| M 2.276 | (Z) | Planung | Funktionsweise eines Routers |
| M 2.277 | (Z) | Planung | Funktionsweise eines Switches |
| M 2.278 | (Z) | Planung | Typische Einsatzszenarien von Routern und Switches |
| M 2.279 | (A) | Planung | Erstellung einer Sicherheitsrichtlinie für Router und Switches |
| M 2.280 | (C) | Beschaff. | Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches |
| M 2.281 | (A) | Betrieb | Dokumentation der Systemkonfiguration von Routern und Switches |

B 3.401 (8.1) TK-Anlage

| | | | |
|---------|-----|-----------|---|
| M 2.282 | (A) | Betrieb | Regelmäßige Kontrolle von Routern und Switches |
| M 2.283 | (B) | Betrieb | Software-Pflege auf Routern und Switches |
| M 2.284 | (C) | Aussnd. | Sichere Außerbetriebnahme von Routern und Switches |
| M 3.38 | (B) | Umsetzg. | Administratorenschulung für Router und Switches |
| M 4.201 | (A) | Umsetzg. | Sichere lokale Grundkonfiguration von Routern und Switches |
| M 4.202 | (A) | Umsetzg. | Sichere Netz-Grundkonfiguration von Routern und Switches |
| M 4.203 | (A) | Umsetzg. | Konfigurations-Checkliste für Router und Switches |
| M 4.204 | (C) | Betrieb | Sichere Administration von Routern und Switches |
| M 4.205 | (C) | Betrieb | Protokollierung bei Routern und Switches |
| M 4.206 | (C) | Betrieb | Sicherung von Switch-Ports |
| M 5.111 | (C) | Umsetzg. | Einrichtung von Access Control Lists auf Routern |
| M 5.112 | (C) | Betrieb | Sicherheitsaspekte von Routing-Protokollen |
| M 6.91 | (C) | Notfallv. | Datensicherung und Recovery bei Routern und Switches |
| M 6.92 | (C) | Notfallv. | Notfallvorsorge bei Routern und Switches |
| M 1.12 | (B) | Planung | Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile |
| M 1.13 | (Z) | Planung | Anordnung schützenswerter Gebäudeteile |
| M 1.25 | (B) | Planung | Überspannungsschutz |
| M 1.28 | (B) | Planung | Lokale unterbrechungsfreie Stromversorgung |
| M 1.30 | (A) | Umsetzg. | Absicherung der Datenträger mit TK-Gebührendaten |
| M 2.27 | (Z) | Planung | Verzicht auf Fernwartung der TK-Anlage |
| M 2.28 | (Z) | Planung | Bereitstellung externer TK-Beratungskapazität |
| M 2.29 | (B) | Umsetzg. | Bedienungsanleitung der TK-Anlage für die Benutzer |
| M 2.105 | (A) | Beschaff. | Beschaffung von TK-Anlagen |
| M 3.12 | (B) | Betrieb | Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne |
| M 3.13 | (B) | Betrieb | Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen |
| M 4.5 | (B) | Betrieb | Protokollierung der TK-Administrationsarbeiten |
| M 4.6 | (C) | Betrieb | Revision der TK-Anlagenkonfiguration |
| M 4.7 | (A) | Umsetzg. | Änderung voreingestellter Passwörter |
| M 4.8 | (A) | Planung | Schutz des TK-Bedienplatzes |
| M 4.10 | (Z) | Umsetzg. | Passwortschutz für TK-Endgeräte |
| M 4.11 | (B) | Umsetzg. | Absicherung der TK-Anlagen-Schnittstellen |
| M 4.12 | (A) | Umsetzg. | Sperrern nicht benötigter TK-Leistungsmerkmale |
| M 4.62 | (Z) | Planung | Einsatz eines D-Kanal-Filters |
| M 5.14 | (A) | Umsetzg. | Absicherung interner Remote-Zugänge |
| M 5.15 | (A) | Umsetzg. | Absicherung externer Remote-Zugänge |
| M 6.10 | (B) | Notfallv. | Notfall-Plan für DFÜ-Ausfall |
| M 6.26 | (B) | Notfallv. | Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten |
| M 6.28 | (Z) | Notfallv. | Vereinbarung über Lieferzeiten "lebensnotwendiger" TK-Baugruppen |
| M 6.29 | (Z) | Notfallv. | TK-Basisanschluss für Notrufe |
| M 6.30 | (Z) | Notfallv. | Katastrophenschaltung |

| | | | | | | |
|---------|-------|------------------|---------|-----|-----------|---|
| B 3.402 | (8.2) | Faxgerät | M 1.37 | (A) | Umsetzg. | Geeignete Aufstellung eines Faxgerätes |
| | | | M 2.47 | (B) | Umsetzg. | Ernennung eines Fax-Verantwortlichen |
| | | | M 2.48 | (Z) | Betrieb | Festlegung berechtigter Faxbediener |
| | | | M 2.49 | (A) | Beschaff. | Beschaffung geeigneter Faxgeräte |
| | | | M 2.50 | (B) | Aussnd. | Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen |
| | | | M 2.51 | (Z) | Betrieb | Fertigung von Kopien eingehender Faxesendungen |
| | | | M 2.52 | (C) | Betrieb | Versorgung und Kontrolle der Verbrauchsgüter |
| | | | M 2.53 | (Z) | Betrieb | Abschalten des Faxgerätes außerhalb der Bürozeiten |
| | | | M 3.15 | (A) | Umsetzg. | Informationen für alle Mitarbeiter über die Faxnutzung |
| | | | M 4.36 | (Z) | Umsetzg. | Sperren bestimmter Faxempfänger-Rufnummern |
| | | | M 4.37 | (Z) | Umsetzg. | Sperren bestimmter Absender-Faxnummern |
| | | | M 4.43 | (Z) | Betrieb | Faxgerät mit automatischer Eingangskuvertierung |
| | | | M 5.24 | (Z) | Betrieb | Nutzung eines geeigneten Faxvorblattes |
| | | | M 5.25 | (A) | Betrieb | Nutzung von Sende- und Empfangsprotokollen |
| | | | M 5.26 | (Z) | Betrieb | Telefonische Ankündigung einer Faxesendung |
| | | | M 5.27 | (Z) | Betrieb | Telefonische Rückversicherung über korrekten Faxempfang |
| | | | M 5.28 | (Z) | Betrieb | Telefonische Rückversicherung über korrekten Faxabsender |
| | | | M 5.29 | (C) | Betrieb | Gelegentliche Kontrolle programmierter Zieladressen und Protokolle |
| | | | M 6.39 | (C) | Notfallv. | Auflistung von Händleradressen zur Fax-Wiederbeschaffung |
| B 3.403 | (8.3) | Anrufbeantworter | M 2.11 | (A) | Planung | Regelung des Passwortgebrauchs |
| | | | M 2.54 | (A) | Beschaff. | Beschaffung geeigneter Anrufbeantworter |
| | | | M 2.55 | (Z) | Umsetzg. | Einsatz eines Sicherungscodes |
| | | | M 2.56 | (A) | Betrieb | Vermeidung schutzbedürftiger Informationen auf dem Anrufbeantworter |
| | | | M 2.57 | (A) | Betrieb | Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche |
| | | | M 2.58 | (Z) | Umsetzg. | Begrenzung der Sprechdauer |
| | | | M 3.16 | (A) | Umsetzg. | Einweisung in die Bedienung des Anrufbeantworters |
| | | | M 4.38 | (A) | Umsetzg. | Abschalten nicht benötigter Leistungsmerkmale |
| | | | M 4.39 | (Z) | Betrieb | Abschalten des Anrufbeantworters bei Anwesenheit |
| | | | M 6.40 | (A) | Notfallv. | Regelmäßige Batterieprüfung/-wechsel |
| B 3.404 | (8.6) | Mobiltelefon | M 2.188 | (A) | Planung | Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung |
| | | | M 2.189 | (A) | Betrieb | Sperrung des Mobiltelefons bei Verlust |
| | | | M 2.190 | (Z) | Beschaff. | Einrichtung eines Mobiltelefon-Pools |
| | | | M 4.114 | (A) | Umsetzg. | Nutzung der Sicherheitsmechanismen von Mobiltelefonen |
| | | | M 4.115 | (B) | Betrieb | Sicherstellung der Energieversorgung von Mobiltelefonen |
| | | | M 4.255 | (A) | Betrieb | Nutzung von IrDA-Schnittstellen |
| | | | M 5.78 | (Z) | Betrieb | Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung |
| | | | M 5.79 | (Z) | Betrieb | Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung |
| | | | M 5.80 | (Z) | Betrieb | Schutz vor Abhören der Raumgespräche über Mobiltelefone |

| | | | | | | |
|---------|-------|----------------------------|---------|-----|-----------|---|
| B 3.405 | (8.7) | PDA | M 5.81 | (B) | Betrieb | Sichere Datenübertragung über Mobiltelefone |
| | | | M 6.72 | (C) | Notfallv. | Ausfallvorsorge bei Mobiltelefonen |
| B 4.1 | (6.7) | Heterogene Netze | M 1.33 | (A) | Betrieb | Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz |
| | | | M 2.218 | (C) | Planung | Regelung der Mitnahme von Datenträgern und IT-Komponenten |
| | | | M 2.303 | (A) | Planung | Festlegung einer Strategie für den Einsatz von PDAs |
| | | | M 2.304 | (A) | Planung | Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung |
| | | | M 2.305 | (B) | Beschaff. | Geeignete Auswahl von PDAs |
| | | | M 2.306 | (A) | Aussnd. | Verlustmeldung |
| | | | M 4.3 | (A) | Betrieb | Regelmäßiger Einsatz eines Anti-Viren-Programms |
| | | | M 4.31 | (A) | Betrieb | Sicherstellung der Energieversorgung im mobilen Einsatz |
| | | | M 4.228 | (A) | Betrieb | Nutzung der Sicherheitsmechanismen von PDAs |
| | | | M 4.229 | (C) | Betrieb | Sicherer Betrieb von PDAs |
| | | | M 4.230 | (Z) | Betrieb | Zentrale Administration von PDAs |
| | | | M 4.231 | (Z) | Beschaff. | Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs |
| | | | M 4.232 | (Z) | Betrieb | Sichere Nutzung von Zusatzspeicherkarten |
| | | | M 4.255 | (A) | Betrieb | Nutzung von IrDA-Schnittstellen |
| | | | M 5.121 | (B) | Umsetzg. | Sichere Kommunikation von unterwegs |
| | | | M 6.95 | (C) | Notfallv. | Ausfallvorsorge und Datensicherung bei PDAs |
| | | | M 2.139 | (A) | Planung | Ist-Aufnahme der aktuellen Netzsituation |
| | | | M 2.140 | (Z) | Planung | Analyse der aktuellen Netzsituation |
| | | | M 2.141 | (B) | Planung | Entwicklung eines Netzkonzeptes |
| | | | M 2.142 | (B) | Planung | Entwicklung eines Netz-Realisierungsplans |
| B 4.2 | (6.8) | Netz- und Systemmanagement | M 4.7 | (A) | Umsetzg. | Änderung voreingestellter Passwörter |
| | | | M 4.79 | (A) | Planung | Sichere Zugriffsmechanismen bei lokaler Administration |
| | | | M 4.80 | (B) | Planung | Sichere Zugriffsmechanismen bei Fernadministration |
| | | | M 4.81 | (B) | Betrieb | Audit und Protokollierung der Aktivitäten im Netz |
| | | | M 4.82 | (A) | Umsetzg. | Sichere Konfiguration der aktiven Netzkomponenten |
| | | | M 4.83 | (C) | Betrieb | Update/Upgrade von Soft- und Hardware im Netzbereich |
| | | | M 5.2 | (A) | Planung | Auswahl einer geeigneten Netz-Topographie |
| | | | M 5.7 | (A) | Umsetzg. | Netzverwaltung |
| | | | M 5.13 | (A) | Planung | Geeigneter Einsatz von Elementen zur Netzkopplung |
| | | | M 5.60 | (A) | Planung | Auswahl einer geeigneten Backbone-Technologie |
| | | | M 5.61 | (A) | Planung | Geeignete physikalische Segmentierung |
| | | | M 5.62 | (Z) | Planung | Geeignete logische Segmentierung |
| | | | M 5.77 | (Z) | Planung | Bildung von Teilnetzen |
| | | | M 6.52 | (A) | Notfallv. | Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten |
| | | | M 6.53 | (Z) | Notfallv. | Redundante Auslegung der Netzkomponenten |
| | | | M 6.54 | (B) | Notfallv. | Verhaltensregeln nach Verlust der Netzintegrität |

| | | | | | | |
|-------|-------|---------------|---------|-----|-----------|---|
| B 4.3 | (7.2) | Modem | M 2.143 | (A) | Planung | Entwicklung eines Netzmanagementkonzeptes |
| | | | M 2.144 | (A) | Planung | Geeignete Auswahl eines Netzmanagement-Protokolls |
| | | | M 2.145 | (B) | Beschaff. | Anforderungen an ein Netzmanagement-Tool |
| | | | M 2.146 | (A) | Betrieb | Sicherer Betrieb eines Netzmanagementsystems |
| | | | M 2.168 | (A) | Planung | IT-System-Analyse vor Einführung eines Systemmanagementsystems |
| | | | M 2.169 | (A) | Planung | Entwickeln einer Systemmanagementstrategie |
| | | | M 2.170 | (A) | Beschaff. | Anforderungen an ein Systemmanagementsystem |
| | | | M 2.171 | (A) | Beschaff. | Geeignete Auswahl eines Systemmanagement-Produktes |
| | | | M 4.91 | (A) | Umsetzg. | Sichere Installation eines Systemmanagementsystems |
| | | | M 4.92 | (A) | Betrieb | Sicherer Betrieb eines Systemmanagementsystems |
| | | | M 6.57 | (C) | Notfallv. | Erstellen eines Notfallplans für den Ausfall des Managementsystems |
| | | | M 1.25 | (Z) | Planung | Überspannungsschutz |
| | | | M 1.38 | (A) | Umsetzg. | Geeignete Aufstellung eines Modems |
| B 4.4 | (7.6) | Remote Access | M 2.42 | (B) | Planung | Festlegung der möglichen Kommunikationspartner |
| | | | M 2.46 | (Z) | Planung | Geeignetes Schlüsselmanagement |
| | | | M 2.59 | (A) | Beschaff. | Auswahl eines geeigneten Modems in der Beschaffung |
| | | | M 2.60 | (A) | Betrieb | Sichere Administration eines Modems |
| | | | M 2.61 | (A) | Planung | Regelung des Modem-Einsatzes |
| | | | M 2.204 | (A) | Umsetzg. | Verhinderung ungesicherter Netzzugänge |
| | | | M 3.17 | (A) | Betrieb | Einweisung des Personals in die Modem-Benutzung |
| | | | M 4.7 | (A) | Umsetzg. | Änderung voreingestellter Passwörter |
| | | | M 4.33 | (A) | Betrieb | Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung |
| | | | M 4.34 | (Z) | Planung | Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen |
| | | | M 5.30 | (Z) | Umsetzg. | Aktivierung einer vorhandenen Callback-Option |
| | | | M 5.31 | (A) | Umsetzg. | Geeignete Modem-Konfiguration |
| | | | M 5.32 | (A) | Planung | Sicherer Einsatz von Kommunikationssoftware |
| | | | M 5.33 | (A) | Betrieb | Absicherung der per Modem durchgeführten Fernwartung |
| | | | M 5.44 | (Z) | Betrieb | Einseitiger Verbindungsaufbau |
| | | | M 2.183 | (A) | Planung | Durchführung einer RAS-Anforderungsanalyse |
| | | | M 2.184 | (A) | Planung | Entwicklung eines RAS-Konzeptes |
| | | | M 2.185 | (A) | Planung | Auswahl einer geeigneten RAS-Systemarchitektur |
| | | | M 2.186 | (A) | Beschaff. | Geeignete Auswahl eines RAS-Produktes |
| | | | M 2.187 | (A) | Planung | Festlegen einer RAS-Sicherheitsrichtlinie |
| | | | M 2.205 | (A) | Planung | Übertragung und Abruf personenbezogener Daten |
| | | | M 4.110 | (A) | Umsetzg. | Sichere Installation des RAS-Systems |
| | | | M 4.111 | (A) | Umsetzg. | Sichere Konfiguration des RAS-Systems |
| | | | M 4.112 | (A) | Betrieb | Sicherer Betrieb des RAS-Systems |
| | | | M 4.113 | (Z) | Planung | Nutzung eines Authentisierungsservers beim RAS-Einsatz |
| | | | M 4.233 | (B) | Aussnd. | Sperrung nicht mehr benötigter RAS-Zugänge |

| | | | | | | |
|-------|-------|--|---------|-----|-----------|---|
| B 4.5 | (8.4) | LAN-Anbindung eines IT-Systems über ISDN | M 5.76 | (Z) | Planung | Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation |
| | | | M 6.70 | (B) | Notfallv. | Erstellen eines Notfallplans für den Ausfall des RAS-Systems |
| | | | M 6.71 | (B) | Notfallv. | Datensicherung bei mobiler Nutzung des IT-Systems |
| B 5.1 | (6.3) | Peer-to-Peer-Dienste | M 1.25 | (B) | Planung | Überspannungsschutz |
| | | | M 1.43 | (A) | Umsetzg. | Gesicherte Aufstellung aktiver Netzkomponenten |
| | | | M 2.42 | (A) | Planung | Festlegung der möglichen Kommunikationspartner |
| | | | M 2.46 | (Z) | Planung | Geeignetes Schlüsselmanagement |
| | | | M 2.64 | (A) | Betrieb | Kontrolle der Protokolldateien |
| | | | M 2.106 | (A) | Beschaff. | Auswahl geeigneter ISDN-Karten in der Beschaffung |
| | | | M 2.107 | (A) | Umsetzg. | Dokumentation der ISDN-Karten-Konfiguration |
| | | | M 2.108 | (Z) | Planung | Verzicht auf Fernwartung der ISDN-Netzkoppelemente |
| | | | M 2.109 | (A) | Umsetzg. | Rechtevergabe für den Fernzugriff |
| | | | M 2.204 | (A) | Umsetzg. | Verhinderung ungesicherter Netzzugänge |
| | | | M 4.7 | (A) | Umsetzg. | Änderung voreingestellter Passwörter |
| | | | M 4.34 | (Z) | Planung | Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen |
| | | | M 4.59 | (A) | Umsetzg. | Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten |
| | | | M 4.60 | (A) | Umsetzg. | Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten |
| | | | M 4.61 | (A) | Umsetzg. | Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten |
| | | | M 4.62 | (Z) | Planung | Einsatz eines D-Kanal-Filters |
| | | | M 5.29 | (C) | Betrieb | Gelegentliche Kontrolle programmierter Zieladressen und Protokolle |
| | | | M 5.32 | (A) | Planung | Sicherer Einsatz von Kommunikationssoftware |
| | | | M 5.47 | (Z) | Planung | Einrichten einer Closed User Group |
| | | | M 5.48 | (A) | Umsetzg. | Authentisierung mittels CLIP/COLP |
| | | | M 5.49 | (A) | Umsetzg. | Callback basierend auf CLIP/COLP |
| | | | M 5.50 | (A) | Umsetzg. | Authentisierung mittels PAP/CHAP |
| B 5.2 | (7.1) | Datenträgeraustausch | M 2.67 | (A) | Planung | Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste |
| | | | M 2.68 | (B) | Betrieb | Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten |
| | | | M 2.94 | (B) | Umsetzg. | Freigabe von Verzeichnissen unter Windows NT |
| | | | M 3.19 | (A) | Umsetzg. | Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten |
| | | | M 4.45 | (A) | Umsetzg. | Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW |
| | | | M 4.46 | (A) | Betrieb | Nutzung des Anmeldepasswortes unter WfW und Windows 95 |
| | | | M 4.58 | (B) | Betrieb | Freigabe von Verzeichnissen unter Windows 95 |
| | | | M 4.149 | (A) | Umsetzg. | Datei- und Freigabeberechtigungen unter Windows 2000/XP |
| | | | M 5.37 | (B) | Planung | Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz |
| | | | M 5.82 | (A) | Betrieb | Sicherer Einsatz von SAMBA |
| B 5.2 | (7.1) | Datenträgeraustausch | M 1.36 | (A) | Betrieb | Sichere Aufbewahrung der Datenträger vor und nach Versand |

| | | | | | | |
|-------|-------|--------|---------|-----|-----------|--|
| B 5.3 | (7.4) | E-Mail | M 2.3 | (B) | Planung | Datenträgerverwaltung |
| | | | M 2.42 | (B) | Planung | Festlegung der möglichen Kommunikationspartner |
| | | | M 2.43 | (A) | Betrieb | Ausreichende Kennzeichnung der Datenträger beim Versand |
| | | | M 2.44 | (A) | Betrieb | Sichere Verpackung der Datenträger |
| | | | M 2.45 | (A) | Planung | Regelung des Datenträgeraustausches |
| | | | M 2.46 | (Z) | Planung | Geeignetes Schlüsselmanagement |
| | | | M 3.14 | (B) | Betrieb | Einweisung des Personals in den geregelten Ablauf eines Datenträgeraustausches |
| | | | M 4.32 | (B) | Aussnd. | Physikalisches Löschen der Datenträger vor und nach Verwendung |
| | | | M 4.33 | (A) | Betrieb | Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung |
| | | | M 4.34 | (Z) | Planung | Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen |
| | | | M 4.35 | (Z) | Betrieb | Verifizieren der zu übertragenden Daten vor Versand |
| | | | M 5.22 | (B) | Umsetzg. | Kompatibilitätsprüfung des Sender- und Empfängersystems |
| | | | M 5.23 | (A) | Umsetzg. | Auswahl einer geeigneten Versandart für den Datenträger |
| | | | M 6.38 | (A) | Notfallv. | Sicherungskopie der übermittelten Daten |
| | | | M 2.30 | (A) | Planung | Regelung für die Einrichtung von Benutzern / Benutzergruppen |
| | | | M 2.42 | (B) | Planung | Festlegung der möglichen Kommunikationspartner |
| | | | M 2.46 | (Z) | Planung | Geeignetes Schlüsselmanagement |
| | | | M 2.118 | (A) | Planung | Konzeption der sicheren E-Mail-Nutzung |
| | | | M 2.119 | (A) | Planung | Regelung für den Einsatz von E-Mail |
| | | | M 2.120 | (A) | Umsetzg. | Einrichtung einer Poststelle |
| | | | M 2.121 | (B) | Betrieb | Regelmäßiges Löschen von E-Mails |
| | | | M 2.122 | (B) | Planung | Einheitliche E-Mail-Adressen |
| | | | M 2.123 | (B) | Beschaff. | Auswahl eines Mailproviders |
| | | | M 2.274 | (A) | Planung | Vertretungsregelungen bei E-Mail-Nutzung |
| | | | M 2.275 | (Z) | Umsetzg. | Einrichtung funktionsbezogener E-Mailadressen |
| | | | M 4.33 | (A) | Betrieb | Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung |
| | | | M 4.34 | (Z) | Betrieb | Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen |
| | | | M 4.44 | (A) | Betrieb | Prüfung eingehender Dateien auf Makro-Viren |
| | | | M 4.64 | (C) | Betrieb | Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen |
| | | | M 4.199 | (B) | Betrieb | Vermeidung gefährlicher Dateiformate |
| | | | M 5.22 | (B) | Umsetzg. | Kompatibilitätsprüfung des Sender- und Empfängersystems |
| | | | M 5.32 | (A) | Umsetzg. | Sicherer Einsatz von Kommunikationssoftware |
| | | | M 5.53 | (B) | Betrieb | Schutz vor Mailbomben |
| | | | M 5.54 | (B) | Betrieb | Schutz vor Mailüberlastung und Spam |
| | | | M 5.55 | (B) | Betrieb | Kontrolle von Alias-Dateien und Verteilerlisten |
| | | | M 5.56 | (A) | Betrieb | Sicherer Betrieb eines Mailservers |
| | | | M 5.57 | (A) | Umsetzg. | Sichere Konfiguration der Mail-Clients |
| | | | M 5.63 | (Z) | Planung | Einsatz von GnuPG oder PGP |
| | | | M 5.67 | (Z) | Planung | Verwendung eines Zeitstempel-Dienstes |

| | | | | | | |
|-------|-------|-------------|---------|-----|-----------|--|
| B 5.4 | (7.5) | Webserver | M 5.108 | (Z) | Planung | Kryptographische Absicherung von E-Mail |
| | | | M 5.109 | (Z) | Betrieb | Einsatz eines E-Mail-Scanners auf dem Mailserver |
| | | | M 5.110 | (Z) | Planung | Absicherung von E-Mail mit SPHINX (S/MIME) |
| | | | M 6.38 | (A) | Notfallv. | Sicherungskopie der übermittelten Daten |
| | | | M 6.90 | (C) | Notfallv. | Datensicherung und Archivierung von E-Mails |
| | | | M 2.172 | (A) | Planung | Entwicklung eines Konzeptes für die WWW-Nutzung |
| | | | M 2.173 | (A) | Planung | Festlegung einer WWW-Sicherheitsstrategie |
| | | | M 2.174 | (A) | Betrieb | Sicherer Betrieb eines WWW-Servers |
| | | | M 2.175 | (A) | Planung | Aufbau eines WWW-Servers |
| | | | M 2.176 | (B) | Beschaff. | Geeignete Auswahl eines Internet Service Providers |
| | | | M 2.271 | (A) | Planung | Festlegung einer Sicherheitsstrategie für den WWW-Zugang |
| | | | M 2.272 | (A) | Planung | Einrichtung eines WWW-Redaktionsteams |
| | | | M 2.273 | (A) | Betrieb | Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates |
| | | | M 2.298 | (Z) | Betrieb | Verwaltung von Internet-Domainnamen |
| | | | M 4.33 | (A) | Betrieb | Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung |
| | | | M 4.34 | (Z) | Betrieb | Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen |
| | | | M 4.64 | (C) | Betrieb | Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen |
| | | | M 4.78 | (A) | Betrieb | Sorgfältige Durchführung von Konfigurationsänderungen |
| | | | M 4.93 | (B) | Betrieb | Regelmäßige Integritätsprüfung |
| B 5.5 | (7.7) | Lotus Notes | M 4.94 | (A) | Umsetzg. | Schutz der WWW-Dateien |
| | | | M 4.95 | (A) | Umsetzg. | Minimales Betriebssystem |
| | | | M 4.96 | (Z) | Umsetzg. | Abschaltung von DNS |
| | | | M 4.97 | (Z) | Umsetzg. | Ein Dienst pro Server |
| | | | M 4.98 | (A) | Umsetzg. | Kommunikation durch Paketfilter auf Minimum beschränken |
| | | | M 4.99 | (C) | Umsetzg. | Schutz gegen nachträgliche Veränderungen von Informationen |
| | | | M 4.176 | (B) | Planung | Auswahl einer Authentisierungsmethode für Webangebote |
| | | | M 4.177 | (B) | Betrieb | Sicherstellung der Integrität und Authentizität von Softwarepaketen |
| | | | M 5.59 | (A) | Betrieb | Schutz vor DNS-Spoofing |
| | | | M 5.64 | (Z) | Planung | Secure Shell |
| | | | M 5.66 | (Z) | Planung | Verwendung von SSL |
| | | | M 5.69 | (A) | Planung | Schutz vor aktiven Inhalten |
| | | | M 6.88 | (B) | Notfallv. | Erstellen eines Notfallplans für den Webserver |
| | | | M 2.206 | (A) | Planung | Planung des Einsatzes von Lotus Notes |
| | | | M 2.207 | (A) | Planung | Festlegen einer Sicherheitsrichtlinie für Lotus Notes |
| | | | M 2.208 | (A) | Planung | Planung der Domänen und der Zertifikathierarchie von Lotus Notes |
| | | | M 2.209 | (B) | Planung | Planung des Einsatzes von Lotus Notes im Intranet |
| | | | M 2.210 | (B) | Planung | Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff |
| | | | M 2.211 | (A) | Planung | Planung des Einsatzes von Lotus Notes in einer DMZ |

| | | | |
|---------|-----|-----------|--|
| M 3.24 | (A) | Umsetzg. | Schulung zur Lotus Notes Systemarchitektur für Administratoren |
| M 3.25 | (A) | Umsetzg. | Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer |
| M 4.116 | (A) | Umsetzg. | Sichere Installation von Lotus Notes |
| M 4.117 | (A) | Umsetzg. | Sichere Konfiguration eines Lotus Notes Servers |
| M 4.118 | (A) | Umsetzg. | Konfiguration als Lotus Notes Server |
| M 4.119 | (A) | Umsetzg. | Einrichten von Zugangsbeschränkungen auf Lotus Notes Server |
| M 4.120 | (A) | Umsetzg. | Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken |
| M 4.121 | (A) | Umsetzg. | Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes |
| M 4.122 | (B) | Umsetzg. | Konfiguration für den Browser-Zugriff auf Lotus Notes |
| M 4.123 | (B) | Umsetzg. | Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes |
| M 4.124 | (A) | Umsetzg. | Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes |
| M 4.125 | (A) | Umsetzg. | Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken |
| | | | |
| M 4.126 | (A) | Umsetzg. | Sichere Konfiguration eines Lotus Notes Clients |
| M 4.127 | (A) | Umsetzg. | Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes |
| M 4.128 | (A) | Betrieb | Sicherer Betrieb von Lotus Notes |
| M 4.129 | (A) | Betrieb | Sicherer Umgang mit Notes-ID-Dateien |
| M 4.130 | (A) | Betrieb | Sicherheitsmaßnahmen nach dem Anlegen neuer Lotus Notes Datenbanken |
| M 4.131 | (Z) | Planung | Verschlüsselung von Lotus Notes Datenbanken |
| M 4.132 | (C) | Betrieb | Überwachen eines Lotus Notes-Systems |
| M 5.84 | (Z) | Betrieb | Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation |
| M 5.85 | (Z) | Betrieb | Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail |
| M 5.86 | (C) | Betrieb | Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes |
| M 6.49 | (A) | Notfallv. | Datensicherung einer Datenbank |
| M 6.73 | (B) | Notfallv. | Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems |
| | | | |
| M 2.178 | (A) | Planung | Erstellung einer Sicherheitsleitlinie für die Faxnutzung |
| M 2.179 | (A) | Planung | Regelungen für den Faxserver-Einsatz |
| M 2.180 | (A) | Umsetzg. | Einrichten einer Fax-Poststelle |
| M 2.181 | (A) | Beschaff. | Auswahl eines geeigneten Faxservers |
| M 3.15 | (A) | Betrieb | Informationen für alle Mitarbeiter über die Faxnutzung |
| M 4.36 | (Z) | Umsetzg. | Sperrern bestimmter Faxempfänger-Rufnummern |
| M 4.37 | (Z) | Umsetzg. | Sperrern bestimmter Absender-Faxnummern |
| M 5.24 | (Z) | Betrieb | Nutzung eines geeigneten Faxvorblattes |
| M 5.25 | (A) | Betrieb | Nutzung von Sende- und Empfangsprotokollen |
| M 5.26 | (Z) | Betrieb | Telefonische Ankündigung einer Faxsendung |
| M 5.27 | (Z) | Betrieb | Telefonische Rückversicherung über korrekten Faxempfang |
| M 5.28 | (Z) | Betrieb | Telefonische Rückversicherung über korrekten Faxabsender |
| M 5.73 | (A) | Betrieb | Sicherer Betrieb eines Faxservers |
| M 5.74 | (A) | Betrieb | Pflege der Faxserver-Adressbücher und der Verteillisten |
| M 5.75 | (Z) | Betrieb | Schutz vor Überlastung des Faxservers |

B 5.6 (8.5) Faxserver

| | | | | | | |
|-------|-------|-------------|---------|-----|-----------|--|
| B 5.7 | (9.2) | Datenbanken | M 6.69 | (B) | Notfallv. | Notfallvorsorge und Ausfallsicherheit bei Faxservern |
| | | | M 2.31 | (A) | Betrieb | Dokumentation der zugelassenen Benutzer und Rechteprofile |
| | | | M 2.34 | (A) | Betrieb | Dokumentation der Veränderungen an einem bestehenden System |
| | | | M 2.65 | (B) | Betrieb | Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System |
| | | | M 2.80 | (A) | Planung | Erstellung eines Anforderungskatalogs für Standardsoftware |
| | | | M 2.124 | (A) | Beschaff. | Geeignete Auswahl einer Datenbank-Software |
| | | | M 2.125 | (A) | Umsetzg. | Installation und Konfiguration einer Datenbank |
| | | | M 2.126 | (A) | Planung | Erstellung eines Datenbanksicherheitskonzeptes |
| | | | M 2.127 | (B) | Umsetzg. | Inferenzprävention |
| | | | M 2.128 | (A) | Umsetzg. | Zugangskontrolle einer Datenbank |
| | | | M 2.129 | (A) | Umsetzg. | Zugriffskontrolle einer Datenbank |
| | | | M 2.130 | (A) | Betrieb | Gewährleistung der Datenbankintegrität |
| | | | M 2.131 | (C) | Planung | Aufteilung von Administrationstätigkeiten bei Datenbanksystemen |
| | | | M 2.132 | (A) | Planung | Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen |
| | | | M 2.133 | (A) | Betrieb | Kontrolle der Protokolldateien eines Datenbanksystems |
| | | | M 2.134 | (B) | Planung | Richtlinien für Datenbank-Anfragen |
| | | | M 2.135 | (C) | Umsetzg. | Gesicherte Datenübernahme in eine Datenbank |
| | | | M 3.18 | (A) | Betrieb | Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung |
| | | | M 4.7 | (A) | Umsetzg. | Änderung voreingestellter Passwörter |
| | | | M 4.67 | (A) | Umsetzg. | Sperren und Löschen nicht benötigter Datenbank-Accounts |
| | | | M 4.68 | (A) | Betrieb | Sicherstellung einer konsistenten Datenbankverwaltung |
| | | | M 4.69 | (B) | Betrieb | Regelmäßiger Sicherheitscheck der Datenbank |
| | | | M 4.70 | (C) | Betrieb | Durchführung einer Datenbanküberwachung |
| | | | M 4.71 | (C) | Umsetzg. | Restriktive Handhabung von Datenbank-Links |
| | | | M 4.72 | (Z) | Planung | Datenbank-Verschlüsselung |
| | | | M 4.73 | (C) | Planung | Festlegung von Obergrenzen für selektierbare Datensätze |
| | | | M 5.58 | (B) | Umsetzg. | Installation von ODBC-Treibern |
| | | | M 6.48 | (A) | Notfallv. | Verhaltensregeln nach Verlust der Datenbankintegrität |
| | | | M 6.49 | (A) | Notfallv. | Datensicherung einer Datenbank |
| | | | M 6.50 | (A) | Notfallv. | Archivierung von Datenbeständen |
| | | | M 6.51 | (B) | Notfallv. | Wiederherstellung einer Datenbank |
| B 5.8 | (9.3) | Telearbeit | M 2.113 | (A) | Planung | Regelungen für Telearbeit |
| | | | M 2.114 | (A) | Planung | Informationsfluss zwischen Telearbeiter und Institution |
| | | | M 2.115 | (B) | Planung | Betreuungs- und Wartungskonzept für Telearbeitsplätze |
| | | | M 2.116 | (A) | Planung | Geregelte Nutzung der Kommunikationsmöglichkeiten |
| | | | M 2.117 | (A) | Planung | Regelung der Zugriffsmöglichkeiten des Telearbeiters |
| | | | M 2.205 | (C) | Planung | Übertragung und Abruf personenbezogener Daten |
| | | | M 2.241 | (C) | Planung | Durchführung einer Anforderungsanalyse für den Telearbeitsplatz |
| | | | M 3.21 | (A) | Betrieb | Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters |

| | | | | | | |
|--------|-------|-----------------------------|---------|-----|-----------|--|
| B 5.9 | (9.4) | Novell eDirectory | M 3.22 | (B) | Betrieb | Vertretungsregelung für Telearbeit |
| | | | M 4.3 | (A) | Betrieb | Regelmäßiger Einsatz eines Anti-Viren-Programms |
| | | | M 4.33 | (A) | Betrieb | Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung |
| | | | M 4.63 | (A) | Umsetzg. | Sicherheitstechnische Anforderungen an den Telearbeitsrechner |
| | | | M 5.51 | (A) | Umsetzg. | Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution |
| | | | M 5.52 | (A) | Umsetzg. | Sicherheitstechnische Anforderungen an den Kommunikationsrechner |
| | | | M 6.38 | (B) | Notfallv. | Sicherungskopie der übermittelten Daten |
| | | | M 6.47 | (B) | Notfallv. | Datensicherung bei der Telearbeit |
| | | | M 2.236 | (A) | Planung | Planung des Einsatzes von Novell eDirectory |
| | | | M 2.237 | (B) | Planung | Planung der Partitionierung und Replikation im Novell eDirectory |
| | | | M 2.238 | (A) | Planung | Festlegung einer Sicherheitsrichtlinie für Novell eDirectory |
| | | | M 2.239 | (A) | Planung | Planung des Einsatzes von Novell eDirectory im Intranet |
| | | | M 2.240 | (A) | Planung | Planung des Einsatzes von Novell eDirectory im Extranet |
| | | | M 3.29 | (A) | Umsetzg. | Schulung zur Administration von Novell eDirectory |
| | | | M 3.30 | (A) | Umsetzg. | Schulung zum Einsatz von Novell eDirectory Clientsoftware |
| | | | M 4.153 | (A) | Umsetzg. | Sichere Installation von Novell eDirectory |
| | | | M 4.154 | (A) | Umsetzg. | Sichere Installation der Novell eDirectory Clientsoftware |
| | | | M 4.155 | (A) | Umsetzg. | Sichere Konfiguration von Novell eDirectory |
| | | | M 4.156 | (A) | Umsetzg. | Sichere Konfiguration der Novell eDirectory Clientsoftware |
| B 5.10 | (7.8) | Internet Information Server | M 4.157 | (A) | Umsetzg. | Einrichten von Zugriffsberechtigungen auf Novell eDirectory |
| | | | M 4.158 | (B) | Umsetzg. | Einrichten des LDAP-Zugriffs auf Novell eDirectory |
| | | | M 4.159 | (A) | Betrieb | Sicherer Betrieb von Novell eDirectory |
| | | | M 4.160 | (B) | Betrieb | Überwachen von Novell eDirectory |
| | | | M 5.97 | (B) | Betrieb | Absicherung der Kommunikation mit Novell eDirectory |
| | | | M 6.80 | (A) | Notfallv. | Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes |
| | | | M 6.81 | (A) | Notfallv. | Erstellen von Datensicherungen für Novell eDirectory |
| | | | M 2.267 | (A) | Planung | Planen des IIS-Einsatzes |
| | | | M 2.268 | (A) | Planung | Festlegung einer IIS-Sicherheitsrichtlinie |
| | | | M 3.36 | (A) | Umsetzg. | Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS |
| | | | M 4.174 | (A) | Umsetzg. | Vorbereitung der Installation von Windows NT/2000 für den IIS |
| | | | M 4.175 | (A) | Umsetzg. | Sichere Konfiguration von Windows NT/2000 für den IIS |
| | | | M 4.178 | (A) | Umsetzg. | Absicherung der Administrator- und Benutzerkonten beim IIS-Einsatz |
| | | | M 4.179 | (A) | Umsetzg. | Schutz von sicherheitskritischen Dateien beim IIS-Einsatz |
| | | | M 4.180 | (A) | Umsetzg. | Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS |
| | | | M 4.181 | (A) | Umsetzg. | Ausführen des IIS in einem separaten Prozess |
| | | | M 4.182 | (B) | Betrieb | Überwachen des IIS-Systems |
| | | | M 4.183 | (A) | Betrieb | Sicherstellen der Verfügbarkeit und Performance des IIS |
| | | | M 4.184 | (A) | Umsetzg. | Deaktivieren nicht benötigter Dienste beim IIS-Einsatz |

| | | | | | | |
|--------|--------|------------------------------|---------|-----|-----------|---|
| B 5.11 | (7.9) | Apache Webserver | M 4.185 | (A) | Umsetzg. | Absichern von virtuellen Verzeichnissen und Web-Anwendungen beim IIS-Einsatz |
| | | | M 4.186 | (A) | Umsetzg. | Entfernen von Beispieldateien und Administrations-Scripts des IIS |
| | | | M 4.187 | (A) | Umsetzg. | Entfernen der FrontPage Server-Erweiterung des IIS |
| | | | M 4.188 | (B) | Umsetzg. | Prüfen der Benutzereingaben beim IIS-Einsatz |
| | | | M 4.189 | (B) | Umsetzg. | Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz |
| | | | M 4.190 | (B) | Umsetzg. | Entfernen der RDS-Unterstützung des IIS |
| | | | M 5.101 | (B) | Umsetzg. | Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz |
| | | | M 5.102 | (B) | Umsetzg. | Installation von URL-Filtern beim IIS-Einsatz |
| | | | M 5.103 | (B) | Umsetzg. | Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz |
| | | | M 5.104 | (C) | Umsetzg. | Konfiguration des TCP/IP-Filters beim IIS-Einsatz |
| | | | M 5.105 | (C) | Umsetzg. | Vorbeugen vor SYN-Attacken auf den IIS |
| | | | M 5.106 | (A) | Umsetzg. | Entfernen nicht vertrauenswürdiger Root-Zertifikate beim IIS-Einsatz |
| | | | M 6.85 | (C) | Notfallv. | Erstellung eines Notfallplans für den Ausfall des IIS |
| | | | M 6.86 | (B) | Umsetzg. | Schutz vor schädlichem Code auf dem IIS |
| | | | M 6.87 | (A) | Notfallv. | Datensicherung auf dem IIS |
| B 5.12 | (7.10) | Exchange 2000 / Outlook 2000 | M 2.269 | (A) | Planung | Planung des Einsatzes eines Apache Webserver |
| | | | M 2.270 | (Z) | Planung | Planung des SSL-Einsatzes beim Apache Webserver (zusätzlich) |
| | | | M 3.37 | (A) | Umsetzg. | Schulung der Administratoren eines Apache-Webserver |
| | | | M 4.191 | (A) | Beschaff. | Überprüfung der Integrität und Authentizität der Apache-Pakete |
| | | | M 4.192 | (A) | Umsetzg. | Konfiguration des Betriebssystems für einen Apache-Webserver |
| | | | M 4.193 | (A) | Umsetzg. | Sichere Installation eines Apache-Webserver |
| | | | M 4.194 | (A) | Umsetzg. | Sichere Grundkonfiguration eines Apache-Webserver |
| | | | M 4.195 | (A) | Umsetzg. | Konfiguration der Zugriffssteuerung beim Apache-Webserver |
| | | | M 4.196 | (A) | Betrieb | Sicherer Betrieb eines Apache-Webserver |
| | | | M 4.197 | (B) | Umsetzg. | Servererweiterungen für dynamische Webseiten beim Apache-Webserver |
| | | | M 4.198 | (Z) | Umsetzg. | Installation eines Apache-Webserver in einem chroot-Käfig |
| | | | M 5.107 | (Z) | Umsetzg. | Verwendung von SSL im Apache-Webserver |
| | | | M 6.89 | (A) | Notfallv. | Notfallvorsorge für einen Apache-Webserver |
| | | | M 2.247 | (A) | Planung | Planung des Einsatzes von Exchange/Outlook 2000 |
| | | | M 2.248 | (A) | Planung | Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000 |
| | | | M 2.249 | (B) | Planung | Planung der Migration von "Exchange 5.5-Servern" nach "Exchange 2000" |
| | | | M 3.31 | (A) | Umsetzg. | Schulung zur Systemarchitektur und Sicherheit von Exchange 2000 für Administratoren |
| | | | M 3.32 | (A) | Umsetzg. | Schulung zu Sicherheitsmechanismen von Outlook 2000 für Benutzer |
| | | | M 4.161 | (A) | Umsetzg. | Sichere Installation von Exchange/Outlook 2000 |
| | | | M 4.162 | (A) | Umsetzg. | Sichere Konfiguration von Exchange 2000 Servern |
| | | | M 4.163 | (A) | Umsetzg. | Zugriffsrechte auf Exchange 2000 Objekte |
| | | | M 4.164 | (A) | Umsetzg. | Browser-Zugriff auf Exchange 2000 |
| | | | M 4.165 | (A) | Umsetzg. | Sichere Konfiguration von Outlook 2000 |
| | | | M 4.166 | (A) | Betrieb | Sicherer Betrieb von Exchange/Outlook 2000 |

| | | | |
|---------|-----|-----------|---|
| M 4.167 | (B) | Betrieb | Überwachung und Protokollierung von Exchange 2000 Systemen |
| M 5.99 | (C) | Umsetzg. | SSL/TLS-Absicherung für Exchange 2000 |
| M 5.100 | (Z) | Betrieb | Einsatz von Verschlüsselungs- und Signaturverfahren für die Exchange 2000 Kommunikation |
| M 6.82 | (C) | Notfallv. | Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen |