## Inhaltlich geänderte Maßnahmen

| Nr. | Bereich | Maßnahme | Maßnahmentitel |
|---|---|---|---|
| M1 | Infrastruktur | | |
| | | M 1.2 | Regelungen für Zutritt zu Verteilern |
| | | M 1.6 | Einhaltung von Brandschutzvorschriften |
| | | M 1.7 | Handfeuerlöscher |
| | | M 1.10 | Verwendung von Sicherheitstüren und -fenstern |
| | | M 1.15 | Geschlossene Fenster und Türen |
| | | M 1.27 | Klimatisierung |
| | | M 1.30 | Absicherung der Datenträger mit TK-Gebührendaten |
| | | M 1.32 | Geeignete Aufstellung von Druckern und Kopierern |
| | | M 1.34 | Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz |
| | | M 1.35 | Sammelaufbewahrung tragbarer IT-Systeme |
| | | M 1.37 | Geeignete Aufstellung eines Faxgerätes |
| | | M 1.38 | Geeignete Aufstellung eines Modems |
| | | M 1.42 | Gesicherte Aufstellung von Novell Netware Servern |
| | | M 1.43 | Gesicherte Aufstellung aktiver Netzkomponenten |
| | | M 1.45 | Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger |
| | | M 1.46 | Einsatz von Diebstahl-Sicherungen |
| | | M 1.47 | Eigener Brandabschnitt |
| | | M 1.59 | Geeignete Aufstellung von Archivsystemen |
| | | M 1.60 | Geeignete Lagerung von Archivmedien |
| M2 | Organisation | | |
| | | M 2.1 | Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz |
| | | M 2.2 | Betriebsmittelverwaltung |
| | | M 2.3 | Datenträgerverwaltung |
| | | M 2.4 | Regelungen für Wartungs- und Reparaturarbeiten |
| | | M 2.5 | Aufgabenverteilung und Funktionstrennung |
| | | M 2.6 | Vergabe von Zutrittsberechtigungen |
| | | M 2.7 | Vergabe von Zugangsberechtigungen |
| | | M 2.8 | Vergabe von Zugriffsrechten |
| | | M 2.9 | Nutzungsverbot nicht freigegebener Hard- und Software |
| | | M 2.13 | Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln |
| | | M 2.14 | Schlüsselverwaltung |
| | | M 2.16 | Beaufsichtigung oder Begleitung von Fremdpersonen |
| | | M 2.22 | Hinterlegen des Passwortes |
| | | M 2.25 | Dokumentation der Systemkonfiguration |
| | | M 2.27 | Verzicht auf Fernwartung der TK-Anlage |
| | | M 2.30 | Regelung für die Einrichtung von Benutzern / Benutzergruppen |
| | | M 2.33 | Aufteilung der Administrationstätigkeiten unter Unix |
| | | M 2.36 | Geregelte Übergabe und Rücknahme eines tragbaren PC |

| | |
|---|---|
| M 2.37 | "Der aufgeräumte Arbeitsplatz" |
| M 2.39 | Reaktion auf Verletzungen der Sicherheitspolitik |
| M 2.40 | Rechtzeitige Beteiligung des Personal-/Betriebsrates |
| M 2.47 | Ernennung eines Fax-Verantwortlichen |
| M 2.55 | Einsatz eines Sicherungscodes |
| M 2.62 | Software-Abnahme- und Freigabe-Verfahren |
| M 2.63 | Einrichten der Zugriffsrechte |
| M 2.64 | Kontrolle der Protokolldateien |
| M 2.66 | Beachtung des Beitrags der Zertifizierung für die Beschaffung |
| M 2.70 | Entwicklung eines Konzepts für Sicherheitsgateways |
| M 2.71 | Festlegung einer Policy für ein Sicherheitsgateway |
| M 2.77 | Integration von Servern in das Sicherheitsgateway |
| M 2.79 | Festlegung der Verantwortlichkeiten im Bereich Standardsoftware |
| M 2.80 | Erstellung eines Anforderungskatalogs für Standardsoftware |
| M 2.81 | Vorauswahl eines geeigneten Standardsoftwareproduktes |
| M 2.82 | Entwicklung eines Testplans für Standardsoftware |
| M 2.83 | Testen von Standardsoftware |
| M 2.86 | Sicherstellen der Integrität von Standardsoftware |
| M 2.91 | Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz |
| M 2.93 | Planung des Windows NT Netzes |
| M 2.94 | Freigabe von Verzeichnissen unter Windows NT |
| M 2.97 | Korrekter Umgang mit Codeschlössern |
| M 2.100 | Sicherer Betrieb von Novell Netware Servern |
| M 2.103 | Einrichten von Benutzerprofilen unter Windows 95 |
| M 2.104 | Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95 |
| M 2.105 | Beschaffung von TK-Anlagen |
| M 2.110 | Datenschutzaspekte bei der Protokollierung |
| M 2.112 | Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution |
| M 2.115 | Betreuungs- und Wartungskonzept für Telearbeitsplätze |
| M 2.126 | Erstellung eines Datenbanksicherheitskonzeptes |
| M 2.127 | Inferenzprävention |
| M 2.139 | Ist-Aufnahme der aktuellen Netzsituation |
| M 2.141 | Entwicklung eines Netzkonzeptes |
| M 2.144 | Geeignete Auswahl eines Netzmanagement-Protokolls |
| M 2.149 | Sicherer Betrieb von Novell Netware 4.x Netzen |
| M 2.153 | Dokumentation von Novell Netware 4.x Netzen |
| M 2.155 | Identifikation potentiell von Computer-Viren betroffener IT-Systeme |
| M 2.158 | Meldung von Computer-Virusinfektionen |
| M 2.160 | Regelungen zum Computer-Virenschutz |
| M 2.161 | Entwicklung eines Kryptokonzepts |
| M 2.162 | Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte |

| | |
|---|---|
| M 2.163 | Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte |
| M 2.164 | Auswahl eines geeigneten kryptographischen Verfahrens |
| M 2.172 | Entwicklung eines Konzeptes für die WWW-Nutzung |
| M 2.173 | Festlegung einer WWW-Sicherheitsstrategie |
| M 2.174 | Sicherer Betrieb eines WWW-Servers |
| M 2.175 | Aufbau eines WWW-Servers |
| M 2.177 | Sicherheit bei Umzügen |
| M 2.178 | Erstellung einer Sicherheitsleitlinie für die Faxnutzung |
| M 2.184 | Entwicklung eines RAS-Konzeptes |
| M 2.185 | Auswahl einer geeigneten RAS-Systemarchitektur |
| M 2.191 | Etablierung des IT-Sicherheitsprozesses |
| M 2.192 | Erstellung einer IT-Sicherheitsleitlinie |
| M 2.193 | Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit |
| M 2.194 | Erstellung einer Übersicht über vorhandene IT-Systeme |
| M 2.195 | Erstellung eines IT-Sicherheitskonzepts |
| M 2.196 | Umsetzung des IT-Sicherheitskonzepts nach einem Realisierungsplan |
| M 2.197 | Integration der Mitarbeiter in den Sicherheitsprozess |
| M 2.198 | Sensibilisierung der Mitarbeiter für IT-Sicherheit |
| M 2.199 | Aufrechterhaltung der IT-Sicherheit |
| M 2.200 | Managementreporte und -bewertungen der IT-Sicherheit |
| M 2.201 | Dokumentation des IT-Sicherheitsprozesses |
| M 2.204 | Verhinderung ungesicherter Netzzugänge |
| M 2.205 | Übertragung und Abruf personenbezogener Daten |
| M 2.206 | Planung des Einsatzes von Lotus Notes |
| M 2.209 | Planung des Einsatzes von Lotus Notes im Intranet |
| M 2.210 | Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff |
| M 2.211 | Planung des Einsatzes von Lotus Notes in einer DMZ |
| M 2.216 | Genehmigungsverfahren für IT-Komponenten |
| M 2.217 | Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen |
| M 2.220 | Richtlinien für die Zugriffs- bzw. Zugangskontrolle |
| M 2.221 | Änderungsmanagement |
| M 2.223 | Sicherheitsvorgaben für die Nutzung von Standardsoftware |
| M 2.224 | Vorbeugung gegen Trojanische Pferde |
| M 2.225 | Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten |
| M 2.227 | Planung des Windows 2000 Einsatzes |
| M 2.228 | Festlegen einer Windows 2000 Sicherheitsrichtlinie |
| M 2.229 | Planung des Active Directory |
| M 2.230 | Planung der Active Directory-Administration |
| M 2.232 | Planung der Windows 2000 CA-Struktur |
| M 2.234 | Konzeption von Internet-PCs |
| M 2.240 | Planung des Einsatzes von Novell eDirectory im Extranet |

| | | |
|---|---|---|
| | M 2.241 | Durchführung einer Anforderungsanalyse für den Telearbeitsplatz |
| | M 2.247 | Planung des Einsatzes von Exchange/Outlook 2000 |
| | M 2.251 | Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben |
| | M 2.262 | Regelung der Nutzung von Archivsystemen |
| | M 2.264 | Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung |
| | M 2.267 | Planen des IIS-Einsatzes |
| | M 2.268 | Festlegung einer IIS-Sicherheitsrichtlinie |
| | M 2.271 | Festlegung einer Sicherheitsstrategie für den WWW-Zugang |
| | M 2.276 | Funktionsweise eines Routers |
| | M 2.277 | Funktionsweise eines Switches |
| | M 2.278 | Typische Einsatzszenarien von Routern und Switches |
| | M 2.280 | Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches |
| | M 2.286 | Planung und Einsatz von zSeries-Systemen |
| | M 2.288 | Erstellung von Sicherheitsrichtlinien für z/OS-Systeme |
| | M 2.293 | Wartung von zSeries-Systemen |
| | M 2.299 | Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway |
| | M 2.301 | Outsourcing des Sicherheitsgateway |
| | M 2.306 | Verlustmeldung |
| M3 Personal | | |
| | M 3.5 | Schulung zu IT-Sicherheitsmaßnahmen |
| | M 3.9 | Ergonomischer Arbeitsplatz |
| | M 3.11 | Schulung des Wartungs- und Administrationspersonals |
| | M 3.16 | Einweisung in die Bedienung des Anrufbeantworters |
| | M 3.19 | Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten |
| | M 3.23 | Einführung in kryptographische Grundbegriffe |
| | M 3.24 | Schulung zur Lotus Notes Systemarchitektur für Administratoren |
| | M 3.26 | Einweisung des Personals in den sicheren Umgang mit IT |
| | M 3.27 | Schulung zur Active Directory-Verwaltung |
| | M 3.28 | Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer |
| | M 3.30 | Schulung zum Einsatz von Novell eDirectory Clientsoftware |
| | M 3.39 | Einführung in die zSeries-Plattform |
| | M 3.43 | Schulung der Administratoren des Sicherheitsgateways |
| M4 Hard- und Software | | |
| | M 4.1 | Passwortschutz für IT-Systeme |
| | M 4.3 | Regelmäßiger Einsatz eines Anti-Viren-Programms |
| | M 4.6 | Revision der TK-Anlagenkonfiguration |
| | M 4.7 | Änderung voreingestellter Passwörter |
| | M 4.8 | Schutz des TK-Bedienplatzes |
| | M 4.9 | Einsatz der Sicherheitsmechanismen von X-Windows |
| | M 4.12 | Sperren nicht benötigter TK-Leistungsmerkmale |
| | M 4.14 | Obligatorischer Passwortschutz unter Unix |

| | |
|---|---|
| M 4.15 | Gesichertes Login |
| M 4.18 | Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus |
| M 4.19 | Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen |
| M 4.21 | Verhinderung des unautorisierten Erlangens von Administratorrechten |
| M 4.24 | Sicherstellung einer konsistenten Systemverwaltung |
| M 4.27 | Zugriffsschutz am Laptop |
| M 4.28 | Software-Reinstallation bei Benutzerwechsel eines Laptops |
| M 4.29 | Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme |
| M 4.31 | Sicherstellung der Energieversorgung im mobilen Einsatz |
| M 4.33 | Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung |
| M 4.34 | Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen |
| M 4.37 | Sperren bestimmter Absender-Faxnummern |
| M 4.39 | Abschalten des Anrufbeantworters bei Anwesenheit |
| M 4.41 | Einsatz angemessener Sicherheitsprodukte für IT-Systeme |
| M 4.43 | Faxgerät mit automatischer Eingangskuvertierung |
| M 4.44 | Prüfung eingehender Dateien auf Makro-Viren |
| M 4.45 | Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW |
| M 4.46 | Nutzung des Anmeldepasswortes unter WfW und Windows 95 |
| M 4.47 | Protokollierung der Sicherheitsgateway-Aktivitäten |
| M 4.48 | Passwortschutz unter Windows NT/2000/XP |
| M 4.49 | Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System |
| M 4.50 | Strukturierte Systemverwaltung unter Windows NT |
| M 4.51 | Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT |
| M 4.52 | Geräteschutz unter Windows NT/2000/XP |
| M 4.53 | Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT |
| M 4.55 | Sichere Installation von Windows NT |
| M 4.56 | Sicheres Löschen unter Windows-Betriebssystemen |
| M 4.57 | Deaktivieren der automatischen CD-ROM-Erkennung |
| M 4.61 | Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten |
| M 4.62 | Einsatz eines D-Kanal-Filters |
| M 4.63 | Sicherheitstechnische Anforderungen an den Telearbeitsrechner |
| M 4.65 | Test neuer Hard- und Software |
| M 4.70 | Durchführung einer Datenbanküberwachung |
| M 4.72 | Datenbank-Verschlüsselung |
| M 4.73 | Festlegung von Obergrenzen für selektierbare Datensätze |
| M 4.75 | Schutz der Registrierung unter Windows NT/2000/XP |
| M 4.79 | Sichere Zugriffsmechanismen bei lokaler Administration |
| M 4.83 | Update/Upgrade von Soft- und Hardware im Netzbereich |
| M 4.84 | Nutzung der BIOS-Sicherheitsmechanismen |
| M 4.85 | Geeignetes Schnittstellendesign bei Kryptomodulen |
| M 4.86 | Sichere Rollenteilung und Konfiguration der Kryptomodule |

| | |
|---|---|
| M 4.91 | Sichere Installation eines Systemmanagementsystems |
| M 4.92 | Sicherer Betrieb eines Systemmanagementsystems |
| M 4.95 | Minimales Betriebssystem |
| M 4.96 | Abschaltung von DNS |
| M 4.97 | Ein Dienst pro Server |
| M 4.98 | Kommunikation durch Paketfilter auf Minimum beschränken |
| M 4.99 | Schutz gegen nachträgliche Veränderungen von Informationen |
| M 4.100 | Sicherheitsgateways und aktive Inhalte |
| M 4.101 | Sicherheitsgateways und Verschlüsselung |
| M 4.105 | Erste Maßnahmen nach einer Unix-Standardinstallation |
| M 4.107 | Nutzung von Hersteller-Ressourcen |
| M 4.108 | Vereinfachtes und sicheres Netzmanagement mit DNS Services unter Novell NetWare 4.11 |
| M 4.109 | Software-Reinstallation bei Arbeitsplatzrechnern |
| M 4.112 | Sicherer Betrieb des RAS-Systems |
| M 4.114 | Nutzung der Sicherheitsmechanismen von Mobiltelefonen |
| M 4.115 | Sicherstellung der Energieversorgung von Mobiltelefonen |
| M 4.118 | Konfiguration als Lotus Notes Server |
| M 4.123 | Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes |
| M 4.124 | Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes |
| M 4.126 | Sichere Konfiguration eines Lotus Notes Clients |
| M 4.127 | Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes |
| M 4.131 | Verschlüsselung von Lotus Notes Datenbanken |
| M 4.132 | Überwachen eines Lotus Notes-Systems |
| M 4.133 | Geeignete Auswahl von Authentikationsmechanismen |
| M 4.137 | Sichere Konfiguration von Windows 2000 |
| M 4.138 | Konfiguration von Windows 2000 als Domänen-Controller |
| M 4.139 | Konfiguration von Windows 2000 als Server |
| M 4.140 | Sichere Konfiguration wichtiger Windows 2000 Dienste |
| M 4.144 | Nutzung der Windows 2000 CA |
| M 4.145 | Sichere Konfiguration von RRAS unter Windows 2000 |
| M 4.146 | Sicherer Betrieb von Windows 2000/XP |
| M 4.147 | Sichere Nutzung von EFS unter Windows 2000/XP |
| M 4.148 | Überwachung eines Windows 2000/XP Systems |
| M 4.149 | Datei- und Freigabeberechtigungen unter Windows 2000/XP |
| M 4.150 | Konfiguration von Windows 2000 als Workstation |
| M 4.151 | Sichere Installation von Internet-PCs |
| M 4.153 | Sichere Installation von Novell eDirectory |
| M 4.155 | Sichere Konfiguration von Novell eDirectory |
| M 4.157 | Einrichten von Zugriffsberechtigungen auf Novell eDirectory |
| M 4.158 | Einrichten des LDAP-Zugriffs auf Novell eDirectory |
| M 4.159 | Sicherer Betrieb von Novell eDirectory |

| | | |
|---|---|---|
| | M 4.161 | Sichere Installation von Exchange/Outlook 2000 |
| | M 4.162 | Sichere Konfiguration von Exchange 2000 Servern |
| | M 4.163 | Zugriffsrechte auf Exchange 2000 Objekte |
| | M 4.165 | Sichere Konfiguration von Outlook 2000 |
| | M 4.166 | Sicherer Betrieb von Exchange/Outlook 2000 |
| | M 4.167 | Überwachung und Protokollierung von Exchange 2000 Systemen |
| | M 4.169 | Verwendung geeigneter Archivmedien |
| | M 4.171 | Schutz der Integrität der Index-Datenbank von Archivsystemen |
| | M 4.175 | Sichere Konfiguration von Windows NT/2000 für den IIS |
| | M 4.176 | Auswahl einer Authentisierungsmethode für Webangebote |
| | M 4.178 | Absicherung der Administrator- und Benutzerkonten beim IIS-Einsatz |
| | M 4.179 | Schutz von sicherheitskritischen Dateien beim IIS-Einsatz |
| | M 4.180 | Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS |
| | M 4.189 | Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz |
| | M 4.190 | Entfernen der RDS-Unterstützung des IIS |
| | M 4.192 | Konfiguration des Betriebssystems für einen Apache-Webserver |
| | M 4.193 | Sichere Installation eines Apache-Webservers |
| | M 4.198 | Installation eines Apache-Webservers in einem chroot-Käfig |
| | M 4.200 | Umgang mit USB-Speichermedien |
| | M 4.202 | Sichere Netz-Grundkonfiguration von Routern und Switches |
| | M 4.204 | Sichere Administration von Routern und Switches |
| | M 4.206 | Sicherung von Switch-Ports |
| | M 4.207 | Einsatz und Sicherung systemnaher z/OS-Terminals |
| | M 4.209 | Sichere Grundkonfiguration von z/OS-Systemen |
| | M 4.211 | Einsatz des z/OS-Sicherheitssystems RACF |
| | M 4.212 | Absicherung von Linux für zSeries |
| | M 4.214 | Datenträgerverwaltung unter z/OS-Systemen |
| | M 4.218 | Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen |
| | M 4.219 | Lizenzschlüssel-Management für z/OS-Software |
| | M 4.220 | Absicherung von Unix System Services bei z/OS-Systemen |
| | M 4.222 | Festlegung geeigneter Einstellungen von Sicherheitsproxies |
| | M 4.223 | Integration von Proxy-Servern in das Sicherheitsgateway |
| | M 4.224 | Integration von Virtual Private Networks in ein Sicherheitsgateway |
| | M 4.225 | Einsatz eines Protokollierungsservers in einem Sicherheitsgateway |
| M5 IT Kommunikation | | |
| | M 5.1 | Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen |
| | M 5.2 | Auswahl einer geeigneten Netz-Topographie |
| | M 5.3 | Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht |
| | M 5.8 | Regelmäßiger Sicherheitscheck des Netzes |
| | M 5.13 | Geeigneter Einsatz von Elementen zur Netzkopplung |
| | M 5.14 | Absicherung interner Remote-Zugänge |

| | |
|---|---|
| M 5.15 | Absicherung externer Remote-Zugänge |
| M 5.19 | Einsatz der Sicherheitsmechanismen von sendmail |
| M 5.20 | Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp |
| M 5.25 | Nutzung von Sende- und Empfangsprotokollen |
| M 5.31 | Geeignete Modem-Konfiguration |
| M 5.36 | Verschlüsselung unter Unix und Windows NT |
| M 5.37 | Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz |
| M 5.38 | Sichere Einbindung von DOS-PCs in ein Unix-Netz |
| M 5.39 | Sicherer Einsatz der Protokolle und Dienste |
| M 5.40 | Sichere Einbindung von DOS-PCs in ein Windows NT Netz |
| M 5.42 | Sichere Konfiguration der TCP/IP-Netzverwaltung unter Windows NT |
| M 5.43 | Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT |
| M 5.46 | Einsatz von Stand-alone-Systemen zur Nutzung des Internets |
| M 5.52 | Sicherheitstechnische Anforderungen an den Kommunikationsrechner |
| M 5.54 | Schutz vor Mailüberlastung und Spam |
| M 5.60 | Auswahl einer geeigneten Backbone-Technologie |
| M 5.61 | Geeignete physikalische Segmentierung |
| M 5.63 | Einsatz von GnuPG oder PGP |
| M 5.64 | Secure Shell |
| M 5.68 | Einsatz von Verschlüsselungsverfahren zur Netzkommunikation |
| M 5.69 | Schutz vor aktiven Inhalten |
| M 5.73 | Sicherer Betrieb eines Faxservers |
| M 5.75 | Schutz vor Überlastung des Faxservers |
| M 5.76 | Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation |
| M 5.81 | Sichere Datenübertragung über Mobiltelefone |
| M 5.82 | Sicherer Einsatz von SAMBA |
| M 5.83 | Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN |
| M 5.84 | Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation |
| M 5.85 | Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail |
| M 5.89 | Konfiguration des sicheren Kanals unter Windows 2000/XP |
| M 5.90 | Einsatz von IPSec unter Windows 2000/XP |
| M 5.93 | Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs |
| M 5.94 | Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs |
| M 5.95 | Sicherer E-Commerce bei der Nutzung von Internet-PCs |
| M 5.96 | Sichere Nutzung von Webmail |
| M 5.98 | Schutz vor Missbrauch kostenpflichtiger Einwahlnummern |
| M 5.101 | Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz |
| M 5.102 | Installation von URL-Filtern beim IIS-Einsatz |
| M 5.103 | Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz |
| M 5.104 | Konfiguration des TCP/IP-Filters beim IIS-Einsatz |
| M 5.105 | Vorbeugen vor SYN-Attacken auf den IIS |

| | | |
|---|---|---|
| | M 5.106 | Entfernen nicht vertrauenswürdiger Root-Zertifikate beim IIS-Einsatz |
| | M 5.108 | Kryptographische Absicherung von E-Mail |
| | M 5.109 | Einsatz eines E-Mail-Scanners auf dem Mailserver |
| | M 5.110 | Absicherung von E-Mail mit SPHINX (S/MIME) |
| | M 5.118 | Integration eines DNS-Servers in ein Sicherheitsgateway |
| | M 5.119 | Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway |
| | M 5.121 | Sichere Kommunikation von unterwegs |
| M6 Notfallvorsorge | | |
| | M 6.2 | Notfall-Definition, Notfall-Verantwortlicher |
| | M 6.3 | Erstellung eines Notfall-Handbuches |
| | M 6.10 | Notfall-Plan für DFÜ-Ausfall |
| | M 6.12 | Durchführung von Notfallübungen |
| | M 6.15 | Lieferantenvereinbarungen |
| | M 6.16 | Abschließen von Versicherungen |
| | M 6.17 | Alarmierungsplan und Brandschutzübungen |
| | M 6.19 | Datensicherung am PC |
| | M 6.20 | Geeignete Aufbewahrung der Backup-Datenträger |
| | M 6.22 | Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen |
| | M 6.23 | Verhaltensregeln bei Auftreten eines Computer-Virus |
| | M 6.24 | Erstellen eines Notfall-Bootmediums |
| | M 6.25 | Regelmäßige Datensicherung der Server-Festplatte |
| | M 6.29 | TK-Basisanschluss für Notrufe |
| | M 6.31 | Verhaltensregeln nach Verlust der Systemintegrität |
| | M 6.32 | Regelmäßige Datensicherung |
| | M 6.35 | Festlegung der Verfahrensweise für die Datensicherung |
| | M 6.38 | Sicherungskopie der übermittelten Daten |
| | M 6.39 | Auflistung von Händleradressen zur Fax-Wiederbeschaffung |
| | M 6.41 | Übungen zur Datenrekonstruktion |
| | M 6.43 | Einsatz redundanter Windows NT/2000 Server |
| | M 6.45 | Datensicherung unter Windows 95 |
| | M 6.47 | Datensicherung bei der Telearbeit |
| | M 6.48 | Verhaltensregeln nach Verlust der Datenbankintegrität |
| | M 6.49 | Datensicherung einer Datenbank |
| | M 6.50 | Archivierung von Datenbeständen |
| | M 6.52 | Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten |
| | M 6.54 | Verhaltensregeln nach Verlust der Netzintegrität |
| | M 6.55 | Reduzierung der Wiederanlaufzeit für Novell Netware Server |
| | M 6.56 | Datensicherung bei Einsatz kryptographischer Verfahren |
| | M 6.57 | Erstellen eines Notfallplans für den Ausfall des Managementsystems |
| | M 6.58 | Etablierung eines Managementsystems zur Behandlung von Sicherheitsvorfällen |
| | M 6.59 | Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen |

| | |
|---|---|
| M 6.61 | Eskalationsstrategie für Sicherheitsvorfälle |
| M 6.62 | Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen |
| M 6.63 | Untersuchung und Bewertung eines Sicherheitsvorfalls |
| M 6.65 | Benachrichtigung betroffener Stellen |
| M 6.67 | Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle |
| M 6.70 | Erstellen eines Notfallplans für den Ausfall des RAS-Systems |
| M 6.73 | Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems |
| M 6.75 | Redundante Kommunikationsverbindungen |
| M 6.76 | Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes |
| M 6.78 | Datensicherung unter Windows 2000/XP |
| M 6.80 | Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes |
| M 6.82 | Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen |
| M 6.84 | Regelmäßige Datensicherung der System- und Archivdaten |
| M 6.85 | Erstellung eines Notfallplans für den Ausfall des IIS |
| M 6.86 | Schutz vor schädlichem Code auf dem IIS |
| M 6.88 | Erstellen eines Notfallplans für den Webserver |
| M 6.90 | Datensicherung und Archivierung von E-Mails |
| M 6.92 | Notfallvorsorge bei Routern und Switches |
| M 6.93 | Notfallvorsorge für z/OS-Systeme |
| M 6.94 | Notfallvorsorge bei Sicherheitsgateways |