Neu zugeordnete Bausteine

Maßnahme	Maßnahmentitel
M 1.25	Überspannungsschutz
M 1.29	Geeignete Aufstellung eines IT-Systems
M 1.31	Fernanzeige von Störungen
M 1.46	Einsatz von Diebstahl-Sicherungen
M 1.62	Brandschutz von Patchfeldern
M 2.16	Beaufsichtigung oder Begleitung von Fremdpersonen
M 2.18	Kontrollgänge
M 2.22	Hinterlegen des Passwortes
M 2.25	Dokumentation der Systemkonfiguration
M 2.26	Ernennung eines Administrators und eines Vertreters
M 2.34	Dokumentation der Veränderungen an einem bestehenden System
M 2.35	Informationsbeschaffung über Sicherheitslücken des Systems
M 2.38	Aufteilung der Administrationstätigkeiten
M 2.65	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
M 2.145	Anforderungen an ein Netzmanagement-Tool
M 2.146	Sicherer Betrieb eines Netzmanagementsystems
M 2.218	Regelung der Mitnahme von Datenträgern und IT-Komponenten
M 2.224	Vorbeugung gegen Trojanische Pferde
M 2.273	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

Baustein	Alt	Zertifikat	Zyklus	Bausteinname
B 4.5	(8.4)	(B)	Planung	LAN-Anbindung eines IT-Systems über ISDN
B 1.9	(3.9)	(Z)	Umsetzg.	Hard- und Software-Management
B 2.9	(4.6)	(Z)	Planung	Rechenzentrum
B 3.203	(5.3)	(Z)	Betrieb	Laptop
B 2.4	(4.3.2)	(C)	Planung	Serverraum
B 2.9	(4.6)	(C)	Planung	Rechenzentrum
B 1.1	(3.1)	(B)	Betrieb	Organisation
B 1.1	(3.1)	(Z)	Betrieb	Organisation
B 1.9	(3.9)	(Z)	Betrieb	Hard- und Software-Management
B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management
B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management
B 1.9	(3.9)	(A)	Betrieb	Hard- und Software-Management
B 1.9	(3.9)	(B)	Betrieb	Hard- und Software-Management
B 1.9	(3.9)	(B)	Umsetzg.	Hard- und Software-Management
B 1.9	(3.9)	(C)	Betrieb	Hard- und Software-Management
B 4.2	(6.8)	(B)	Beschaff.	Netz- und Systemmanagement
B 4.2	(6.8)	(A)	Betrieb	Netz- und Systemmanagement
B 3.203	(5.3)	(B)	Planung	Laptop
B 1.6	(3.6)	(A)	Betrieb	Computer-Virenschutzkonzept
B 3.101	(6.1)	(A)	Betrieb	Allgemeiner Server

M 2.306	Verlustmeldung	B 3.203	(5.3)	(B)	Aussnd.	Laptop
M 2.307	Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses	B 1.11	(3.10)	(A)	Aussnd.	Outsourcing
M 2.308	Auszug aus Gebäuden	B 2.1	(4.1)	(Z)	Aussnd.	Gebäude
M 2.309	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung	B 3.203	(5.3)	(A)	Planung	Laptop
M 2.310	Geeignete Auswahl von Laptops	B 3.203	(5.3)	(A)	Beschaff.	Laptop
M 2.311	Planung von Schutzschränken	B 2.7	(4.4)	(A)	Planung	Schutzschrank
M 2.313	Sichere Anmeldung bei Internet-Diensten	B 3.208	(5.8)	(A)	Betrieb	Internet-PC
M 2.314	Verwendung von hochverfügbaren Architekturen für Server	B 3.101	(6.1)	(Z)	Planung	Allgemeiner Server
M 2.315	Planung des Servereinsatzes	B 3.101	(6.1)	(A)	Planung	Allgemeiner Server
M 2.316	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server	B 3.101	(6.1)	(A)	Planung	Allgemeiner Server
M 2.317	Beschaffungskriterien für einen Server	B 3.101	(6.1)	(C)	Beschaff.	Allgemeiner Server
M 2.318	Sichere Installation eines Servers	B 3.101	(6.1)	(A)	Umsetzg.	Allgemeiner Server
M 2.319	Migration eines Servers	B 3.101	(6.1)	(C)	Aussnd.	Allgemeiner Server
M 2.320	Geregelte Außerbetriebnahme eines Servers	B 3.101	(6.1)	(A)	Aussnd.	Allgemeiner Server
M 2.334	Auswahl eines geeigneten Gebäudes	B 2.1	(4.1)	(Z)	Planung	Gebäude
M 2.335	Festlegung der IT-Sicherheitsziele und -strategie	B 1.0	(3.0)	(A)	Planung	IT-Sicherheitsmanagement
M 2.336	Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene	B 1.0	(3.0)	(A)	Planung	IT-Sicherheitsmanagement
M 2.337	Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse	B 1.0	(3.0)	(A)	Umsetzg.	IT-Sicherheitsmanagement
M 2.338	Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien	B 1.0	(3.0)	(Z)	Umsetzg.	IT-Sicherheitsmanagement
M 2.339	Wirtschaftlicher Einsatz von Ressourcen für IT-Sicherheit	B 1.0	(3.0)	(Z)	Umsetzg.	IT-Sicherheitsmanagement
M 2.340	Beachtung rechtlicher Rahmenbedingungen					

M 3.10	Auswahl eines vertrauenswürdigen Administrators und Vertreters
M 3.11	Schulung des Wartungs- und Administrationspersonals
M 3.33	Sicherheitsüberprüfung von Mitarbeitern
M 3.50	Auswahl von Personal
M 3.51	Geeignetes Konzept für Personaleinsatz und -qualifizierung
M 4.1	Passwortschutz für IT-Systeme
M 4.7	Änderung voreingestellter Passwörter
M 4.15	Gesichertes Login
M 4.40	Verhinderung der unautorisierten Nutzung des Rechnermikrofons
M 4.42	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
M 4.48	Passwortschutz unter Windows NT/2000/XP
M 4.75	Schutz der Registrierung unter Windows NT/2000/XP
M 4.84	Nutzung der BIOS-Sicherheitsmechanismen
M 4.107	Nutzung von Hersteller-Ressourcen
M 4.147	Sichere Nutzung von EFS unter Windows 2000/XP
M 4.233	Sperrung nicht mehr benötigter RAS-Zugänge
M 4.234	Aussonderung von IT-Systemen
M 4.235	Abgleich der Datenbestände von Laptops
M 4.236	Zentrale Administration von Laptops

B 1.0	(3.0)	(A)	Betrieb	IT-Sicherheitsmanagement
B 1.2	(3.2)	(A)	Umsetzg.	Personal
B 1.2	(3.2)	(A)	Betrieb	Personal
B 1.2	(3.2)	(Z)	Umsetzg.	Personal
B 1.2	(3.2)	(Z)	Beschaff.	Personal
B 1.2	(3.2)	(Z)	Planung	Personal
B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management
B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management
B 3.202	(5.99)	(A)	Umsetzg.	Allgemeines nicht vernetztes IT-System
B 3.101	(6.1)	(C)	Umsetzg.	Allgemeiner Server
B 3.202	(5.99)	(C)	Betrieb	Allgemeines nicht vernetztes IT-System
B 3.203	(5.3)	(A)	Umsetzg.	Laptop
B 1.10	(9.1)	(Z)	Umsetzg.	Standardsoftware
B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management
B 1.9	(3.9)	(B)	Betrieb	Hard- und Software-Management
B 3.207	(5.7)	(Z)	Betrieb	Client unter Windows 2000
B 4.4	(7.6)	(B)	Aussnd.	Remote Access
B 1.9	(3.9)	(B)	Aussnd.	Hard- und Software-Management
B 3.203	(5.3)	(B)	Betrieb	Laptop
B 3.203	(5.3)	(Z)	Betrieb	Laptop

M 4.237	Sichere Grundkonfiguration eines IT-Systems	B 3.101	(6.1)	(A)	Umsetzg.	Allgemeiner Server
M 4.238	Einsatz eines lokalen Paketfilters	B 3.101	(6.1)	(A)	Betrieb	Allgemeiner Server
M 4.239	Sicherer Betrieb eines Servers	B 3.101	(6.1)	(A)	Betrieb	Allgemeiner Server
M 4.240	Einrichten einer Testumgebung für einen Server	B 3.101	(6.1)	(Z)	Betrieb	Allgemeiner Server
M 4.253	Schutz vor Spyware	B 1.6	(3.6)	(A)	Planung	Computer-Virenschutzkonzept
M 4.254	Sicherer Einsatz von drahtlosen Tastaturen und Mäusen	B 1.9	(3.9)	(Z)	Betrieb	Hard- und Software-Management
M 4.255	Nutzung von IrDA-Schnittstellen	B 3.203	(5.3)	(A)	Betrieb	Laptop
		B 3.404	(8.6)	(A)	Betrieb	Mobiltelefon
		B 3.405	(8.7)	(A)	Betrieb	PDA
M 5.37	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz	B 3.101	(6.1)	(B)	Planung	Allgemeiner Server
M 5.91	Einsatz von Personal Firewalls für Internet-PCs	B 3.203	(5.3)	(A)	Betrieb	Laptop
M 5.121	Sichere Kommunikation von unterwegs	B 3.203	(5.3)	(A)	Betrieb	Laptop
M 5.122	Sicherer Anschluss von Laptops an lokale Netze	B 3.203	(5.3)	(A)	Betrieb	Laptop
M 6.20	Geeignete Aufbewahrung der Backup-Datenträger	B 1.4	(3.4)	(A)	Betrieb	Datensicherungskonzept
M 6.21	Sicherungskopie der eingesetzten Software	B 1.4	(3.4)	(C)	Umsetzg.	Datensicherungskonzept
		B 1.9	(3.9)	(C)	Notfallv.	Hard- und Software-Management
M 6.22	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen	B 1.4	(3.4)	(A)	Betrieb	Datensicherungskonzept
M 6.24	Erstellen eines Notfall-Bootmediums	B 3.101	(6.1)	(A)	Notfallv.	Allgemeiner Server
M 6.27	Sicheres Update des BIOS	B 1.9	(3.9)	(C)	Notfallv.	Hard- und Software-Management
M 6.32	Regelmäßige Datensicherung	B 1.4	(3.4)	(A)	Betrieb	Datensicherungskonzept
M 6.96	Notfallvorsorge für einen Server	B 3.101	(6.1)	(A)	Notfallv.	Allgemeiner Server