

Gefährdungen und zugeordnete Bausteine

Gefährdung Gefährdungstitel

G 1.1	Personalausfall
G 1.2	Ausfall des IT-Systems

Baustein	Alt	Bausteinname
B 1.2	(3.2)	Personal
B 1.9	(3.9)	Hard- und Software-Management
B 3.101	(6.1)	Allgemeiner Server
B 3.201	(neu)	Allgemeiner Client
B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
B 3.204	(5.2)	Client unter Unix
B 3.205	(5.5)	Client unter Windows NT
B 3.207	(5.7)	Client unter Windows 2000
B 4.2	(6.8)	Netz- und Systemmanagement
B 5.5	(7.7)	Lotus Notes
B 5.7	(9.2)	Datenbanken
B 5.8	(9.3)	Telearbeit
B 1.2	(3.2)	Personal
B 1.3	(3.3)	Notfallvorsorgekonzept
B 1.9	(3.9)	Hard- und Software-Management
B 1.10	(9.1)	Standardsoftware
B 1.12	(9.5)	Archivierung
B 2.9	(4.6)	Rechenzentrum
B 3.101	(6.1)	Allgemeiner Server
B 3.104	(6.5)	Server unter Novell Netware 3.x
B 3.105	(6.6)	Server unter Novell Netware 4.x
B 3.106	(6.9)	Server unter Windows 2000
B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
B 3.203	(5.3)	Laptop
B 3.204	(5.2)	Client unter Unix
B 3.205	(5.5)	Client unter Windows NT
B 3.206	(5.6)	Client unter Windows 95
B 3.207	(5.7)	Client unter Windows 2000
B 3.208	(5.8)	Internet-PC
B 3.209	(neu)	Client unter Windows XP
B 4.1	(6.7)	Heterogene Netze
B 4.2	(6.8)	Netz- und Systemmanagement
B 4.3	(7.2)	Modem
B 4.4	(7.6)	Remote Access
B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
B 5.5	(7.7)	Lotus Notes
B 5.9	(9.4)	Novell eDirectory

G 1.3	Blitz	B 5.12	(7.10)	Exchange 2000 / Outlook 2000
		B 2.1	(4.1)	Gebäude
		B 2.9	(4.6)	Rechenzentrum
G 1.4	Feuer	B 4.1	(6.7)	Heterogene Netze
		B 1.1	(3.1)	Organisation
		B 1.9	(3.9)	Hard- und Software-Management
		B 2.1	(4.1)	Gebäude
		B 2.4	(4.3.2)	Serverraum
		B 2.5	(4.3.3)	Datenträgerarchiv
		B 2.6	(4.3.4)	Raum für technische Infrastruktur
		B 2.7	(4.4)	Schutzschrank
		B 2.9	(4.6)	Rechenzentrum
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.206	(5.6)	Client unter Windows 95
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 3.401	(8.1)	TK-Anlage
G 1.5	Wasser	B 4.1	(6.7)	Heterogene Netze
		B 1.1	(3.1)	Organisation
		B 1.9	(3.9)	Hard- und Software-Management
		B 2.1	(4.1)	Gebäude
		B 2.4	(4.3.2)	Serverraum
		B 2.5	(4.3.3)	Datenträgerarchiv
		B 2.6	(4.3.4)	Raum für technische Infrastruktur
		B 2.7	(4.4)	Schutzschrank
		B 2.8	(4.5)	Häuslicher Arbeitsplatz
		B 2.9	(4.6)	Rechenzentrum
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.206	(5.6)	Client unter Windows 95
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
G 1.6	Kabelbrand	B 4.1	(6.7)	Heterogene Netze
		B 2.2	(4.2)	Verkabelung
		B 2.9	(4.6)	Rechenzentrum
G 1.7	Unzulässige Temperatur und Luftfeuchte	B 1.1	(3.1)	Organisation
		B 1.12	(9.5)	Archivierung

		B 2.4	(4.3.2)	Serverraum
		B 2.5	(4.3.3)	Datenträgerarchiv
		B 2.6	(4.3.4)	Raum für technische Infrastruktur
		B 2.7	(4.4)	Schutzschrank
		B 2.9	(4.6)	Rechenzentrum
		B 4.1	(6.7)	Heterogene Netze
		B 4.2	(6.8)	Netz- und Systemmanagement
		B 5.2	(7.1)	Datenträgeraustausch
G 1.8	Staub, Verschmutzung			
		B 1.9	(3.9)	Hard- und Software-Management
		B 2.5	(4.3.3)	Datenträgerarchiv
		B 2.7	(4.4)	Schutzschrank
		B 2.9	(4.6)	Rechenzentrum
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.204	(5.2)	Client unter Unix
		B 3.206	(5.6)	Client unter Windows 95
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 4.1	(6.7)	Heterogene Netze
		B 5.2	(7.1)	Datenträgeraustausch
G 1.9	Datenverlust durch starke Magnetfelder			
		B 1.12	(9.5)	Archivierung
		B 5.2	(7.1)	Datenträgeraustausch
G 1.10	Ausfall eines Weitverkehrsnetzes			
G 1.11	Technische Katastrophen im Umfeld	B 1.11	(3.10)	Outsourcing
G 1.12	Beeinträchtigung durch Großveranstaltungen	B 2.9	(4.6)	Rechenzentrum
G 1.13	Sturm	B 2.9	(4.6)	Rechenzentrum
G 1.14	Datenverlust durch starkes Licht	B 2.9	(4.6)	Rechenzentrum
G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebung	B 1.12	(9.5)	Archivierung
		B 2.10	(neu)	Mobiler Arbeitsplatz
		B 3.203	(5.3)	Laptop
		B 3.405	(8.7)	PDA
G 1.16	Ausfall von Patchfeldern durch Brand	B 2.4	(4.3.2)	Serverraum
G 2.1	Fehlende oder unzureichende Regelungen	B 2.9	(4.6)	Rechenzentrum

G 2.2 Unzureichende Kenntnis über Regelungen

B 1.1	(3.1)	Organisation
B 1.6	(3.6)	Computer-Virenschutzkonzept
B 1.7	(3.7)	Kryptokonzept
B 1.9	(3.9)	Hard- und Software-Management
B 1.10	(9.1)	Standardsoftware
B 1.11	(3.10)	Outsourcing
B 2.1	(4.1)	Gebäude
B 2.3	(4.3.1)	Bürraum
B 2.4	(4.3.2)	Serverraum
B 2.5	(4.3.3)	Datenträgerarchiv
B 2.6	(4.3.4)	Raum für technische Infrastruktur
B 2.8	(4.5)	Häuslicher Arbeitsplatz
B 2.9	(4.6)	Rechenzentrum
B 2.10	(neu)	Mobiler Arbeitsplatz
B 2.11	(neu)	Besprechungs-, Veranstaltungs- und Schulungsräume
B 3.106	(6.9)	Server unter Windows 2000
B 3.201	(neu)	Allgemeiner Client
B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
B 3.206	(5.6)	Client unter Windows 95
B 3.208	(5.8)	Internet-PC
B 3.302	(7.11)	Router und Switches
B 3.403	(8.3)	Anrufbeantworter
B 5.2	(7.1)	Datenträgeraustausch
B 5.3	(7.4)	E-Mail
B 5.4	(7.5)	Webserver
B 5.5	(7.7)	Lotus Notes
B 5.8	(9.3)	Telearbeit
B 5.9	(9.4)	Novell eDirectory
B 5.10	(7.8)	Internet Information Server
B 5.11	(7.9)	Apache Webserver
B 5.12	(7.10)	Exchange 2000 / Outlook 2000

B 1.1	(3.1)	Organisation
B 1.2	(3.2)	Personal
B 1.6	(3.6)	Computer-Virenschutzkonzept
B 1.7	(3.7)	Kryptokonzept
B 1.9	(3.9)	Hard- und Software-Management
B 1.10	(9.1)	Standardsoftware
B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
B 2.9	(4.6)	Rechenzentrum
B 2.11	(neu)	Besprechungs-, Veranstaltungs- und Schulungsräume

		B 3.106	(6.9)	Server unter Windows 2000
		B 3.208	(5.8)	Internet-PC
		B 3.404	(8.6)	Mobiltelefon
		B 3.405	(8.7)	PDA
		B 4.4	(7.6)	Remote Access
		B 5.5	(7.7)	Lotus Notes
		B 5.9	(9.4)	Novell eDirectory
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel			
		B 1.1	(3.1)	Organisation
		B 1.6	(3.6)	Computer-Virenschutzkonzept
		B 1.10	(9.1)	Standardsoftware
		B 3.302	(7.11)	Router und Switches
		B 5.2	(7.1)	Datenträgeraustausch
		B 5.7	(9.2)	Datenbanken
G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen			
		B 1.6	(3.6)	Computer-Virenschutzkonzept
		B 1.7	(3.7)	Kryptokonzept
		B 1.9	(3.9)	Hard- und Software-Management
		B 2.7	(4.4)	Schutzschrank
		B 2.9	(4.6)	Rechenzentrum
		B 2.10	(neu)	Mobiler Arbeitsplatz
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.107	(6.10)	S/390- und zSeries-Mainframe
		B 3.302	(7.11)	Router und Switches
		B 3.404	(8.6)	Mobiltelefon
		B 3.405	(8.7)	PDA
		B 5.4	(7.5)	Webserver
		B 5.5	(7.7)	Lotus Notes
		B 5.8	(9.3)	Telearbeit
G 2.5	Fehlende oder unzureichende Wartung			
		B 1.1	(3.1)	Organisation
		B 3.403	(8.3)	Anrufbeantworter
		B 5.8	(9.3)	Telearbeit
G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen			
		B 1.1	(3.1)	Organisation
		B 1.9	(3.9)	Hard- und Software-Management
		B 2.1	(4.1)	Gebäude
		B 2.3	(4.3.1)	Bürraum
		B 2.4	(4.3.2)	Serverraum
		B 2.5	(4.3.3)	Datenträgerarchiv

G 2.7	Unerlaubte Ausübung von Rechten	B 2.6	(4.3.4)	Raum für technische Infrastruktur
		B 2.8	(4.5)	Häuslicher Arbeitsplatz
		B 2.9	(4.6)	Rechenzentrum
		B 3.401	(8.1)	TK-Anlage
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
G 2.8	Unkontrollierter Einsatz von Betriebsmitteln	B 1.1	(3.1)	Organisation
		B 1.2	(3.2)	Personal
		B 1.9	(3.9)	Hard- und Software-Management
		B 1.10	(9.1)	Standardsoftware
		B 1.11	(3.10)	Outsourcing
		B 1.12	(9.5)	Archivierung
		B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
		B 3.101	(6.1)	Allgemeiner Server
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.201	(neu)	Allgemeiner Client
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.203	(5.3)	Laptop
		B 3.204	(5.2)	Client unter Unix
		B 3.205	(5.5)	Client unter Windows NT
		B 3.206	(5.6)	Client unter Windows 95
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 3.404	(8.6)	Mobiltelefon
		B 3.405	(8.7)	PDA
		B 4.1	(6.7)	Heterogene Netze
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.3	(7.4)	E-Mail
G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	B 5.4	(7.5)	Webserver
		B 5.5	(7.7)	Lotus Notes
		B 5.6	(8.5)	Faxserver
		B 5.8	(9.3)	Telearbeit
		B 5.9	(9.4)	Novell eDirectory
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000
		B 1.1	(3.1)	Organisation
		B 1.6	(3.6)	Computer-Virenschutzkonzept
		B 3.203	(5.3)	Laptop
		B 1.6	(3.6)	Computer-Virenschutzkonzept
		B 1.9	(3.9)	Hard- und Software-Management

		B 3.101	(6.1)	Allgemeiner Server
		B 3.204	(5.2)	Client unter Unix
		B 3.205	(5.5)	Client unter Windows NT
		B 3.206	(5.6)	Client unter Windows 95
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 4.1	(6.7)	Heterogene Netze
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.3	(7.4)	E-Mail
		B 5.4	(7.5)	Webserver
		B 5.6	(8.5)	Faxserver
		B 5.11	(7.9)	Apache Webserver
G 2.10	Nicht fristgerecht verfügbare Datenträger	B 1.9	(3.9)	Hard- und Software-Management
G 2.11	Unzureichende Trassendimensionierung	B 5.2	(7.1)	Datenträgeraustausch
G 2.12	Unzureichende Dokumentation der Verkabelung	B 2.2	(4.2)	Verkabelung
		B 2.9	(4.6)	Rechenzentrum
G 2.13	Unzureichend geschützte Verteiler	B 2.2	(4.2)	Verkabelung
		B 2.9	(4.6)	Rechenzentrum
G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen	B 2.2	(4.2)	Verkabelung
		B 2.3	(4.3.1)	Bürraum
		B 2.8	(4.5)	Häuslicher Arbeitsplatz
		B 2.11	(neu)	Besprechungs-, Veranstaltungs- und Schulungsräume
G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System	B 1.9	(3.9)	Hard- und Software-Management
		B 3.102	(6.2)	Server unter Unix
		B 3.204	(5.2)	Client unter Unix
G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PCs	B 3.203	(5.3)	Laptop
		B 4.4	(7.6)	Remote Access
		B 5.5	(7.7)	Lotus Notes
G 2.17	Mangelhafte Kennzeichnung der Datenträger	B 5.2	(7.1)	Datenträgeraustausch
G 2.18	Ungeordnete Zustellung der Datenträger	B 3.106	(6.9)	Server unter Windows 2000
		B 5.2	(7.1)	Datenträgeraustausch
		B 5.5	(7.7)	Lotus Notes

G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung	B 1.7	(3.7)	Kryptokonzept
		B 4.4	(7.6)	Remote Access
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.2	(7.1)	Datenträgeraustausch
		B 5.3	(7.4)	E-Mail
		B 5.5	(7.7)	Lotus Notes
G 2.20	Unzureichende oder falsche Versorgung mit Verbrauchsgütern			
G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern	B 3.402	(8.2)	Faxgerät
		B 1.9	(3.9)	Hard- und Software-Management
		B 3.201	(neu)	Allgemeiner Client
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.206	(5.6)	Client unter Windows 95
		B 3.208	(5.8)	Internet-PC
G 2.22	Fehlende Auswertung von Protokolldaten	B 1.9	(3.9)	Hard- und Software-Management
		B 3.206	(5.6)	Client unter Windows 95
		B 3.302	(7.11)	Router und Switches
		B 4.1	(6.7)	Heterogene Netze
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.6	(8.5)	Faxserver
		B 5.7	(9.2)	Datenbanken
		B 5.8	(9.3)	Telearbeit
G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz	B 1.9	(3.9)	Hard- und Software-Management
		B 3.102	(6.2)	Server unter Unix
		B 3.103	(6.4)	Server unter Windows NT
G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes	B 3.201	(neu)	Allgemeiner Client
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.8	(9.3)	Telearbeit
G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten	B 3.101	(6.1)	Allgemeiner Server
		B 3.103	(6.4)	Server unter Windows NT
		B 3.201	(neu)	Allgemeiner Client
		B 5.1	(6.3)	Peer-to-Peer-Dienste
G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren	B 1.6	(3.6)	Computer-Virenschutzkonzept

G 2.27	Fehlende oder unzureichende Dokumentation	B 1.10	(9.1)	Standardsoftware
		B 1.11	(3.10)	Outsourcing
		B 5.7	(9.2)	Datenbanken
G 2.28	Verstöße gegen das Urheberrecht	B 1.10	(9.1)	Standardsoftware
		B 3.107	(6.10)	S/390- und zSeries-Mainframe
		B 3.302	(7.11)	Router und Switches
		B 4.1	(6.7)	Heterogene Netze
		B 4.2	(6.8)	Netz- und Systemmanagement
G 2.29	Softwaretest mit Produktionsdaten	B 1.10	(9.1)	Standardsoftware
		B 5.4	(7.5)	Webserver
G 2.30	Unzureichende Domänenplanung	B 1.10	(9.1)	Standardsoftware
G 2.31	Unzureichender Schutz des Windows NT Systems	B 3.103	(6.4)	Server unter Windows NT
G 2.32	Unzureichende Leitungskapazitäten	B 3.103	(6.4)	Server unter Windows NT
		B 3.205	(5.5)	Client unter Windows NT
		B 2.2	(4.2)	Verkabelung
		B 4.1	(6.7)	Heterogene Netze
		B 4.2	(6.8)	Netz- und Systemmanagement
G 2.33	Nicht gesicherter Aufstellungsort von Novell Netware Servern	B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.4	(7.5)	Webserver
		B 3.104	(6.5)	Server unter Novell Netware 3.x
		B 3.105	(6.6)	Server unter Novell Netware 4.x
		B 3.104	(6.5)	Server unter Novell Netware 3.x
G 2.34	Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen	B 3.105	(6.6)	Server unter Novell Netware 4.x
		B 3.105	(6.6)	Server unter Novell Netware 4.x
G 2.35	Fehlende Protokollierung unter Windows 95	B 3.206	(5.6)	Client unter Windows 95
G 2.36	Ungeeignete Einschränkung der Benutzerumgebung	B 3.206	(5.6)	Client unter Windows 95
G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen	B 3.201	(neu)	Allgemeiner Client
		B 4.4	(7.6)	Remote Access
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.4	(7.5)	Webserver
		B 5.5	(7.7)	Lotus Notes

G 2.38	Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen	B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 2.39	Komplexität eines DBMS	B 5.7	(9.2)	Datenbanken
G 2.40	Komplexität des Datenbankzugangs/-zugriffs	B 5.7	(9.2)	Datenbanken
G 2.41	Mangelhafte Organisation des Wechsels von Datenbank-Benutzern	B 5.5	(7.7)	Lotus Notes
G 2.42	Komplexität der NDS	B 5.7	(9.2)	Datenbanken
G 2.43	Migration von Novell Netware 3.x nach Novell Netware Version 4	B 5.7	(9.2)	Datenbanken
G 2.44	Inkompatible aktive und passive Netzkomponenten	B 3.105	(6.6)	Server unter Novell Netware 4.x
G 2.45	Konzeptionelle Schwächen des Netzes	B 3.105	(6.6)	Server unter Novell Netware 4.x
G 2.46	Überschreiten der zulässigen Kabel- bzw. Buslänge oder der Ringgröße	B 3.302	(7.11)	Router und Switches
G 2.47	Ungesicherter Akten- und Datenträgertransport	B 4.1	(6.7)	Heterogene Netze
G 2.48	Ungeeignete Entsorgung der Datenträger und Dokumente	B 4.4	(7.6)	Remote Access
G 2.49	Fehlende oder unzureichende Schulung der Telearbeiter	B 4.1	(6.7)	Heterogene Netze
G 2.50	Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter	B 4.1	(6.7)	Heterogene Netze
G 2.51	Mangelhafte Einbindung des Telearbeiters in den Informationsfluss	B 1.11	(3.10)	Outsourcing
G 2.52	Erhöhte Reaktionszeiten bei IT-Systemausfall	B 2.8	(4.5)	Häuslicher Arbeitsplatz
G 2.53	Unzureichende Vertretungsregelungen für Telearbeit	B 2.10	(neu)	Mobiler Arbeitsplatz
G 2.54	Vertraulichkeitsverlust durch Restinformationen	B 2.8	(4.5)	Häuslicher Arbeitsplatz
		B 2.10	(neu)	Mobiler Arbeitsplatz
		B 5.5	(7.7)	Lotus Notes
		B 5.8	(9.3)	Telearbeit
		B 5.8	(9.3)	Telearbeit
		B 5.8	(9.3)	Telearbeit
		B 5.8	(9.3)	Telearbeit

		B 3.107	(6.10)	S/390- und zSeries-Mainframe
		B 3.302	(7.11)	Router und Switches
		B 5.3	(7.4)	E-Mail
G 2.55	Ungeordnete E-Mail-Nutzung			
		B 5.3	(7.4)	E-Mail
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 2.56	Mangelhafte Beschreibung von Dateien			
		B 5.3	(7.4)	E-Mail
G 2.57	Nicht ausreichende Speichermedien für den Notfall			
		B 5.7	(9.2)	Datenbanken
G 2.59	Betreiben von nicht angemeldeten Komponenten			
		B 4.2	(6.8)	Netz- und Systemmanagement
G 2.60	Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement			
		B 4.2	(6.8)	Netz- und Systemmanagement
G 2.61	Unberechtigte Sammlung personenbezogener Daten			
		B 4.2	(6.8)	Netz- und Systemmanagement
G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen			
		B 1.8	(3.8)	Behandlung von Sicherheitsvorfällen
G 2.63	Ungeordnete Faxnutzung			
		B 5.6	(8.5)	Faxserver
G 2.64	Fehlende Regelungen für das RAS-System			
		B 4.4	(7.6)	Remote Access
G 2.65	Komplexität der SAMBA-Konfiguration			
		B 3.102	(6.2)	Server unter Unix
		B 5.1	(6.3)	Peer-to-Peer-Dienste
G 2.66	Unzureichendes IT-Sicherheitsmanagement			
		B 1.0	(3.0)	IT-Sicherheitsmanagement
		B 1.11	(3.10)	Outsourcing
G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten			
		B 1.9	(3.9)	Hard- und Software-Management
		B 1.10	(9.1)	Standardsoftware
		B 1.11	(3.10)	Outsourcing
G 2.68	Fehlende oder unzureichende Planung des Active Directory			
		B 3.106	(6.9)	Server unter Windows 2000
G 2.69	Fehlende oder unzureichende Planung des Einsatzes von Novell eDirectory			
		B 5.9	(9.4)	Novell eDirectory
G 2.70	Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Novell eDirectory			
		B 5.9	(9.4)	Novell eDirectory
G 2.71	Fehlerhafte oder unzureichende Planung des LDAP-Zugriffs auf Novell eDirectory			
		B 5.9	(9.4)	Novell eDirectory

G 2.72	Unzureichende Migration von Archivsystemen	B 1.12	(9.5)	Archivierung
G 2.73	Fehlende Revisionsmöglichkeit von Archivsystemen	B 1.12	(9.5)	Archivierung
G 2.74	Unzureichende Ordnungskriterien für Archive	B 1.12	(9.5)	Archivierung
G 2.75	Mangelnde Kapazität von Archivdatenträgern	B 1.12	(9.5)	Archivierung
G 2.76	Unzureichende Dokumentation von Archivzugriffen	B 1.12	(9.5)	Archivierung
G 2.77	Unzulängliche Übertragung von Papierdaten in elektronische Archive	B 1.12	(9.5)	Archivierung
G 2.78	Unzulängliche Auffrischung von Datenbeständen bei der Archivierung	B 1.12	(9.5)	Archivierung
G 2.79	Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung	B 1.12	(9.5)	Archivierung
G 2.80	Unzureichende Durchführung von Revisionen bei der Archivierung	B 1.12	(9.5)	Archivierung
G 2.81	Unzureichende Vernichtung von Datenträgern bei der Archivierung	B 1.12	(9.5)	Archivierung
G 2.82	Fehlerhafte Planung des Aufstellungsortes von Archivsystemen	B 1.12	(9.5)	Archivierung
G 2.83	Fehlerhafte Outsourcing-Strategie	B 1.11	(3.10)	Outsourcing
G 2.84	Unzulängliche vertragliche Regelungen mit einem externen Dienstleister	B 1.11	(3.10)	Outsourcing
G 2.85	Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens	B 1.11	(3.10)	Outsourcing
G 2.86	Abhängigkeit von einem Outsourcing-Dienstleister	B 1.11	(3.10)	Outsourcing
G 2.87	Verwendung unsicherer Protokolle in öffentlichen Netzen	B 5.11	(7.9)	Apache Webserver
G 2.88	Störung des Betriebsklimas durch ein Outsourcing-Vorhaben	B 1.11	(3.10)	Outsourcing
G 2.89	Mangelhafte IT-Sicherheit in der Outsourcing-Einführungsphase	B 1.11	(3.10)	Outsourcing
G 2.90	Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister	B 1.11	(3.10)	Outsourcing
G 2.91	Fehlerhafte Planung der Migration von Exchange 5.5 nach Exchange 2000	B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 2.92	Fehlerhafte Regelungen für den Browser-Zugriff auf Exchange			

G 2.93	Unzureichendes Notfallvorsorgekonzept beim Outsourcing	B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 2.94	Unzureichende Planung des IIS-Einsatzes	B 1.11	(3.10)	Outsourcing
G 2.95	Fehlendes Konzept zur Anbindung anderer E-Mail-Systeme an Exchange/Outlook	B 5.10	(7.8)	Internet Information Server
G 2.96	Veraltete oder falsche Informationen in einem Webangebot	B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 2.97	Unzureichende Notfallplanung bei einem Apache-Webserver	B 5.4	(7.5)	Webserver
G 2.98	Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switches	B 5.11	(7.9)	Apache Webserver
G 2.99	Unzureichende oder fehlerhafte Konfiguration der zSeries-Systemumgebung	B 3.302	(7.11)	Router und Switches
G 2.100	Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 2.101	Unzureichende Notfallvorsorge bei einem Sicherheitsgateway	B 5.4	(7.5)	Webserver
G 2.102	Unzureichende Sensibilisierung für IT-Sicherheit	B 3.301	(7.3)	Sicherheitsgateway (Firewall)
G 2.103	Unzureichende Schulung der Mitarbeiter	B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
G 2.104	Inkompatibilität zwischen fremder und eigener IT	B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
G 2.105	Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen	B 2.11	(neu)	Besprechungs-, Veranstaltungs- und Schulungsräume
G 2.106	Störung der Geschäftsabläufe aufgrund von IT-Sicherheitsvorfällen	B 1.0	(3.0)	IT-Sicherheitsmanagement
G 2.107	Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes IT-Sicherheitsmanagement	B 1.0	(3.0)	IT-Sicherheitsmanagement
G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	B 1.0	(3.0)	IT-Sicherheitsmanagement
		B 1.2	(3.2)	Personal
		B 1.6	(3.6)	Computer-Virenschutzkonzept
		B 1.7	(3.7)	Kryptokonzept
		B 1.9	(3.9)	Hard- und Software-Management
		B 1.11	(3.10)	Outsourcing
		B 1.12	(9.5)	Archivierung
		B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
		B 3.208	(5.8)	Internet-PC
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN

G 3.2 Fahrlässige Zerstörung von Gerät oder Daten

B 5.2 (7.1) Datenträgeraustausch
B 5.3 (7.4) E-Mail
B 5.4 (7.5) Webserver
B 5.8 (9.3) Telearbeit
B 5.11 (7.9) Apache Webserver
B 5.12 (7.10) Exchange 2000 / Outlook 2000

G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen

B 1.2 (3.2) Personal
B 1.9 (3.9) Hard- und Software-Management
B 1.10 (9.1) Standardsoftware
B 3.101 (6.1) Allgemeiner Server
B 3.107 (6.10) S/390- und zSeries-Mainframe
B 3.202 (5.99) Allgemeines nicht vernetztes IT-System
B 3.203 (5.3) Laptop
B 3.204 (5.2) Client unter Unix
B 3.205 (5.5) Client unter Windows NT
B 3.206 (5.6) Client unter Windows 95
B 3.207 (5.7) Client unter Windows 2000
B 3.209 (neu) Client unter Windows XP
B 4.1 (6.7) Heterogene Netze
B 4.3 (7.2) Modem

B 1.2 (3.2) Personal
B 1.6 (3.6) Computer-Virenschutzkonzept
B 1.9 (3.9) Hard- und Software-Management
B 1.10 (9.1) Standardsoftware
B 1.13 (neu) IT-Sicherheitssensibilisierung und -schulung
B 2.10 (neu) Mobiler Arbeitsplatz
B 3.101 (6.1) Allgemeiner Server
B 3.107 (6.10) S/390- und zSeries-Mainframe
B 3.201 (neu) Allgemeiner Client
B 3.202 (5.99) Allgemeines nicht vernetztes IT-System
B 3.203 (5.3) Laptop
B 3.204 (5.2) Client unter Unix
B 3.205 (5.5) Client unter Windows NT
B 3.206 (5.6) Client unter Windows 95
B 3.207 (5.7) Client unter Windows 2000
B 3.208 (5.8) Internet-PC
B 3.209 (neu) Client unter Windows XP
B 3.301 (7.3) Sicherheitgateway (Firewall)
B 3.404 (8.6) Mobiltelefon

		B 3.405	(8.7)	PDA
		B 4.1	(6.7)	Heterogene Netze
		B 4.3	(7.2)	Modem
		B 5.2	(7.1)	Datenträgeraustausch
		B 5.3	(7.4)	E-Mail
		B 5.6	(8.5)	Faxserver
		B 5.8	(9.3)	Telearbeit
G 3.4	Unzulässige Kabelverbindungen			
G 3.5	Unbeabsichtigte Leitungsbeschädigung			
		B 2.2	(4.2)	Verkabelung
		B 1.9	(3.9)	Hard- und Software-Management
		B 2.2	(4.2)	Verkabelung
		B 3.101	(6.1)	Allgemeiner Server
		B 4.1	(6.7)	Heterogene Netze
		B 4.3	(7.2)	Modem
G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal			
		B 1.1	(3.1)	Organisation
		B 1.9	(3.9)	Hard- und Software-Management
		B 2.3	(4.3.1)	Bürraum
		B 2.8	(4.5)	Häuslicher Arbeitsplatz
		B 2.11	(neu)	Besprechungs-, Veranstaltungs- und Schulungsräume
		B 3.101	(6.1)	Allgemeiner Server
		B 3.201	(neu)	Allgemeiner Client
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.203	(5.3)	Laptop
		B 3.204	(5.2)	Client unter Unix
		B 3.205	(5.5)	Client unter Windows NT
		B 3.206	(5.6)	Client unter Windows 95
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 3.401	(8.1)	TK-Anlage
		B 4.1	(6.7)	Heterogene Netze
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.7	(9.2)	Datenbanken
G 3.7	Ausfall der TK-Anlage durch Fehlbedienung			
G 3.8	Fehlerhafte Nutzung des IT-Systems			
		B 3.401	(8.1)	TK-Anlage
		B 1.2	(3.2)	Personal
		B 1.9	(3.9)	Hard- und Software-Management
		B 1.10	(9.1)	Standardsoftware
		B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung

G 3.9	Fehlerhafte Administration des IT-Systems	B 3.101	(6.1)	Allgemeiner Server
		B 3.105	(6.6)	Server unter Novell Netware 4.x
		B 3.201	(neu)	Allgemeiner Client
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.203	(5.3)	Laptop
		B 3.204	(5.2)	Client unter Unix
		B 3.205	(5.5)	Client unter Windows NT
		B 3.206	(5.6)	Client unter Windows 95
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 4.1	(6.7)	Heterogene Netze
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.3	(7.4)	E-Mail
		B 1.2	(3.2)	Personal
		B 1.9	(3.9)	Hard- und Software-Management
G 3.10	Falsches Exportieren von Dateisystemen unter Unix	B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
		B 3.101	(6.1)	Allgemeiner Server
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.107	(6.10)	S/390- und zSeries-Mainframe
		B 3.201	(neu)	Allgemeiner Client
		B 3.204	(5.2)	Client unter Unix
		B 3.205	(5.5)	Client unter Windows NT
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.208	(5.8)	Internet-PC
		B 3.209	(neu)	Client unter Windows XP
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 4.1	(6.7)	Heterogene Netze
		B 4.2	(6.8)	Netz- und Systemmanagement
		B 5.1	(6.3)	Peer-to-Peer-Dienste
		B 5.5	(7.7)	Lotus Notes
G 3.11	Fehlerhafte Konfiguration von sendmail	B 5.8	(9.3)	Telearbeit
		B 5.9	(9.4)	Novell eDirectory
		B 5.11	(7.9)	Apache Webserver
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000
		B 3.102	(6.2)	Server unter Unix
G 3.12	Verlust der Datenträger beim Versand	B 1.9	(3.9)	Hard- und Software-Management
		B 3.102	(6.2)	Server unter Unix

G 3.13	Übertragung falscher oder nicht gewünschter Datensätze	B 5.2	(7.1)	Datenträgeraustausch
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.2	(7.1)	Datenträgeraustausch
		B 5.3	(7.4)	E-Mail
		B 5.8	(9.3)	Telearbeit
G 3.14	Fehleinschätzung der Rechtsverbindlichkeit eines Fax	B 5.9	(9.4)	Novell eDirectory
		B 3.402	(8.2)	Faxgerät
G 3.15	Fehlbedienung eines Anrufbeantworters	B 5.6	(8.5)	Faxserver
		B 3.403	(8.3)	Anrufbeantworter
G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten	B 1.10	(9.1)	Standardsoftware
		B 1.12	(9.5)	Archivierung
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.206	(5.6)	Client unter Windows 95
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.7	(9.2)	Datenbanken
		B 5.8	(9.3)	Telearbeit
		B 5.9	(9.4)	Novell eDirectory
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000
		B 1.9	(3.9)	Hard- und Software-Management
G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel	B 1.10	(9.1)	Standardsoftware
		B 3.201	(neu)	Allgemeiner Client
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.206	(5.6)	Client unter Windows 95
		B 5.1	(6.3)	Peer-to-Peer-Dienste
G 3.18	Freigabe von Verzeichnissen, Druckern oder der Ablagemappe	B 5.1	(6.3)	Peer-to-Peer-Dienste
G 3.19	Speichern von Passwörtern unter WfW und Windows 95	B 5.1	(6.3)	Peer-to-Peer-Dienste
G 3.20	Ungewollte Freigabe des Leserechtes bei Schedule+	B 5.1	(6.3)	Peer-to-Peer-Dienste
G 3.21	Fehlbedienung von Codeschlössern	B 2.7	(4.4)	Schutzschrank
G 3.22	Fehlerhafte Änderung der Registrierung	B 3.206	(5.6)	Client unter Windows 95
		B 3.209	(neu)	Client unter Windows XP
G 3.23	Fehlerhafte Administration eines DBMS	B 5.7	(9.2)	Datenbanken

G 3.24	Unbeabsichtigte Datenmanipulation	B 5.7	(9.2)	Datenbanken
G 3.25	Fahrlässiges Löschen von Objekten	B 3.105	(6.6)	Server unter Novell Netware 4.x
G 3.26	Ungewollte Freigabe des Dateisystems	B 3.105	(6.6)	Server unter Novell Netware 4.x
G 3.27	Fehlerhafte Zeitsynchronisation	B 3.105	(6.6)	Server unter Novell Netware 4.x
G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten	B 4.1	(6.7)	Heterogene Netze
		B 4.2	(6.8)	Netz- und Systemmanagement
G 3.29	Fehlende oder ungeeignete Segmentierung	B 4.1	(6.7)	Heterogene Netze
G 3.30	Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners	B 5.8	(9.3)	Telearbeit
G 3.31	Unstrukturierte Datenhaltung	B 3.101	(6.1)	Allgemeiner Server
G 3.32	Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahren	B 1.7	(3.7)	Kryptokonzept
G 3.33	Fehlbedienung von Kryptomodulen	B 1.7	(3.7)	Kryptokonzept
G 3.34	Ungeeignete Konfiguration des Managementsystems	B 4.2	(6.8)	Netz- und Systemmanagement
		B 5.9	(9.4)	Novell eDirectory
G 3.35	Server im laufenden Betrieb ausschalten	B 1.9	(3.9)	Hard- und Software-Management
		B 1.12	(9.5)	Archivierung
		B 4.2	(6.8)	Netz- und Systemmanagement
		B 5.9	(9.4)	Novell eDirectory
G 3.36	Fehlinterpretation von Ereignissen	B 1.2	(3.2)	Personal
		B 4.2	(6.8)	Netz- und Systemmanagement
		B 5.9	(9.4)	Novell eDirectory
G 3.37	Unproduktive Suchzeiten	B 1.2	(3.2)	Personal
		B 5.4	(7.5)	Webserver
G 3.38	Konfigurations- und Bedienungsfehler	B 3.105	(6.6)	Server unter Novell Netware 4.x
		B 3.107	(6.10)	S/390- und zSeries-Mainframe
		B 3.203	(5.3)	Laptop
		B 3.208	(5.8)	Internet-PC

		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 5.4	(7.5)	Webserver
		B 5.9	(9.4)	Novell eDirectory
		B 5.11	(7.9)	Apache Webserver
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 3.39	Fehlerhafte Administration des RAS-Systems			
G 3.40	Ungeeignete Nutzung von Authentisierungsdiensten bei Remote Access	B 4.4	(7.6)	Remote Access
G 3.41	Fehlverhalten bei der Nutzung von RAS-Diensten	B 4.4	(7.6)	Remote Access
G 3.42	Unsichere Konfiguration der RAS-Clients	B 4.4	(7.6)	Remote Access
G 3.43	Ungeeigneter Umgang mit Passwörtern	B 4.4	(7.6)	Remote Access
		B 1.2	(3.2)	Personal
		B 2.10	(neu)	Mobiler Arbeitsplatz
		B 3.404	(8.6)	Mobiltelefon
		B 3.405	(8.7)	PDA
		B 4.4	(7.6)	Remote Access
		B 5.5	(7.7)	Lotus Notes
		B 5.9	(9.4)	Novell eDirectory
G 3.44	Sorglosigkeit im Umgang mit Informationen			
		B 1.2	(3.2)	Personal
		B 1.6	(3.6)	Computer-Virenschutzkonzept
		B 1.9	(3.9)	Hard- und Software-Management
		B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
		B 2.10	(neu)	Mobiler Arbeitsplatz
		B 3.404	(8.6)	Mobiltelefon
		B 3.405	(8.7)	PDA
		B 4.4	(7.6)	Remote Access
		B 5.5	(7.7)	Lotus Notes
G 3.45	Unzureichende Identifikationsprüfung von Kommunikationspartnern			
		B 3.404	(8.6)	Mobiltelefon
		B 3.405	(8.7)	PDA
G 3.46	Fehlkonfiguration eines Lotus Notes Servers			
G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Notes	B 5.5	(7.7)	Lotus Notes
G 3.48	Fehlkonfiguration von Windows 2000/XP Rechnern	B 5.5	(7.7)	Lotus Notes
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP

G 3.49	Fehlkonfiguration des Active Directory	B 3.106	(6.9)	Server unter Windows 2000
G 3.50	Fehlkonfiguration von Novell eDirectory	B 5.9	(9.4)	Novell eDirectory
G 3.51	Falsche Vergabe von Zugriffsrechten im Novell eDirectory	B 5.9	(9.4)	Novell eDirectory
G 3.52	Fehlkonfiguration des Intranet-Clientzugriffs auf Novell eDirectory	B 5.9	(9.4)	Novell eDirectory
G 3.53	Fehlkonfiguration des LDAP-Zugriffs auf Novell eDirectory	B 5.9	(9.4)	Novell eDirectory
G 3.54	Verwendung ungeeigneter Datenträger bei der Archivierung	B 1.12	(9.5)	Archivierung
G 3.55	Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen	B 1.12	(9.5)	Archivierung
G 3.56	Fehlerhafte Einbindung des IIS in die Systemumgebung	B 5.10	(7.8)	Internet Information Server
G 3.57	Fehlerhafte Konfiguration des Betriebssystems für den IIS	B 5.10	(7.8)	Internet Information Server
G 3.58	Fehlkonfiguration eines IIS	B 5.10	(7.8)	Internet Information Server
G 3.59	Unzureichende Kenntnisse über aktuelle Sicherheitslücken und Prüfwerkzeuge für den IIS	B 5.10	(7.8)	Internet Information Server
G 3.60	Fehlkonfiguration von Exchange 2000 Servern	B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 3.61	Fehlerhafte Konfiguration von Outlook 2000 Clients	B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 3.62	Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver	B 5.11	(7.9)	Apache Webserver
G 3.63	Fehlerhafte Konfiguration eines Apache-Webservers	B 5.11	(7.9)	Apache Webserver
G 3.64	Fehlerhafte Konfiguration von Routern und Switches	B 3.302	(7.11)	Router und Switches
G 3.65	Fehlerhafte Administration von Routern und Switches	B 3.302	(7.11)	Router und Switches
G 3.66	Fehlerhafte Zeichensatzkonvertierung beim Einsatz von z/OS	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 3.67	Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 3.68	Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 3.69	Fehlerhafte Konfiguration der Unix System Services unter z/OS	B 3.107	(6.10)	S/390- und zSeries-Mainframe

G 3.70	Unzureichender Dateischutz des z/OS-Systems	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 3.71	Fehlerhafte Systemzeit bei z/OS-Systemen	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 3.72	Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 3.73	Fehlbedienung der z/OS-Systemfunktionen	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 3.74	Unzureichender Schutz der z/OS-Systemeinstellungen vor dynamischen Änderungen	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 3.75	Mangelhafte Kontrolle der Batch-Jobs bei z/OS	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 3.76	Fehler bei der Synchronisation mobiler Endgeräte	B 3.203	(5.3)	Laptop
		B 3.405	(8.7)	PDA
G 3.77	Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahmen	B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
G 3.78	Fliegende Verkabelung	B 2.11	(neu)	Besprechungs-, Veranstaltungs- und Schulungsräume
G 4.1	Ausfall der Stromversorgung	B 1.1	(3.1)	Organisation
		B 1.9	(3.9)	Hard- und Software-Management
		B 2.1	(4.1)	Gebäude
		B 2.4	(4.3.2)	Serverraum
		B 2.6	(4.3.4)	Raum für technische Infrastruktur
		B 2.7	(4.4)	Schutzschrank
		B 2.9	(4.6)	Rechenzentrum
		B 2.11	(neu)	Besprechungs-, Veranstaltungs- und Schulungsräume
		B 3.101	(6.1)	Allgemeiner Server
		B 3.104	(6.5)	Server unter Novell Netware 3.x
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.205	(5.5)	Client unter Windows NT
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 3.403	(8.3)	Anrufbeantworter
		B 4.1	(6.7)	Heterogene Netze
G 4.2	Ausfall interner Versorgungsnetze	B 1.1	(3.1)	Organisation
		B 2.1	(4.1)	Gebäude
		B 2.4	(4.3.2)	Serverraum

G 4.3	Ausfall vorhandener Sicherungseinrichtungen	B 2.6	(4.3.4)	Raum für technische Infrastruktur
		B 2.7	(4.4)	Schutzschrank
		B 2.9	(4.6)	Rechenzentrum
		B 2.11	(neu)	Besprechungs-, Veranstaltungs- und Schulungsräume
G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktoren	B 1.1	(3.1)	Organisation
		B 2.1	(4.1)	Gebäude
		B 2.7	(4.4)	Schutzschrank
		B 2.9	(4.6)	Rechenzentrum
G 4.5	Übersprechen	B 2.2	(4.2)	Verkabelung
		B 2.7	(4.4)	Schutzschrank
G 4.6	Spannungsschwankungen/Überspannung/Unterspannung	B 2.2	(4.2)	Verkabelung
		B 2.4	(4.3.2)	Serverraum
G 4.7	Defekte Datenträger	B 2.6	(4.3.4)	Raum für technische Infrastruktur
		B 3.101	(6.1)	Allgemeiner Server
		B 3.401	(8.1)	TK-Anlage
		B 4.3	(7.2)	Modem
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 1.9	(3.9)	Hard- und Software-Management
G 4.8	Bekanntwerden von Softwareschwachstellen	B 1.10	(9.1)	Standardsoftware
		B 1.12	(9.5)	Archivierung
		B 3.101	(6.1)	Allgemeiner Server
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.205	(5.5)	Client unter Windows NT
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 5.2	(7.1)	Datenträgeraustausch
		B 1.9	(3.9)	Hard- und Software-Management
		B 1.10	(9.1)	Standardsoftware
G 4.9	Ausfall der internen Stromversorgung	B 3.204	(5.2)	Client unter Unix
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 3.302	(7.11)	Router und Switches
		B 3.203	(5.3)	Laptop

G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	B 1.9	(3.9)	Hard- und Software-Management
		B 3.101	(6.1)	Allgemeiner Server
		B 3.103	(6.4)	Server unter Windows NT
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.107	(6.10)	S/390- und zSeries-Mainframe
		B 3.201	(neu)	Allgemeiner Client
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 4.1	(6.7)	Heterogene Netze
		B 5.4	(7.5)	Webserver
		B 5.9	(9.4)	Novell eDirectory
G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client	B 3.102	(6.2)	Server unter Unix
		B 3.204	(5.2)	Client unter Unix
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client	B 3.102	(6.2)	Server unter Unix
		B 3.204	(5.2)	Client unter Unix
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
G 4.13	Verlust gespeicherter Daten	B 1.4	(3.4)	Datensicherungskonzept
		B 1.9	(3.9)	Hard- und Software-Management
		B 1.12	(9.5)	Archivierung
		B 3.101	(6.1)	Allgemeiner Server
		B 3.201	(neu)	Allgemeiner Client
		B 3.203	(5.3)	Laptop
		B 5.3	(7.4)	E-Mail
		B 5.8	(9.3)	Telearbeit
		B 5.9	(9.4)	Novell eDirectory
		B 5.10	(7.8)	Internet Information Server
G 4.14	Verblässen spezieller Faxpapiere	B 3.402	(8.2)	Faxgerät
G 4.15	Fehlerhafte Faxübertragung	B 3.402	(8.2)	Faxgerät
		B 5.6	(8.5)	Faxserver
G 4.18	Entladene oder überalterte Notstromversorgung im Anrufbeantworter	B 3.403	(8.3)	Anrufbeantworter
G 4.19	Informationsverlust bei erschöpftem Speichermedium	B 3.203	(5.3)	Laptop
		B 3.403	(8.3)	Anrufbeantworter
G 4.20	Datenverlust bei erschöpftem Speichermedium			

		B 1.12	(9.5)	Archivierung
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 5.3	(7.4)	E-Mail
		B 5.6	(8.5)	Faxserver
G 4.21	Ausgleichsströme auf Schirmungen			
G 4.22	Software-Schwachstellen oder -Fehler	B 2.2	(4.2)	Verkabelung
		B 1.6	(3.6)	Computer-Virenschutzkonzept
		B 1.7	(3.7)	Kryptokonzept
		B 1.9	(3.9)	Hard- und Software-Management
		B 1.10	(9.1)	Standardsoftware
		B 3.101	(6.1)	Allgemeiner Server
		B 3.107	(6.10)	S/390- und zSeries-Mainframe
		B 3.203	(5.3)	Laptop
		B 3.208	(5.8)	Internet-PC
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 5.4	(7.5)	Webserver
		B 5.10	(7.8)	Internet Information Server
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 4.23	Automatische CD-ROM-Erkennung			
		B 3.103	(6.4)	Server unter Windows NT
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.205	(5.5)	Client unter Windows NT
		B 3.206	(5.6)	Client unter Windows 95
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
G 4.24	Dateinamenkonvertierung bei Datensicherungen unter Windows 95			
G 4.25	Nicht getrennte Verbindungen	B 3.206	(5.6)	Client unter Windows 95
G 4.26	Ausfall einer Datenbank	B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 1.12	(9.5)	Archivierung
		B 5.5	(7.7)	Lotus Notes
		B 5.7	(9.2)	Datenbanken
G 4.27	Unterlaufen von Zugriffskontrollen über ODBC			
		B 5.7	(9.2)	Datenbanken
G 4.28	Verlust von Daten einer Datenbank			
		B 5.5	(7.7)	Lotus Notes
		B 5.7	(9.2)	Datenbanken
G 4.29	Datenverlust einer Datenbank bei erschöpftem Speichermedium			
		B 5.7	(9.2)	Datenbanken

G 4.30	Verlust der Datenbankintegrität/-konsistenz	B 1.12	(9.5)	Archivierung
G 4.31	Ausfall oder Störung von Netzkomponenten	B 5.7	(9.2)	Datenbanken
		B 1.9	(3.9)	Hard- und Software-Management
		B 1.12	(9.5)	Archivierung
		B 4.1	(6.7)	Heterogene Netze
G 4.32	Nichtzustellung einer Nachricht	B 4.2	(6.8)	Netz- und Systemmanagement
		B 5.3	(7.4)	E-Mail
G 4.33	Schlechte oder fehlende Authentikation	B 5.12	(7.10)	Exchange 2000 / Outlook 2000
		B 1.7	(3.7)	Kryptokonzept
		B 1.11	(3.10)	Outsourcing
G 4.34	Ausfall eines Kryptomoduls	B 5.9	(9.4)	Novell eDirectory
		B 1.7	(3.7)	Kryptokonzept
		B 1.11	(3.10)	Outsourcing
G 4.35	Unsichere kryptographische Algorithmen	B 5.9	(9.4)	Novell eDirectory
		B 1.7	(3.7)	Kryptokonzept
		B 1.9	(3.9)	Hard- und Software-Management
		B 3.106	(6.9)	Server unter Windows 2000
		B 4.4	(7.6)	Remote Access
		B 5.5	(7.7)	Lotus Notes
G 4.36	Fehler in verschlüsselten Daten	B 1.7	(3.7)	Kryptokonzept
G 4.37	Mangelnde Authentizität und Vertraulichkeit von E-Mail	B 5.3	(7.4)	E-Mail
G 4.38	Ausfall von Komponenten eines Netz- und Systemmanagementsystems	B 1.9	(3.9)	Hard- und Software-Management
G 4.39	Software-Konzeptionsfehler	B 4.2	(6.8)	Netz- und Systemmanagement
		B 1.9	(3.9)	Hard- und Software-Management
		B 3.101	(6.1)	Allgemeiner Server
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 5.4	(7.5)	Webserver
		B 5.10	(7.8)	Internet Information Server
		B 5.11	(7.9)	Apache Webserver
G 4.40	Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients	B 4.4	(7.6)	Remote Access

G 4.41	Nicht-Verfügbarkeit des Mobilfunknetzes			
G 4.42	Ausfall des Mobiltelefons oder des PDAs	B 3.404	(8.6)	Mobiltelefon
		B 3.404	(8.6)	Mobiltelefon
		B 3.405	(8.7)	PDA
G 4.43	Undokumentierte Funktionen			
G 4.44	Ausfall von Novell eDirectory	B 1.9	(3.9)	Hard- und Software-Management
G 4.45	Verzögerte Archivauskunft	B 5.9	(9.4)	Novell eDirectory
G 4.46	Fehlerhafte Synchronisierung von Indexdaten bei der Archivierung	B 1.12	(9.5)	Archivierung
G 4.47	Veralten von Kryptoverfahren	B 1.12	(9.5)	Archivierung
G 4.48	Ausfall der Systeme eines Outsourcing-Dienstleisters	B 1.12	(9.5)	Archivierung
G 4.49	Unsichere Default-Einstellungen auf Routern und Switches	B 1.11	(3.10)	Outsourcing
G 4.50	Überlastung des z/OS-Betriebssystems	B 3.302	(7.11)	Router und Switches
G 4.51	Unzureichende Sicherheitsmechanismen bei PDAs	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 4.52	Datenverlust bei mobilem Einsatz	B 3.405	(8.7)	PDA
		B 3.203	(5.3)	Laptop
		B 3.405	(8.7)	PDA
G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	B 1.1	(3.1)	Organisation
		B 1.2	(3.2)	Personal
		B 1.9	(3.9)	Hard- und Software-Management
		B 2.3	(4.3.1)	Bürraum
		B 2.4	(4.3.2)	Serverraum
		B 2.6	(4.3.4)	Raum für technische Infrastruktur
		B 2.7	(4.4)	Schutzschrank
		B 2.8	(4.5)	Häuslicher Arbeitsplatz
		B 2.10	(neu)	Mobiler Arbeitsplatz
		B 3.101	(6.1)	Allgemeiner Server
		B 3.201	(neu)	Allgemeiner Client
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.203	(5.3)	Laptop
		B 3.204	(5.2)	Client unter Unix

G 5.2 Manipulation an Daten oder Software

B 3.205	(5.5)	Client unter Windows NT
B 3.208	(5.8)	Internet-PC
B 3.401	(8.1)	TK-Anlage
B 3.405	(8.7)	PDA
B 4.1	(6.7)	Heterogene Netze
B 5.2	(7.1)	Datenträgeraustausch
B 5.8	(9.3)	Telearbeit
B 1.1	(3.1)	Organisation
B 1.2	(3.2)	Personal
B 1.6	(3.6)	Computer-Virenschutzkonzept
B 1.9	(3.9)	Hard- und Software-Management
B 1.10	(9.1)	Standardsoftware
B 1.12	(9.5)	Archivierung
B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
B 2.3	(4.3.1)	Bürraum
B 2.4	(4.3.2)	Serverraum
B 2.8	(4.5)	Häuslicher Arbeitsplatz
B 2.10	(neu)	Mobiler Arbeitsplatz
B 3.101	(6.1)	Allgemeiner Server
B 3.107	(6.10)	S/390- und zSeries-Mainframe
B 3.201	(neu)	Allgemeiner Client
B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
B 3.203	(5.3)	Laptop
B 3.204	(5.2)	Client unter Unix
B 3.205	(5.5)	Client unter Windows NT
B 3.206	(5.6)	Client unter Windows 95
B 3.207	(5.7)	Client unter Windows 2000
B 3.208	(5.8)	Internet-PC
B 3.209	(neu)	Client unter Windows XP
B 3.301	(7.3)	Sicherheitsgateway (Firewall)
B 3.404	(8.6)	Mobiltelefon
B 3.405	(8.7)	PDA
B 4.1	(6.7)	Heterogene Netze
B 4.2	(6.8)	Netz- und Systemmanagement
B 4.3	(7.2)	Modem
B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
B 5.2	(7.1)	Datenträgeraustausch
B 5.3	(7.4)	E-Mail
B 5.4	(7.5)	Webserver
B 5.6	(8.5)	Faxserver

G 5.3	Unbefugtes Eindringen in ein Gebäude	B 5.8	(9.3)	Telearbeit
		B 5.10	(7.8)	Internet Information Server
		B 5.11	(7.9)	Apache Webserver
G 5.4	Diebstahl	B 1.1	(3.1)	Organisation
		B 2.1	(4.1)	Gebäude
		B 2.4	(4.3.2)	Serverraum
		B 2.5	(4.3.3)	Datenträgerarchiv
		B 2.6	(4.3.4)	Raum für technische Infrastruktur
		B 2.8	(4.5)	Häuslicher Arbeitsplatz
		B 2.9	(4.6)	Rechenzentrum
		B 1.1	(3.1)	Organisation
		B 1.9	(3.9)	Hard- und Software-Management
		B 2.1	(4.1)	Gebäude
G 5.5	Vandalismus	B 2.3	(4.3.1)	Bürraum
		B 2.4	(4.3.2)	Serverraum
		B 2.5	(4.3.3)	Datenträgerarchiv
		B 2.6	(4.3.4)	Raum für technische Infrastruktur
		B 2.7	(4.4)	Schutzschrank
		B 2.9	(4.6)	Rechenzentrum
		B 2.10	(neu)	Mobiler Arbeitsplatz
		B 2.11	(neu)	Besprechungs-, Veranstaltungs- und Schulungsräume
		B 3.201	(neu)	Allgemeiner Client
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.203	(5.3)	Laptop
		B 3.204	(5.2)	Client unter Unix
		B 3.205	(5.5)	Client unter Windows NT
		B 3.206	(5.6)	Client unter Windows 95
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 3.302	(7.11)	Router und Switches
		B 3.404	(8.6)	Mobiltelefon
		B 4.1	(6.7)	Heterogene Netze
		B 5.2	(7.1)	Datenträgeraustausch
		B 1.1	(3.1)	Organisation
		B 2.1	(4.1)	Gebäude
		B 2.3	(4.3.1)	Bürraum
		B 2.4	(4.3.2)	Serverraum
		B 2.5	(4.3.3)	Datenträgerarchiv

		B 2.6	(4.3.4)	Raum für technische Infrastruktur
		B 2.7	(4.4)	Schutzschrank
		B 2.9	(4.6)	Rechenzentrum
		B 4.1	(6.7)	Heterogene Netze
G 5.6	Anschlag			
		B 1.1	(3.1)	Organisation
		B 1.12	(9.5)	Archivierung
		B 2.1	(4.1)	Gebäude
		B 2.9	(4.6)	Rechenzentrum
		B 4.1	(6.7)	Heterogene Netze
G 5.7	Abhören von Leitungen			
		B 2.2	(4.2)	Verkabelung
		B 3.101	(6.1)	Allgemeiner Server
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.201	(neu)	Allgemeiner Client
		B 3.204	(5.2)	Client unter Unix
		B 3.209	(neu)	Client unter Windows XP
		B 3.402	(8.2)	Faxgerät
		B 4.1	(6.7)	Heterogene Netze
		B 4.3	(7.2)	Modem
		B 4.4	(7.6)	Remote Access
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.3	(7.4)	E-Mail
		B 5.5	(7.7)	Lotus Notes
		B 5.6	(8.5)	Faxserver
		B 5.8	(9.3)	Telearbeit
		B 5.11	(7.9)	Apache Webserver
G 5.8	Manipulation an Leitungen			
		B 2.2	(4.2)	Verkabelung
		B 3.204	(5.2)	Client unter Unix
		B 4.1	(6.7)	Heterogene Netze
		B 4.2	(6.8)	Netz- und Systemmanagement
		B 4.3	(7.2)	Modem
		B 4.4	(7.6)	Remote Access
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.5	(7.7)	Lotus Notes
G 5.9	Unberechtigte IT-Nutzung			
		B 1.9	(3.9)	Hard- und Software-Management
		B 1.10	(9.1)	Standardsoftware
		B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
		B 3.101	(6.1)	Allgemeiner Server

		B 3.201	(neu)	Allgemeiner Client
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.203	(5.3)	Laptop
		B 3.204	(5.2)	Client unter Unix
		B 3.205	(5.5)	Client unter Windows NT
		B 3.206	(5.6)	Client unter Windows 95
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 3.405	(8.7)	PDA
		B 4.1	(6.7)	Heterogene Netze
		B 4.2	(6.8)	Netz- und Systemmanagement
		B 4.3	(7.2)	Modem
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.2	(7.1)	Datenträgeraustausch
		B 5.3	(7.4)	E-Mail
		B 5.6	(8.5)	Faxserver
		B 5.7	(9.2)	Datenbanken
		B 5.8	(9.3)	Telearbeit
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 5.10	Missbrauch von Fernwartungszugängen			
		B 1.11	(3.10)	Outsourcing
		B 3.107	(6.10)	S/390- und zSeries-Mainframe
		B 4.3	(7.2)	Modem
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.7	(9.2)	Datenbanken
		B 5.8	(9.3)	Telearbeit
G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten			
G 5.12	Abhören von Telefongesprächen und Datenübertragungen	B 3.401	(8.1)	TK-Anlage
		B 1.1	(3.1)	Organisation
		B 3.401	(8.1)	TK-Anlage
		B 4.3	(7.2)	Modem
G 5.13	Abhören von Räumen	B 1.1	(3.1)	Organisation
		B 3.401	(8.1)	TK-Anlage
G 5.14	Gebührenbetrug	B 3.401	(8.1)	TK-Anlage
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
G 5.15	"Neugierige" Mitarbeiter	B 3.101	(6.1)	Allgemeiner Server

G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal	B 3.401	(8.1)	TK-Anlage
		B 1.1	(3.1)	Organisation
		B 2.7	(4.4)	Schutzschrank
		B 2.9	(4.6)	Rechenzentrum
		B 3.401	(8.1)	TK-Anlage
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal	B 5.9	(9.4)	Novell eDirectory
		B 1.1	(3.1)	Organisation
		B 2.7	(4.4)	Schutzschrank
		B 2.9	(4.6)	Rechenzentrum
		B 3.401	(8.1)	TK-Anlage
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
G 5.18	Systematisches Ausprobieren von Passwörtern	B 5.9	(9.4)	Novell eDirectory
		B 3.101	(6.1)	Allgemeiner Server
		B 3.107	(6.10)	S/390- und zSeries-Mainframe
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.203	(5.3)	Laptop
		B 3.204	(5.2)	Client unter Unix
G 5.19	Missbrauch von Benutzerrechten	B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 4.1	(6.7)	Heterogene Netze
		B 4.2	(6.8)	Netz- und Systemmanagement
		B 4.3	(7.2)	Modem
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.7	(9.2)	Datenbanken
		B 5.8	(9.3)	Telearbeit
		B 5.9	(9.4)	Novell eDirectory
		B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
		B 3.101	(6.1)	Allgemeiner Server
		B 3.107	(6.10)	S/390- und zSeries-Mainframe
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.204	(5.2)	Client unter Unix
		B 5.4	(7.5)	Webserver
		B 5.8	(9.3)	Telearbeit
		B 5.9	(9.4)	Novell eDirectory
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000

G 5.20 Missbrauch von Administratorrechten

B 1.2	(3.2)	Personal
B 1.11	(3.10)	Outsourcing
B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
B 3.101	(6.1)	Allgemeiner Server
B 3.201	(neu)	Allgemeiner Client
B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
B 3.204	(5.2)	Client unter Unix
B 4.1	(6.7)	Heterogene Netze
B 5.4	(7.5)	Webserver
B 5.8	(9.3)	Telearbeit
B 5.9	(9.4)	Novell eDirectory
B 5.10	(7.8)	Internet Information Server

G 5.21 Trojanische Pferde

B 1.6	(3.6)	Computer-Virenschutzkonzept
B 1.9	(3.9)	Hard- und Software-Management
B 1.10	(9.1)	Standardsoftware
B 3.101	(6.1)	Allgemeiner Server
B 3.107	(6.10)	S/390- und zSeries-Mainframe
B 3.201	(neu)	Allgemeiner Client
B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
B 3.203	(5.3)	Laptop
B 3.204	(5.2)	Client unter Unix
B 3.205	(5.5)	Client unter Windows NT
B 3.206	(5.6)	Client unter Windows 95
B 3.207	(5.7)	Client unter Windows 2000
B 3.208	(5.8)	Internet-PC
B 3.209	(neu)	Client unter Windows XP
B 5.3	(7.4)	E-Mail
B 5.4	(7.5)	Webserver
B 5.8	(9.3)	Telearbeit
B 5.11	(7.9)	Apache Webserver

G 5.22 Diebstahl bei mobiler Nutzung des IT-Systems

B 3.203	(5.3)	Laptop
B 3.405	(8.7)	PDA
B 4.4	(7.6)	Remote Access
B 5.5	(7.7)	Lotus Notes

G 5.23 Computer-Viren

B 1.2	(3.2)	Personal
B 1.6	(3.6)	Computer-Virenschutzkonzept
B 1.9	(3.9)	Hard- und Software-Management

		B 1.10	(9.1)	Standardsoftware
		B 3.101	(6.1)	Allgemeiner Server
		B 3.103	(6.4)	Server unter Windows NT
		B 3.104	(6.5)	Server unter Novell Netware 3.x
		B 3.105	(6.6)	Server unter Novell Netware 4.x
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.201	(neu)	Allgemeiner Client
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.203	(5.3)	Laptop
		B 3.204	(5.2)	Client unter Unix
		B 3.205	(5.5)	Client unter Windows NT
		B 3.206	(5.6)	Client unter Windows 95
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.208	(5.8)	Internet-PC
		B 3.209	(neu)	Client unter Windows XP
		B 3.405	(8.7)	PDA
		B 4.3	(7.2)	Modem
		B 5.2	(7.1)	Datenträgeraustausch
		B 5.3	(7.4)	E-Mail
		B 5.4	(7.5)	Webserver
		B 5.8	(9.3)	Telearbeit
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 5.24	Wiedereinspielen von Nachrichten	B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 5.3	(7.4)	E-Mail
		B 5.6	(8.5)	Faxserver
		B 5.8	(9.3)	Telearbeit
G 5.25	Maskerade	B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 4.3	(7.2)	Modem
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.3	(7.4)	E-Mail
		B 5.6	(8.5)	Faxserver
		B 5.8	(9.3)	Telearbeit
G 5.26	Analyse des Nachrichtenflusses	B 1.9	(3.9)	Hard- und Software-Management
		B 3.101	(6.1)	Allgemeiner Server
		B 5.3	(7.4)	E-Mail
G 5.27	Nichtanerkennung einer Nachricht	B 1.7	(3.7)	Kryptokonzept
		B 5.3	(7.4)	E-Mail

G 5.28	Verhinderung von Diensten	B 5.6	(8.5)	Faxserver
		B 3.107	(6.10)	S/390- und zSeries-Mainframe
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 4.1	(6.7)	Heterogene Netze
		B 4.2	(6.8)	Netz- und Systemmanagement
		B 5.3	(7.4)	E-Mail
		B 5.4	(7.5)	Webserver
		B 5.10	(7.8)	Internet Information Server
		B 5.11	(7.9)	Apache Webserver
G 5.29	Unberechtigtes Kopieren der Datenträger	B 1.12	(9.5)	Archivierung
G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers	B 5.2	(7.1)	Datenträgeraustausch
		B 3.402	(8.2)	Faxgerät
		B 5.6	(8.5)	Faxserver
G 5.31	Unbefugtes Lesen von Faxsendungen	B 3.402	(8.2)	Faxgerät
		B 5.6	(8.5)	Faxserver
G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxservern	B 3.402	(8.2)	Faxgerät
		B 5.6	(8.5)	Faxserver
G 5.33	Vortäuschen eines falschen Absenders bei Faxsendungen	B 3.402	(8.2)	Faxgerät
		B 5.6	(8.5)	Faxserver
G 5.34	Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes	B 3.402	(8.2)	Faxgerät
G 5.35	Überlastung durch Faxsendungen	B 3.402	(8.2)	Faxgerät
		B 5.6	(8.5)	Faxserver
G 5.36	Absichtliche Überlastung des Anrufbeantworters	B 3.403	(8.3)	Anrufbeantworter
G 5.37	Ermitteln des Sicherungscodes	B 3.403	(8.3)	Anrufbeantworter
G 5.38	Missbrauch der Fernabfrage	B 3.403	(8.3)	Anrufbeantworter
G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten	B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 4.3	(7.2)	Modem
		B 4.4	(7.6)	Remote Access
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN

G 5.40	Abhören von Räumen mittels Rechner mit Mikrofon	B 5.6	(8.5)	Faxserver
		B 3.101	(6.1)	Allgemeiner Server
		B 3.201	(neu)	Allgemeiner Client
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp			
		B 3.102	(6.2)	Server unter Unix
		B 3.204	(5.2)	Client unter Unix
G 5.42	Social Engineering			
		B 1.2	(3.2)	Personal
		B 1.11	(3.10)	Outsourcing
		B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
G 5.43	Makro-Viren			
		B 1.2	(3.2)	Personal
		B 1.6	(3.6)	Computer-Virenschutzkonzept
		B 1.9	(3.9)	Hard- und Software-Management
		B 1.10	(9.1)	Standardsoftware
		B 3.103	(6.4)	Server unter Windows NT
		B 3.104	(6.5)	Server unter Novell Netware 3.x
		B 3.105	(6.6)	Server unter Novell Netware 4.x
		B 3.201	(neu)	Allgemeiner Client
		B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System
		B 3.203	(5.3)	Laptop
		B 3.205	(5.5)	Client unter Windows NT
		B 3.206	(5.6)	Client unter Windows 95
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.208	(5.8)	Internet-PC
		B 3.209	(neu)	Client unter Windows XP
		B 5.2	(7.1)	Datenträgeraustausch
		B 5.3	(7.4)	E-Mail
		B 5.4	(7.5)	Webserver
		B 5.8	(9.3)	Telearbeit
G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlagen	B 3.401	(8.1)	TK-Anlage
G 5.45	Ausprobieren von Passwörtern unter WfW und Windows 95			
G 5.46	Maskerade unter WfW	B 5.1	(6.3)	Peer-to-Peer-Dienste
G 5.47	Löschen des Post-Office unter WfW	B 5.1	(6.3)	Peer-to-Peer-Dienste
G 5.48	IP-Spoofing	B 5.1	(6.3)	Peer-to-Peer-Dienste

		B 3.208	(5.8)	Internet-PC
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
		B 5.4	(7.5)	Webserver
G 5.49	Missbrauch des Source-Routing			
G 5.50	Missbrauch des ICMP-Protokolls	B 3.301	(7.3)	Sicherheitsgateway (Firewall)
G 5.51	Missbrauch der Routing-Protokolle	B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 3.302	(7.11)	Router und Switches
G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System			
		B 3.103	(6.4)	Server unter Windows NT
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.205	(5.5)	Client unter Windows NT
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
G 5.53	Bewusste Fehlbedienung von Schutzschranken aus Bequemlichkeit			
G 5.54	Vorsätzliches Herbeiführen eines Abnormal End	B 2.7	(4.4)	Schutzschrank
G 5.55	Login Bypass	B 3.104	(6.5)	Server unter Novell Netware 3.x
		B 3.104	(6.5)	Server unter Novell Netware 3.x
		B 3.105	(6.6)	Server unter Novell Netware 4.x
G 5.56	Temporär frei zugängliche Accounts			
		B 3.104	(6.5)	Server unter Novell Netware 3.x
		B 3.105	(6.6)	Server unter Novell Netware 4.x
G 5.57	Netzanalyse-Tools			
		B 3.104	(6.5)	Server unter Novell Netware 3.x
		B 3.105	(6.6)	Server unter Novell Netware 4.x
		B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 5.58	"Hacking Novell Netware"			
		B 3.104	(6.5)	Server unter Novell Netware 3.x
		B 3.105	(6.6)	Server unter Novell Netware 4.x
G 5.59	Missbrauch von Administratorrechten unter Novell Netware 3.x			
		B 3.104	(6.5)	Server unter Novell Netware 3.x
		B 3.105	(6.6)	Server unter Novell Netware 4.x
G 5.60	Umgehen der Systemrichtlinien			
G 5.61	Missbrauch von Remote-Zugängen für Managementfunktionen von Routern	B 3.206	(5.6)	Client unter Windows 95
		B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN

G 5.62	Missbrauch von Ressourcen über abgesetzte IT-Systeme	B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
G 5.63	Manipulationen über den ISDN-D-Kanal	B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
G 5.64	Manipulation an Daten oder Software bei Datenbanksystemen	B 5.7	(9.2)	Datenbanken
G 5.65	Verhinderung der Dienste eines Datenbanksystems	B 5.7	(9.2)	Datenbanken
		B 5.9	(9.4)	Novell eDirectory
G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz	B 3.302	(7.11)	Router und Switches
		B 4.1	(6.7)	Heterogene Netze
		B 4.2	(6.8)	Netz- und Systemmanagement
G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen	B 4.1	(6.7)	Heterogene Netze
		B 4.2	(6.8)	Netz- und Systemmanagement
G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten	B 1.1	(3.1)	Organisation
		B 1.9	(3.9)	Hard- und Software-Management
		B 2.9	(4.6)	Rechenzentrum
		B 4.1	(6.7)	Heterogene Netze
G 5.69	Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz	B 2.8	(4.5)	Häuslicher Arbeitsplatz
G 5.70	Manipulation durch Familienangehörige und Besucher	B 2.8	(4.5)	Häuslicher Arbeitsplatz
G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	B 1.7	(3.7)	Kryptokonzept
		B 1.9	(3.9)	Hard- und Software-Management
		B 1.11	(3.10)	Outsourcing
		B 2.8	(4.5)	Häuslicher Arbeitsplatz
		B 2.10	(neu)	Mobiler Arbeitsplatz
		B 3.101	(6.1)	Allgemeiner Server
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.201	(neu)	Allgemeiner Client
		B 3.203	(5.3)	Laptop
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 4.4	(7.6)	Remote Access
		B 5.3	(7.4)	E-Mail
		B 5.5	(7.7)	Lotus Notes
		B 5.8	(9.3)	Telearbeit

		B 5.10	(7.8)	Internet Information Server
		B 5.11	(7.9)	Apache Webserver
G 5.72	Mißbräuchliche E-Mail-Nutzung			
G 5.73	Vortäuschen eines falschen Absenders	B 5.3	(7.4)	E-Mail
G 5.74	Manipulation von Alias-Dateien oder Verteilerlisten	B 5.3	(7.4)	E-Mail
G 5.75	Überlastung durch eingehende E-Mails	B 5.3	(7.4)	E-Mail
G 5.76	Mailbomben	B 5.3	(7.4)	E-Mail
G 5.77	Mitlesen von E-Mails	B 5.3	(7.4)	E-Mail
		B 5.3	(7.4)	E-Mail
		B 5.5	(7.7)	Lotus Notes
G 5.78	DNS-Spoofing	B 5.12	(7.10)	Exchange 2000 / Outlook 2000
		B 3.208	(5.8)	Internet-PC
		B 3.301	(7.3)	Sicherheitsgateway (Firewall)
		B 5.4	(7.5)	Webserver
G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen	B 5.9	(9.4)	Novell eDirectory
		B 1.9	(3.9)	Hard- und Software-Management
		B 3.103	(6.4)	Server unter Windows NT
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.205	(5.5)	Client unter Windows NT
		B 3.207	(5.7)	Client unter Windows 2000
G 5.80	Hoax	B 3.209	(neu)	Client unter Windows XP
		B 1.2	(3.2)	Personal
		B 1.6	(3.6)	Computer-Virenschutzkonzept
G 5.81	Unautorisierte Benutzung eines Kryptomoduls	B 3.404	(8.6)	Mobiltelefon
		B 1.7	(3.7)	Kryptokonzept
G 5.82	Manipulation eines Kryptomoduls	B 5.9	(9.4)	Novell eDirectory
		B 1.7	(3.7)	Kryptokonzept
		B 1.9	(3.9)	Hard- und Software-Management
G 5.83	Kompromittierung kryptographischer Schlüssel	B 1.12	(9.5)	Archivierung
		B 1.7	(3.7)	Kryptokonzept

		B 1.9	(3.9)	Hard- und Software-Management
		B 1.12	(9.5)	Archivierung
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 4.4	(7.6)	Remote Access
		B 5.5	(7.7)	Lotus Notes
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 5.84	Gefälschte Zertifikate			
		B 1.7	(3.7)	Kryptokonzept
		B 1.9	(3.9)	Hard- und Software-Management
		B 3.106	(6.9)	Server unter Windows 2000
		B 5.5	(7.7)	Lotus Notes
		B 5.10	(7.8)	Internet Information Server
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 5.85	Integritätsverlust schützenswerter Informationen			
		B 1.7	(3.7)	Kryptokonzept
		B 1.11	(3.10)	Outsourcing
		B 1.12	(9.5)	Archivierung
		B 3.101	(6.1)	Allgemeiner Server
		B 3.106	(6.9)	Server unter Windows 2000
		B 3.201	(neu)	Allgemeiner Client
		B 3.207	(5.7)	Client unter Windows 2000
		B 3.209	(neu)	Client unter Windows XP
		B 5.3	(7.4)	E-Mail
		B 5.5	(7.7)	Lotus Notes
		B 5.11	(7.9)	Apache Webserver
		B 5.12	(7.10)	Exchange 2000 / Outlook 2000
G 5.86	Manipulation von Managementparametern			
G 5.87	Web-Spoofing	B 4.2	(6.8)	Netz- und Systemmanagement
		B 1.9	(3.9)	Hard- und Software-Management
		B 3.208	(5.8)	Internet-PC
		B 5.4	(7.5)	Webserver
G 5.88	Missbrauch aktiver Inhalte			
		B 3.208	(5.8)	Internet-PC
		B 5.4	(7.5)	Webserver
		B 5.10	(7.8)	Internet Information Server
G 5.89	Hijacking von Netz-Verbindungen			
		B 3.102	(6.2)	Server unter Unix
		B 3.204	(5.2)	Client unter Unix
G 5.90	Manipulation von Adressbüchern und Verteillisten			

G 5.91	Abschalten von Sicherheitsmechanismen für den RAS-Zugang	B 5.6	(8.5)	Faxserver
G 5.92	Nutzung des RAS-Clients als RAS-Server	B 3.208	(5.8)	Internet-PC
G 5.93	Erlauben von Fremdnutzung von RAS-Komponenten	B 4.4	(7.6)	Remote Access
G 5.94	Kartenmissbrauch	B 4.4	(7.6)	Remote Access
G 5.95	Abhören von Raumgesprächen über Mobiltelefone	B 4.4	(7.6)	Remote Access
G 5.96	Manipulation von Mobiltelefonen	B 3.404	(8.6)	Mobiltelefon
G 5.97	Unberechtigte Datenweitergabe über Mobiltelefone	B 3.404	(8.6)	Mobiltelefon
G 5.98	Abhören von Mobiltelefonaten	B 3.404	(8.6)	Mobiltelefon
G 5.99	Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen	B 3.404	(8.6)	Mobiltelefon
G 5.100	Missbrauch aktiver Inhalte beim Zugriff auf Lotus Notes	B 3.404	(8.6)	Mobiltelefon
G 5.101	"Hacking Lotus Notes"	B 5.5	(7.7)	Lotus Notes
G 5.102	Sabotage	B 5.5	(7.7)	Lotus Notes
G 5.103	Missbrauch von Webmail	B 1.1	(3.1)	Organisation
G 5.104	Ausspähen von Informationen	B 1.12	(9.5)	Archivierung
G 5.105	Verhinderung der Dienste von Archivsystemen	B 2.9	(4.6)	Rechenzentrum
G 5.106	Unberechtigtes Überschreiben oder Löschen von Archivmedien	B 3.208	(5.8)	Internet-PC
G 5.107	Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister	B 1.2	(3.2)	Personal
G 5.108	Ausnutzen von systemspezifischen Schwachstellen des IIS	B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung
		B 1.12	(9.5)	Archivierung
		B 1.12	(9.5)	Archivierung
		B 1.11	(3.10)	Outsourcing
		B 5.10	(7.8)	Internet Information Server

G 5.109	Ausnutzen systemspezifischer Schwachstellen beim Apache-Webserver	B 5.11	(7.9)	Apache Webserver
G 5.110	Web-Bugs	B 5.3	(7.4)	E-Mail
G 5.111	Missbrauch aktiver Inhalte in E-Mails	B 5.3	(7.4)	E-Mail
G 5.112	Manipulation von ARP-Tabellen	B 3.302	(7.11)	Router und Switches
G 5.113	MAC-Spoofing	B 3.302	(7.11)	Router und Switches
G 5.114	Missbrauch von Spanning Tree	B 3.302	(7.11)	Router und Switches
G 5.115	Überwindung der Grenzen zwischen VLANs	B 3.302	(7.11)	Router und Switches
G 5.116	Manipulation der z/OS-Systemsteuerung	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 5.117	Verschleiern von Manipulationen unter z/OS	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 5.118	Unbefugtes Erlangen höherer Rechte im RACF	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 5.119	Benutzung fremder Kennungen unter z/OS-Systemen	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 5.120	Manipulation der Linux/zSeries Systemsteuerung	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 5.121	Angriffe über TCP/IP auf z/OS-Systeme	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 5.122	Missbrauch von RACF-Attributen unter z/OS	B 3.107	(6.10)	S/390- und zSeries-Mainframe
G 5.123	Abhören von Raumgesprächen über mobile Endgeräte	B 3.203	(5.3)	Laptop
		B 3.405	(8.7)	PDA
G 5.124	Missbrauch der Informationen von mobilen Endgeräten	B 3.203	(5.3)	Laptop
		B 3.405	(8.7)	PDA
G 5.125	Unberechtigte Datenweitergabe über mobile Endgeräte	B 3.203	(5.3)	Laptop
		B 3.405	(8.7)	PDA
G 5.126	Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten	B 3.203	(5.3)	Laptop
		B 3.404	(8.6)	Mobiltelefon
		B 3.405	(8.7)	PDA

G 5.127 Spyware

B 1.6 (3.6) Computer-Virenschutzkonzept