Bausteine und zugeordnete Gefährdungen

Baustein	Alt	Bausteinname	Gefährdung	Gefährdungstitel
B 1.0	(3.0)	IT-Sicherheitsmanagement		
			G 2.66	Unzureichendes IT-Sicherheitsmanagement
			G 2.105	Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen
			G 2.106	Störung der Geschäftsabläufe aufgrund von IT-Sicherheitsvorfällen
			G 2.107	Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes IT-Sicherheitsmanagement
B 1.1	(3.1)	Organisation		
			G 1.4	Feuer
			G 1.5	Wasser
			G 1.7	Unzulässige Temperatur und Luftfeuchte
			G 2.1	Fehlende oder unzureichende Regelungen
			G 2.2	Unzureichende Kenntnis über Regelungen
			G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel
			G 2.5	Fehlende oder unzureichende Wartung
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen
			G 2.7	Unerlaubte Ausübung von Rechten
			G 2.8	Unkontrollierter Einsatz von Betriebsmitteln
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
			G 4.1	Ausfall der Stromversorgung
			G 4.2	Ausfall interner Versorgungsnetze
			G 4.3	Ausfall vorhandener Sicherungseinrichtungen
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.2	Manipulation an Daten oder Software
			G 5.3	Unbefugtes Eindringen in ein Gebäude
			G 5.4	Diebstahl
			G 5.5	Vandalismus
			G 5.6	Anschlag
			G 5.12	Abhören von Telefongesprächen und Datenübertragungen
			G 5.13	Abhören von Räumen
			G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
			G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
			G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
			G 5.102	Sabotage
B 1.2	(3.2)	Personal		
			G 1.1	Personalausfall
			G 1.2	Ausfall des IT-Systems
			G 2.2	Unzureichende Kenntnis über Regelungen
			G 2.7	Unerlaubte Ausübung von Rechten
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten

			G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.8 Fehlerhafte Nutzung des IT-Systems
			G 3.9 Fehlerhafte Administration des IT-Systems
			G 3.36 Fehlinterpretation von Ereignissen
			G 3.37 Unproduktive Suchzeiten
			G 3.43 Ungeeigneter Umgang mit Passwörtern
			G 3.44 Sorglosigkeit im Umgang mit Informationen
			G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.2 Manipulation an Daten oder Software
			G 5.20 Missbrauch von Administratorrechten
			G 5.23 Computer-Viren
			G 5.42 Social Engineering
			G 5.43 Makro-Viren
			G 5.80 Hoax
			G 5.104 Ausspähen von Informationen
B 1.3	(3.3)	Notfallvorsorgekonzept	
			G 1.2 Ausfall des IT-Systems
B 1.4	(3.4)	Datensicherungskonzept	
			G 4.13 Verlust gespeicherter Daten
B 1.6	(3.6)	Computer-Virenschutzkonzept	
			G 2.1 Fehlende oder unzureichende Regelungen
			G 2.2 Unzureichende Kenntnis über Regelungen
			G 2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel
			G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
			G 2.8 Unkontrollierter Einsatz von Betriebsmitteln
			G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			G 2.26 Fehlendes oder unzureichendes Test- und Freigabeverfahren
			G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
			G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.44 Sorglosigkeit im Umgang mit Informationen
			G 4.22 Software-Schwachstellen oder -Fehler
			G 5.2 Manipulation an Daten oder Software
			G 5.21 Trojanische Pferde
			G 5.23 Computer-Viren
			G 5.43 Makro-Viren
			G 5.80 Hoax
			G 5.127 Spyware
B 1.7	(3.7)	Kryptokonzept	
			G 2.1 Fehlende oder unzureichende Regelungen
			G 2.2 Unzureichende Kenntnis über Regelungen
			G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen

			G 2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung
			G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
			G 3.32 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahren
			G 3.33 Fehlbedienung von Kryptomodulen
			G 4.22 Software-Schwachstellen oder -Fehler
			G 4.33 Schlechte oder fehlende Authentikation
			G 4.34 Ausfall eines Kryptomoduls
			G 4.35 Unsichere kryptographische Algorithmen
			G 4.36 Fehler in verschlüsselten Daten
			G 5.27 Nichtanerkennung einer Nachricht
			G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
			G 5.81 Unautorisierte Benutzung eines Kryptomoduls
			G 5.82 Manipulation eines Kryptomoduls
			G 5.83 Kompromittierung kryptographischer Schlüssel
			G 5.84 Gefälschte Zertifikate
			G 5.85 Integritätsverlust schützenswerter Informationen
B 1.8	(3.8)	Behandlung von Sicherheitsvorfällen	
			G 2.62 Ungeeigneter Umgang mit Sicherheitsvorfällen
B 1.9	(3.9)	Hard- und Software-Management	
			G 1.1 Personalausfall
			G 1.2 Ausfall des IT-Systems
			G 1.4 Feuer
			G 1.5 Wasser
			G 1.8 Staub, Verschmutzung
			G 2.1 Fehlende oder unzureichende Regelungen
			G 2.2 Unzureichende Kenntnis über Regelungen
			G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
			G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen
			G 2.7 Unerlaubte Ausübung von Rechten
			G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			G 2.10 Nicht fristgerecht verfügbare Datenträger
			G 2.15 Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
			G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern
			G 2.22 Fehlende Auswertung von Protokolldaten
			G 2.23 Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz
			G 2.67 Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten
			G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
			G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
			G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.5 Unbeabsichtigte Leitungsbeschädigung
			G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal

		G 3.8	Fehlerhafte Nutzung des IT-Systems
		G 3.9	Fehlerhafte Administration des IT-Systems
		G 3.11	Fehlerhafte Konfiguration von sendmail
		G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel
		G 3.35	Server im laufenden Betrieb ausschalten
		G 3.44	Sorglosigkeit im Umgang mit Informationen
		G 4.1	Ausfall der Stromversorgung
		G 4.7	Defekte Datenträger
		G 4.8	Bekanntwerden von Softwareschwachstellen
		G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
		G 4.13	Verlust gespeicherter Daten
		G 4.22	Software-Schwachstellen oder -Fehler
		G 4.31	Ausfall oder Störung von Netzkomponenten
		G 4.35	Unsichere kryptographische Algorithmen
		G 4.38	Ausfall von Komponenten eines Netz- und Systemmanagementsystems
		G 4.39	Software-Konzeptionsfehler
		G 4.43	Undokumentierte Funktionen
		G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
		G 5.2	Manipulation an Daten oder Software
		G 5.4	Diebstahl
		G 5.9	Unberechtigte IT-Nutzung
		G 5.21	Trojanische Pferde
		G 5.23	Computer-Viren
		G 5.26	Analyse des Nachrichtenflusses
		G 5.43	Makro-Viren
		G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
		G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
		G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
		G 5.82	Manipulation eines Kryptomoduls
		G 5.83	Kompromittierung kryptographischer Schlüssel
		G 5.84	Gefälschte Zertifikate
		G 5.87	Web-Spoofing
B 1.10	(9.1) Standardsoftware		
		G 1.2	Ausfall des IT-Systems
		G 2.1	Fehlende oder unzureichende Regelungen
		G 2.2	Unzureichende Kenntnis über Regelungen
		G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel
		G 2.7	Unerlaubte Ausübung von Rechten
		G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
		G 2.27	Fehlende oder unzureichende Dokumentation
		G 2.28	Verstöße gegen das Urheberrecht

	G 2.29	Softwaretest mit Produktionsdaten
	G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten
	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
	G 3.8	Fehlerhafte Nutzung des IT-Systems
	G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten
	G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel
	G 4.7	Defekte Datenträger
	G 4.8	Bekanntwerden von Softwareschwachstellen
	G 4.22	Software-Schwachstellen oder -Fehler
	G 5.2	Manipulation an Daten oder Software
	G 5.9	Unberechtigte IT-Nutzung
	G 5.21	Trojanische Pferde
	G 5.23	Computer-Viren
	G 5.43	Makro-Viren
B 1.11 (3.10) Outsourcing		
	G 1.10	Ausfall eines Weitverkehrsnetzes
	G 2.1	Fehlende oder unzureichende Regelungen
	G 2.7	Unerlaubte Ausübung von Rechten
	G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
	G 2.47	Ungesicherter Akten- und Datenträgertransport
	G 2.66	Unzureichendes IT-Sicherheitsmanagement
	G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten
	G 2.83	Fehlerhafte Outsourcing-Strategie
	G 2.84	Unzulängliche vertragliche Regelungen mit einem externen Dienstleister
	G 2.85	Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens
	G 2.86	Abhängigkeit von einem Outsourcing-Dienstleister
	G 2.88	Störung des Betriebsklimas durch ein Outsourcing-Vorhaben
	G 2.89	Mangelhafte IT-Sicherheit in der Outsourcing-Einführungsphase
	G 2.90	Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister
	G 2.93	Unzureichendes Notfallvorsorgekonzept beim Outsourcing
	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
	G 4.33	Schlechte oder fehlende Authentikation
	G 4.34	Ausfall eines Kryptomoduls
	G 4.48	Ausfall der Systeme eines Outsourcing-Dienstleisters
	G 5.10	Missbrauch von Fernwartungszugängen
	G 5.20	Missbrauch von Administratorrechten
	G 5.42	Social Engineering
	G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
	G 5.85	Integritätsverlust schützenswerter Informationen
	G 5.107	Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister

B 1.12 (9.5) Archivierung

G 1.2	Ausfall des IT-Systems
G 1.7	Unzulässige Temperatur und Luftfeuchte
G 1.9	Datenverlust durch starke Magnetfelder
G 1.14	Datenverlust durch starkes Licht
G 2.7	Unerlaubte Ausübung von Rechten
G 2.72	Unzureichende Migration von Archivsystemen
G 2.73	Fehlende Revisionsmöglichkeit von Archivsystemen
G 2.74	Unzureichende Ordnungskriterien für Archive
G 2.75	Mangelnde Kapazität von Archivdatenträgern
G 2.76	Unzureichende Dokumentation von Archivzugriffen
G 2.77	Unzulängliche Übertragung von Papierdaten in elektronische Archive
G 2.78	Unzulängliche Auffrischung von Datenbeständen bei der Archivierung
G 2.79	Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung
G 2.80	Unzureichende Durchführung von Revisionen bei der Archivierung
G 2.81	Unzureichende Vernichtung von Datenträgern bei der Archivierung
G 2.82	Fehlerhafte Planung des Aufstellungsortes von Archivsystemen
G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten
G 3.35	Server im laufenden Betrieb ausschalten
G 3.54	Verwendung ungeeigneter Datenträger bei der Archivierung
G 3.55	Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen
G 4.7	Defekte Datenträger
G 4.13	Verlust gespeicherter Daten
G 4.20	Datenverlust bei erschöpftem Speichermedium
G 4.26	Ausfall einer Datenbank
G 4.30	Verlust der Datenbankintegrität/-konsistenz
G 4.31	Ausfall oder Störung von Netzkomponenten
G 4.45	Verzögerte Archivauskunft
G 4.46	Fehlerhafte Synchronisierung von Indexdaten bei der Archivierung
G 4.47	Veralten von Kryptoverfahren
G 5.2	Manipulation an Daten oder Software
G 5.6	Anschlag
G 5.29	Unberechtigtes Kopieren der Datenträger
G 5.82	Manipulation eines Kryptomoduls
G 5.83	Kompromittierung kryptographischer Schlüssel
G 5.85	Integritätsverlust schützenswerter Informationen
G 5.102	Sabotage
G 5.105	Verhinderung der Dienste von Archivsystemen
G 5.106	Unberechtigtes Überschreiben oder Löschen von Archivmedien

B 1.13 (neu) IT-Sicherheitssensibilisierung und -schulung

			G 2.2	Unzureichende Kenntnis über Regelungen
			G 2.7	Unerlaubte Ausübung von Rechten
			G 2.102	Unzureichende Sensibilisierung für IT-Sicherheit
			G 2.103	Unzureichende Schulung der Mitarbeiter
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.8	Fehlerhafte Nutzung des IT-Systems
			G 3.9	Fehlerhafte Administration des IT-Systems
			G 3.44	Sorglosigkeit im Umgang mit Informationen
			G 3.77	Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahmen
			G 5.2	Manipulation an Daten oder Software
			G 5.9	Unberechtigte IT-Nutzung
			G 5.19	Missbrauch von Benutzerrechten
			G 5.20	Missbrauch von Administratorrechten
			G 5.42	Social Engineering
			G 5.104	Ausspähen von Informationen
B 2.1	(4.1)	Gebäude		
			G 1.3	Blitz
			G 1.4	Feuer
			G 1.5	Wasser
			G 2.1	Fehlende oder unzureichende Regelungen
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen
			G 4.1	Ausfall der Stromversorgung
			G 4.2	Ausfall interner Versorgungsnetze
			G 4.3	Ausfall vorhandener Sicherungseinrichtungen
			G 5.3	Unbefugtes Eindringen in ein Gebäude
			G 5.4	Diebstahl
			G 5.5	Vandalismus
			G 5.6	Anschlag
B 2.2	(4.2)	Verkabelung		
			G 1.6	Kabelbrand
			G 2.11	Unzureichende Trassendimensionierung
			G 2.12	Unzureichende Dokumentation der Verkabelung
			G 2.13	Unzureichend geschützte Verteiler
			G 2.32	Unzureichende Leitungskapazitäten
			G 3.4	Unzulässige Kabelverbindungen
			G 3.5	Unbeabsichtigte Leitungsbeschädigung
			G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktoren
			G 4.5	Übersprechen
			G 4.21	Ausgleichsströme auf Schirmungen
			G 5.7	Abhören von Leitungen

			G 5.8 Manipulation an Leitungen
B 2.3	(4.3.1)	Büroraum	
			G 2.1 Fehlende oder unzureichende Regelungen
			G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen
			G 2.14 Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
			G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
			G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.2 Manipulation an Daten oder Software
			G 5.4 Diebstahl
			G 5.5 Vandalismus
B 2.4	(4.3.2)	Serverraum	
			G 1.4 Feuer
			G 1.5 Wasser
			G 1.7 Unzulässige Temperatur und Luftfeuchte
			G 1.16 Ausfall von Patchfeldern durch Brand
			G 2.1 Fehlende oder unzureichende Regelungen
			G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen
			G 4.1 Ausfall der Stromversorgung
			G 4.2 Ausfall interner Versorgungsnetze
			G 4.6 Spannungsschwankungen/Überspannung/Unterspannung
			G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.2 Manipulation an Daten oder Software
			G 5.3 Unbefugtes Eindringen in ein Gebäude
			G 5.4 Diebstahl
			G 5.5 Vandalismus
B 2.5	(4.3.3)	Datenträgerarchiv	
			G 1.4 Feuer
			G 1.5 Wasser
			G 1.7 Unzulässige Temperatur und Luftfeuchte
			G 1.8 Staub, Verschmutzung
			G 2.1 Fehlende oder unzureichende Regelungen
			G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen
			G 5.3 Unbefugtes Eindringen in ein Gebäude
			G 5.4 Diebstahl
			G 5.5 Vandalismus
B 2.6	(4.3.4)	Raum für technische Infrastruktur	
			G 1.4 Feuer
			G 1.5 Wasser
			G 1.7 Unzulässige Temperatur und Luftfeuchte
			G 2.1 Fehlende oder unzureichende Regelungen
			G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen

			G 4.1	Ausfall der Stromversorgung
			G 4.2	Ausfall interner Versorgungsnetze
			G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.3	Unbefugtes Eindringen in ein Gebäude
			G 5.4	Diebstahl
			G 5.5	Vandalismus
B 2.7	(4.4)	Schutzschrank		
			G 1.4	Feuer
			G 1.5	Wasser
			G 1.7	Unzulässige Temperatur und Luftfeuchte
			G 1.8	Staub, Verschmutzung
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
			G 3.21	Fehlbedienung von Codeschlössern
			G 4.1	Ausfall der Stromversorgung
			G 4.2	Ausfall interner Versorgungsnetze
			G 4.3	Ausfall vorhandener Sicherungseinrichtungen
			G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktoren
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.4	Diebstahl
			G 5.5	Vandalismus
			G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
			G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
			G 5.53	Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit
B 2.8	(4.5)	Häuslicher Arbeitsplatz		
			G 1.5	Wasser
			G 2.1	Fehlende oder unzureichende Regelungen
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen
			G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
			G 2.47	Ungesicherter Akten- und Datenträgertransport
			G 2.48	Ungeeignete Entsorgung der Datenträger und Dokumente
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.2	Manipulation an Daten oder Software
			G 5.3	Unbefugtes Eindringen in ein Gebäude
			G 5.69	Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz
			G 5.70	Manipulation durch Familienangehörige und Besucher
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
B 2.9	(4.6)	Rechenzentrum		
			G 1.2	Ausfall des IT-Systems
			G 1.3	Blitz

			G 1.4	Feuer
			G 1.5	Wasser
			G 1.6	Kabelbrand
			G 1.7	Unzulässige Temperatur und Luftfeuchte
			G 1.8	Staub, Verschmutzung
			G 1.11	Technische Katastrophen im Umfeld
			G 1.12	Beeinträchtigung durch Großveranstaltungen
			G 1.13	Sturm
			G 1.16	Ausfall von Patchfeldern durch Brand
			G 2.1	Fehlende oder unzureichende Regelungen
			G 2.2	Unzureichende Kenntnis über Regelungen
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen
			G 2.11	Unzureichende Trassendimensionierung
			G 2.12	Unzureichende Dokumentation der Verkabelung
			G 4.1	Ausfall der Stromversorgung
			G 4.2	Ausfall interner Versorgungsnetze
			G 4.3	Ausfall vorhandener Sicherungseinrichtungen
			G 5.3	Unbefugtes Eindringen in ein Gebäude
			G 5.4	Diebstahl
			G 5.5	Vandalismus
			G 5.6	Anschlag
			G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
			G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
			G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
			G 5.102	Sabotage
B 2.10	(neu)	Mobiler Arbeitsplatz		
			G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebung
			G 2.1	Fehlende oder unzureichende Regelungen
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
			G 2.47	Ungesicherter Akten- und Datenträgertransport
			G 2.48	Ungeeignete Entsorgung der Datenträger und Dokumente
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.43	Ungeeigneter Umgang mit Passwörtern
			G 3.44	Sorglosigkeit im Umgang mit Informationen
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.2	Manipulation an Daten oder Software
			G 5.4	Diebstahl
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
B 2.11	(neu)	Besprechungs-, Veranstaltungs- und Schulungsräume		

		G 2.1	Fehlende oder unzureichende Regelungen
		G 2.2	Unzureichende Kenntnis über Regelungen
		G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
		G 2.104	Inkompatibilität zwischen fremder und eigener IT
		G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
		G 3.78	Fliegende Verkabelung
		G 4.1	Ausfall der Stromversorgung
		G 4.2	Ausfall interner Versorgungsnetze
		G 5.4	Diebstahl
B 3.101	(6.1)	Allgemeiner Server	
		G 1.1	Personalausfall
		G 1.2	Ausfall des IT-Systems
		G 2.7	Unerlaubte Ausübung von Rechten
		G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
		G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten
		G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
		G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
		G 3.5	Unbeabsichtigte Leitungsbeschädigung
		G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
		G 3.8	Fehlerhafte Nutzung des IT-Systems
		G 3.9	Fehlerhafte Administration des IT-Systems
		G 3.31	Unstrukturierte Datenhaltung
		G 4.1	Ausfall der Stromversorgung
		G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
		G 4.7	Defekte Datenträger
		G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
		G 4.13	Verlust gespeicherter Daten
		G 4.22	Software-Schwachstellen oder -Fehler
		G 4.39	Software-Konzeptionsfehler
		G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
		G 5.2	Manipulation an Daten oder Software
		G 5.7	Abhören von Leitungen
		G 5.9	Unberechtigte IT-Nutzung
		G 5.15	"Neugierige" Mitarbeiter
		G 5.18	Systematisches Ausprobieren von Passwörtern
		G 5.19	Missbrauch von Benutzerrechten
		G 5.20	Missbrauch von Administratorrechten
		G 5.21	Trojanische Pferde
		G 5.23	Computer-Viren
		G 5.26	Analyse des Nachrichtenflusses
		G 5.40	Abhören von Räumen mittels Rechner mit Mikrofon

			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
			G 5.85	Integritätsverlust schützenswerter Informationen
B 3.102	(6.2)	Server unter Unix		
			G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
			G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz
			G 2.65	Komplexität der SAMBA-Konfiguration
			G 3.10	Falsches Exportieren von Dateisystemen unter Unix
			G 3.11	Fehlerhafte Konfiguration von sendmail
			G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client
			G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client
			G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			G 5.89	Hijacking von Netz-Verbindungen
B 3.103	(6.4)	Server unter Windows NT		
			G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz
			G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten
			G 2.30	Unzureichende Domänenplanung
			G 2.31	Unzureichender Schutz des Windows NT Systems
			G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
			G 4.23	Automatische CD-ROM-Erkennung
			G 5.23	Computer-Viren
			G 5.43	Makro-Viren
			G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
			G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
B 3.104	(6.5)	Server unter Novell Netware 3.x		
			G 1.2	Ausfall des IT-Systems
			G 2.33	Nicht gesicherter Aufstellungsort von Novell Netware Servern
			G 2.34	Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen
			G 4.1	Ausfall der Stromversorgung
			G 5.23	Computer-Viren
			G 5.43	Makro-Viren
			G 5.54	Vorsätzliches Herbeiführen eines Abnormal End
			G 5.55	Login Bypass
			G 5.56	Temporär frei zugängliche Accounts
			G 5.57	Netzanalyse-Tools
			G 5.58	"Hacking Novell Netware"
			G 5.59	Missbrauch von Administratorrechten unter Novell Netware 3.x
B 3.105	(6.6)	Server unter Novell Netware 4.x		
			G 1.2	Ausfall des IT-Systems
			G 2.33	Nicht gesicherter Aufstellungsort von Novell Netware Servern
			G 2.34	Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen
			G 2.42	Komplexität der NDS

		G 2.43	Migration von Novell Netware 3.x nach Novell Netware Version 4
		G 3.8	Fehlerhafte Nutzung des IT-Systems
		G 3.25	Fahrlässiges Löschen von Objekten
		G 3.26	Ungewollte Freigabe des Dateisystems
		G 3.27	Fehlerhafte Zeitsynchronisation
		G 3.38	Konfigurations- und Bedienungsfehler
		G 5.23	Computer-Viren
		G 5.43	Makro-Viren
		G 5.55	Login Bypass
		G 5.56	Temporär frei zugängliche Accounts
		G 5.57	Netzanalyse-Tools
		G 5.58	"Hacking Novell Netware"
		G 5.59	Missbrauch von Administratorrechten unter Novell Netware 3.x
B 3.106	(6.9)	Server unter Windows 2000	
		G 1.2	Ausfall des IT-Systems
		G 2.1	Fehlende oder unzureichende Regelungen
		G 2.2	Unzureichende Kenntnis über Regelungen
		G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
		G 2.7	Unerlaubte Ausübung von Rechten
		G 2.18	Ungeordnete Zustellung der Datenträger
		G 2.68	Fehlende oder unzureichende Planung des Active Directory
		G 3.9	Fehlerhafte Administration des IT-Systems
		G 3.48	Fehlkonfiguration von Windows 2000/XP Rechnern
		G 3.49	Fehlkonfiguration des Active Directory
		G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
		G 4.23	Automatische CD-ROM-Erkennung
		G 4.35	Unsichere kryptographische Algorithmen
		G 5.7	Abhören von Leitungen
		G 5.23	Computer-Viren
		G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
		G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
		G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
		G 5.83	Kompromittierung kryptographischer Schlüssel
		G 5.84	Gefälschte Zertifikate
		G 5.85	Integritätsverlust schützenswerter Informationen
B 3.107	(6.10)	S/390- und zSeries-Mainframe	
		G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
		G 2.27	Fehlende oder unzureichende Dokumentation
		G 2.54	Vertraulichkeitsverlust durch Restinformationen
		G 2.99	Unzureichende oder fehlerhafte Konfiguration der zSeries-Systemumgebung
		G 3.2	Fahrlässige Zerstörung von Gerät oder Daten

	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
	G 3.9	Fehlerhafte Administration des IT-Systems
	G 3.38	Konfigurations- und Bedienungsfehler
	G 3.66	Fehlerhafte Zeichensatzkonvertierung beim Einsatz von z/OS
	G 3.67	Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems
	G 3.68	Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers
	G 3.69	Fehlerhafte Konfiguration der Unix System Services unter z/OS
	G 3.70	Unzureichender Dateischutz des z/OS-Systems
	G 3.71	Fehlerhafte Systemzeit bei z/OS-Systemen
	G 3.72	Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF
	G 3.73	Fehlbedienung der z/OS-Systemfunktionen
	G 3.74	Unzureichender Schutz der z/OS-Systemeinstellungen vor dynamischen Änderungen
	G 3.75	Mangelhafte Kontrolle der Batch-Jobs bei z/OS
	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
	G 4.22	Software-Schwachstellen oder -Fehler
	G 4.50	Überlastung des z/OS-Betriebssystems
	G 5.2	Manipulation an Daten oder Software
	G 5.10	Missbrauch von Fernwartungszugängen
	G 5.18	Systematisches Ausprobieren von Passwörtern
	G 5.19	Missbrauch von Benutzerrechten
	G 5.21	Trojanische Pferde
	G 5.28	Verhinderung von Diensten
	G 5.57	Netzanalyse-Tools
	G 5.116	Manipulation der z/OS-Systemsteuerung
	G 5.117	Verschleiern von Manipulationen unter z/OS
	G 5.118	Unbefugtes Erlangen höherer Rechte im RACF
	G 5.119	Benutzung fremder Kennungen unter z/OS-Systemen
	G 5.120	Manipulation der Linux/zSeries Systemsteuerung
	G 5.121	Angriffe über TCP/IP auf z/OS-Systeme
	G 5.122	Missbrauch von RACF-Attributen unter z/OS
B 3.201 (neu) Allgemeiner Client		
	G 1.1	Personalausfall
	G 2.1	Fehlende oder unzureichende Regelungen
	G 2.7	Unerlaubte Ausübung von Rechten
	G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern
	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
	G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten
	G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen
	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
	G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
	G 3.8	Fehlerhafte Nutzung des IT-Systems

	G 3.9	Fehlerhafte Administration des IT-Systems
	G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel
	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
	G 4.13	Verlust gespeicherter Daten
	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
	G 5.2	Manipulation an Daten oder Software
	G 5.4	Diebstahl
	G 5.7	Abhören von Leitungen
	G 5.9	Unberechtigte IT-Nutzung
	G 5.20	Missbrauch von Administratorrechten
	G 5.21	Trojanische Pferde
	G 5.23	Computer-Viren
	G 5.40	Abhören von Räumen mittels Rechner mit Mikrofon
	G 5.43	Makro-Viren
	G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
	G 5.85	Integritätsverlust schützenswerter Informationen

B 3.202 (5.99) Allgemeines nicht vernetztes IT-System

G 1.1	Personalausfall
G 1.2	Ausfall des IT-Systems
G 1.4	Feuer
G 1.5	Wasser
G 1.8	Staub, Verschmutzung
G 2.1	Fehlende oder unzureichende Regelungen
G 2.7	Unerlaubte Ausübung von Rechten
G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern
G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
G 3.8	Fehlerhafte Nutzung des IT-Systems
G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten
G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel
G 4.1	Ausfall der Stromversorgung
G 4.7	Defekte Datenträger
G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
G 5.2	Manipulation an Daten oder Software
G 5.4	Diebstahl
G 5.9	Unberechtigte IT-Nutzung
G 5.18	Systematisches Ausprobieren von Passwörtern
G 5.19	Missbrauch von Benutzerrechten
G 5.20	Missbrauch von Administratorrechten
G 5.21	Trojanische Pferde

			G 5.23	Computer-Viren
			G 5.40	Abhören von Räumen mittels Rechner mit Mikrofon
			G 5.43	Makro-Viren
B 3.203	(5.3)	Laptop		
			G 1.2	Ausfall des IT-Systems
			G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebung
			G 2.7	Unerlaubte Ausübung von Rechten
			G 2.8	Unkontrollierter Einsatz von Betriebsmitteln
			G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PCs
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
			G 3.8	Fehlerhafte Nutzung des IT-Systems
			G 3.38	Konfigurations- und Bedienungsfehler
			G 3.76	Fehler bei der Synchronisation mobiler Endgeräte
			G 4.9	Ausfall der internen Stromversorgung
			G 4.13	Verlust gespeicherter Daten
			G 4.19	Informationsverlust bei erschöpftem Speichermedium
			G 4.22	Software-Schwachstellen oder -Fehler
			G 4.52	Datenverlust bei mobilem Einsatz
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.2	Manipulation an Daten oder Software
			G 5.4	Diebstahl
			G 5.9	Unberechtigte IT-Nutzung
			G 5.18	Systematisches Ausprobieren von Passwörtern
			G 5.21	Trojanische Pferde
			G 5.22	Diebstahl bei mobiler Nutzung des IT-Systems
			G 5.23	Computer-Viren
			G 5.43	Makro-Viren
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
			G 5.123	Abhören von Raumgesprächen über mobile Endgeräte
			G 5.124	Missbrauch der Informationen von mobilen Endgeräten
			G 5.125	Unberechtigte Datenweitergabe über mobile Endgeräte
			G 5.126	Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten
B 3.204	(5.2)	Client unter Unix		
			G 1.1	Personalausfall
			G 1.2	Ausfall des IT-Systems
			G 1.8	Staub, Verschmutzung
			G 2.7	Unerlaubte Ausübung von Rechten
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System

	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
	G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
	G 3.8	Fehlerhafte Nutzung des IT-Systems
	G 3.9	Fehlerhafte Administration des IT-Systems
	G 4.8	Bekanntwerden von Softwareschwachstellen
	G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client
	G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client
	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
	G 5.2	Manipulation an Daten oder Software
	G 5.4	Diebstahl
	G 5.7	Abhören von Leitungen
	G 5.8	Manipulation an Leitungen
	G 5.9	Unberechtigte IT-Nutzung
	G 5.18	Systematisches Ausprobieren von Passwörtern
	G 5.19	Missbrauch von Benutzerrechten
	G 5.20	Missbrauch von Administratorrechten
	G 5.21	Trojanische Pferde
	G 5.23	Computer-Viren
	G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
	G 5.89	Hijacking von Netz-Verbindungen
B 3.205 (5.5) Client unter Windows NT		
	G 1.1	Personalausfall
	G 1.2	Ausfall des IT-Systems
	G 2.7	Unerlaubte Ausübung von Rechten
	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
	G 2.31	Unzureichender Schutz des Windows NT Systems
	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
	G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
	G 3.8	Fehlerhafte Nutzung des IT-Systems
	G 3.9	Fehlerhafte Administration des IT-Systems
	G 4.1	Ausfall der Stromversorgung
	G 4.7	Defekte Datenträger
	G 4.23	Automatische CD-ROM-Erkennung
	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
	G 5.2	Manipulation an Daten oder Software
	G 5.4	Diebstahl
	G 5.9	Unberechtigte IT-Nutzung
	G 5.21	Trojanische Pferde
	G 5.23	Computer-Viren

			G 5.43	Makro-Viren
			G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
			G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
B 3.206	(5.6)	Client unter Windows 95		
			G 1.2	Ausfall des IT-Systems
			G 1.4	Feuer
			G 1.5	Wasser
			G 1.8	Staub, Verschmutzung
			G 2.1	Fehlende oder unzureichende Regelungen
			G 2.7	Unerlaubte Ausübung von Rechten
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern
			G 2.22	Fehlende Auswertung von Protokolldaten
			G 2.35	Fehlende Protokollierung unter Windows 95
			G 2.36	Ungeeignete Einschränkung der Benutzerumgebung
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
			G 3.8	Fehlerhafte Nutzung des IT-Systems
			G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten
			G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel
			G 3.22	Fehlerhafte Änderung der Registrierung
			G 4.23	Automatische CD-ROM-Erkennung
			G 4.24	Dateinamenkonvertierung bei Datensicherungen unter Windows 95
			G 5.2	Manipulation an Daten oder Software
			G 5.4	Diebstahl
			G 5.9	Unberechtigte IT-Nutzung
			G 5.21	Trojanische Pferde
			G 5.23	Computer-Viren
			G 5.43	Makro-Viren
			G 5.60	Umgehen der Systemrichtlinien
B 3.207	(5.7)	Client unter Windows 2000		
			G 1.1	Personalausfall
			G 1.2	Ausfall des IT-Systems
			G 1.4	Feuer
			G 1.5	Wasser
			G 1.8	Staub, Verschmutzung
			G 2.7	Unerlaubte Ausübung von Rechten
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen

			G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
			G 3.8 Fehlerhafte Nutzung des IT-Systems
			G 3.9 Fehlerhafte Administration des IT-Systems
			G 4.1 Ausfall der Stromversorgung
			G 4.7 Defekte Datenträger
			G 4.8 Bekanntwerden von Softwareschwachstellen
			G 4.23 Automatische CD-ROM-Erkennung
			G 5.2 Manipulation an Daten oder Software
			G 5.4 Diebstahl
			G 5.9 Unberechtigte IT-Nutzung
			G 5.18 Systematisches Ausprobieren von Passwörtern
			G 5.21 Trojanische Pferde
			G 5.23 Computer-Viren
			G 5.43 Makro-Viren
			G 5.52 Missbrauch von Administratorrechten im Windows NT/2000/XP System
			G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
			G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			G 5.85 Integritätsverlust schützenswerter Informationen
B 3.208	(5.8)	Internet-PC	
			G 1.2 Ausfall des IT-Systems
			G 2.1 Fehlende oder unzureichende Regelungen
			G 2.2 Unzureichende Kenntnis über Regelungen
			G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern
			G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
			G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.9 Fehlerhafte Administration des IT-Systems
			G 3.38 Konfigurations- und Bedienungsfehler
			G 4.22 Software-Schwachstellen oder -Fehler
			G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.2 Manipulation an Daten oder Software
			G 5.21 Trojanische Pferde
			G 5.23 Computer-Viren
			G 5.43 Makro-Viren
			G 5.48 IP-Spoofing
			G 5.78 DNS-Spoofing
			G 5.87 Web-Spoofing
			G 5.88 Missbrauch aktiver Inhalte
			G 5.91 Abschalten von Sicherheitsmechanismen für den RAS-Zugang
			G 5.103 Missbrauch von Webmail
B 3.209	(neu)	Client unter Windows XP	
			G 1.2 Ausfall des IT-Systems

		G 1.4	Feuer
		G 1.5	Wasser
		G 1.8	Staub, Verschmutzung
		G 2.7	Unerlaubte Ausübung von Rechten
		G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
		G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
		G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
		G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
		G 3.8	Fehlerhafte Nutzung des IT-Systems
		G 3.9	Fehlerhafte Administration des IT-Systems
		G 3.22	Fehlerhafte Änderung der Registrierung
		G 3.48	Fehlkonfiguration von Windows 2000/XP Rechnern
		G 4.1	Ausfall der Stromversorgung
		G 4.7	Defekte Datenträger
		G 4.8	Bekanntwerden von Softwareschwachstellen
		G 4.23	Automatische CD-ROM-Erkennung
		G 5.2	Manipulation an Daten oder Software
		G 5.4	Diebstahl
		G 5.7	Abhören von Leitungen
		G 5.9	Unberechtigte IT-Nutzung
		G 5.18	Systematisches Ausprobieren von Passwörtern
		G 5.21	Trojanische Pferde
		G 5.23	Computer-Viren
		G 5.43	Makro-Viren
		G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
		G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
		G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
		G 5.83	Kompromittierung kryptographischer Schlüssel
		G 5.85	Integritätsverlust schützenswerter Informationen
B 3.301	(7.3)	Sicherheitsgateway (Firewall)	
		G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
		G 2.101	Unzureichende Notfallvorsorge bei einem Sicherheitsgateway
		G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
		G 3.9	Fehlerhafte Administration des IT-Systems
		G 3.38	Konfigurations- und Bedienungsfehler
		G 4.8	Bekanntwerden von Softwareschwachstellen
		G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
		G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client
		G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client
		G 4.20	Datenverlust bei erschöpftem Speichermedium
		G 4.22	Software-Schwachstellen oder -Fehler

			G 4.39	Software-Konzeptionsfehler
			G 5.2	Manipulation an Daten oder Software
			G 5.9	Unberechtigte IT-Nutzung
			G 5.18	Systematisches Ausprobieren von Passwörtern
			G 5.24	Wiedereinspielen von Nachrichten
			G 5.25	Maskerade
			G 5.28	Verhinderung von Diensten
			G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten
			G 5.48	IP-Spoofing
			G 5.49	Missbrauch des Source-Routing
			G 5.50	Missbrauch des ICMP-Protokolls
			G 5.51	Missbrauch der Routing-Protokolle
			G 5.78	DNS-Spoofing
B 3.302	(7.11)	Router und Switches		
			G 2.1	Fehlende oder unzureichende Regelungen
			G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
			G 2.22	Fehlende Auswertung von Protokolldaten
			G 2.27	Fehlende oder unzureichende Dokumentation
			G 2.44	Inkompatible aktive und passive Netzkomponenten
			G 2.54	Vertraulichkeitsverlust durch Restinformationen
			G 2.98	Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switches
			G 3.64	Fehlerhafte Konfiguration von Routern und Switches
			G 3.65	Fehlerhafte Administration von Routern und Switches
			G 4.8	Bekanntwerden von Softwareschwachstellen
			G 4.49	Unsichere Default-Einstellungen auf Routern und Switches
			G 5.4	Diebstahl
			G 5.51	Missbrauch der Routing-Protokolle
			G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
			G 5.112	Manipulation von ARP-Tabellen
			G 5.113	MAC-Spoofing
			G 5.114	Missbrauch von Spanning Tree
			G 5.115	Überwindung der Grenzen zwischen VLANs
B 3.401	(8.1)	TK-Anlage		
			G 1.4	Feuer
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
			G 3.7	Ausfall der TK-Anlage durch Fehlbedienung
			G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten

			G 5.12	Abhören von Telefongesprächen und Datenübertragungen
			G 5.13	Abhören von Räumen
			G 5.14	Gebührenbetrug
			G 5.15	"Neugierige" Mitarbeiter
			G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
			G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
			G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlagen
B 3.402	(8.2)	Faxgerät		
			G 2.20	Unzureichende oder falsche Versorgung mit Verbrauchsgütern
			G 3.14	Fehleinschätzung der Rechtsverbindlichkeit eines Fax
			G 4.14	Verblassen spezieller Faxpapiere
			G 4.15	Fehlerhafte Faxübertragung
			G 5.7	Abhören von Leitungen
			G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
			G 5.31	Unbefugtes Lesen von Faxsendungen
			G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxservern
			G 5.33	Vortäuschen eines falschen Absenders bei Faxsendungen
			G 5.34	Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes
			G 5.35	Überlastung durch Faxsendungen
B 3.403	(8.3)	Anrufbeantworter		
			G 2.1	Fehlende oder unzureichende Regelungen
			G 2.5	Fehlende oder unzureichende Wartung
			G 3.15	Fehlbedienung eines Anrufbeantworters
			G 4.1	Ausfall der Stromversorgung
			G 4.18	Entladene oder überalterte Notstromversorgung im Anrufbeantworter
			G 4.19	Informationsverlust bei erschöpftem Speichermedium
			G 5.36	Absichtliche Überlastung des Anrufbeantworters
			G 5.37	Ermitteln des Sicherungscodes
			G 5.38	Missbrauch der Fernabfrage
B 3.404	(8.6)	Mobiltelefon		
			G 2.2	Unzureichende Kenntnis über Regelungen
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
			G 2.7	Unerlaubte Ausübung von Rechten
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.43	Ungeeigneter Umgang mit Passwörtern
			G 3.44	Sorglosigkeit im Umgang mit Informationen
			G 3.45	Unzureichende Identifikationsprüfung von Kommunikationspartnern
			G 4.41	Nicht-Verfügbarkeit des Mobilfunknetzes
			G 4.42	Ausfall des Mobiltelefons oder des PDAs
			G 5.2	Manipulation an Daten oder Software
			G 5.4	Diebstahl

			G 5.80	Hoax
			G 5.94	Kartenmissbrauch
			G 5.95	Abhören von Raumgesprächen über Mobiltelefone
			G 5.96	Manipulation von Mobiltelefonen
			G 5.97	Unberechtigte Datenweitergabe über Mobiltelefone
			G 5.98	Abhören von Mobiltelefonaten
			G 5.99	Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen
			G 5.126	Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten
B 3.405	(8.7)	PDA		
			G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebung
			G 2.2	Unzureichende Kenntnis über Regelungen
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
			G 2.7	Unerlaubte Ausübung von Rechten
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.43	Ungeeigneter Umgang mit Passwörtern
			G 3.44	Sorglosigkeit im Umgang mit Informationen
			G 3.45	Unzureichende Identifikationsprüfung von Kommunikationspartnern
			G 3.76	Fehler bei der Synchronisation mobiler Endgeräte
			G 4.42	Ausfall des Mobiltelefons oder des PDAs
			G 4.51	Unzureichende Sicherheitsmechanismen bei PDAs
			G 4.52	Datenverlust bei mobilem Einsatz
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.2	Manipulation an Daten oder Software
			G 5.9	Unberechtigte IT-Nutzung
			G 5.22	Diebstahl bei mobiler Nutzung des IT-Systems
			G 5.23	Computer-Viren
			G 5.123	Abhören von Raumgesprächen über mobile Endgeräte
			G 5.124	Missbrauch der Informationen von mobilen Endgeräten
			G 5.125	Unberechtigte Datenweitergabe über mobile Endgeräte
			G 5.126	Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten
B 4.1	(6.7)	Heterogene Netze		
			G 1.2	Ausfall des IT-Systems
			G 1.3	Blitz
			G 1.4	Feuer
			G 1.5	Wasser
			G 1.7	Unzulässige Temperatur und Luftfeuchte
			G 1.8	Staub, Verschmutzung
			G 2.7	Unerlaubte Ausübung von Rechten
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			G 2.22	Fehlende Auswertung von Protokolldaten
			G 2.27	Fehlende oder unzureichende Dokumentation

	G 2.32	Unzureichende Leitungskapazitäten
	G 2.44	Inkompatible aktive und passive Netzkomponenten
	G 2.45	Konzeptionelle Schwächen des Netzes
	G 2.46	Überschreiten der zulässigen Kabel- bzw. Buslänge oder der Ringgröße
	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
	G 3.5	Unbeabsichtigte Leitungsbeschädigung
	G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
	G 3.8	Fehlerhafte Nutzung des IT-Systems
	G 3.9	Fehlerhafte Administration des IT-Systems
	G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten
	G 3.29	Fehlende oder ungeeignete Segmentierung
	G 4.1	Ausfall der Stromversorgung
	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
	G 4.31	Ausfall oder Störung von Netzkomponenten
	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
	G 5.2	Manipulation an Daten oder Software
	G 5.4	Diebstahl
	G 5.5	Vandalismus
	G 5.6	Anschlag
	G 5.7	Abhören von Leitungen
	G 5.8	Manipulation an Leitungen
	G 5.9	Unberechtigte IT-Nutzung
	G 5.18	Systematisches Ausprobieren von Passwörtern
	G 5.20	Missbrauch von Administratorrechten
	G 5.28	Verhinderung von Diensten
	G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
	G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen
	G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
B 4.2 (6.8) Netz- und Systemmanagement		
	G 1.1	Personalausfall
	G 1.2	Ausfall des IT-Systems
	G 1.7	Unzulässige Temperatur und Luftfeuchte
	G 2.27	Fehlende oder unzureichende Dokumentation
	G 2.32	Unzureichende Leitungskapazitäten
	G 2.59	Betreiben von nicht angemeldeten Komponenten
	G 2.60	Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement
	G 2.61	Unberechtigte Sammlung personenbezogener Daten
	G 3.9	Fehlerhafte Administration des IT-Systems
	G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten
	G 3.34	Ungeeignete Konfiguration des Managementsystems

			G 3.35	Server im laufenden Betrieb ausschalten
			G 3.36	Fehlinterpretation von Ereignissen
			G 4.31	Ausfall oder Störung von Netzkomponenten
			G 4.38	Ausfall von Komponenten eines Netz- und Systemmanagementsystems
			G 5.2	Manipulation an Daten oder Software
			G 5.8	Manipulation an Leitungen
			G 5.9	Unberechtigte IT-Nutzung
			G 5.18	Systematisches Ausprobieren von Passwörtern
			G 5.28	Verhinderung von Diensten
			G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
			G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen
			G 5.86	Manipulation von Managementparametern
B 4.3	(7.2)	Modem		
			G 1.2	Ausfall des IT-Systems
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.5	Unbeabsichtigte Leitungsbeschädigung
			G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
			G 5.2	Manipulation an Daten oder Software
			G 5.7	Abhören von Leitungen
			G 5.8	Manipulation an Leitungen
			G 5.9	Unberechtigte IT-Nutzung
			G 5.10	Missbrauch von Fernwartungszugängen
			G 5.12	Abhören von Telefongesprächen und Datenübertragungen
			G 5.18	Systematisches Ausprobieren von Passwörtern
			G 5.23	Computer-Viren
			G 5.25	Maskerade
			G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten
B 4.4	(7.6)	Remote Access		
			G 1.2	Ausfall des IT-Systems
			G 2.2	Unzureichende Kenntnis über Regelungen
			G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PCs
			G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung
			G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen
			G 2.44	Inkompatible aktive und passive Netzkomponenten
			G 2.64	Fehlende Regelungen für das RAS-System
			G 3.39	Fehlerhafte Administration des RAS-Systems
			G 3.40	Ungeeignete Nutzung von Authentisierungsdiensten bei Remote Access
			G 3.41	Fehlverhalten bei der Nutzung von RAS-Diensten
			G 3.42	Unsichere Konfiguration der RAS-Clients
			G 3.43	Ungeeigneter Umgang mit Passwörtern

		G 3.44	Sorglosigkeit im Umgang mit Informationen
		G 4.35	Unsichere kryptographische Algorithmen
		G 4.40	Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients
		G 5.7	Abhören von Leitungen
		G 5.8	Manipulation an Leitungen
		G 5.22	Diebstahl bei mobiler Nutzung des IT-Systems
		G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten
		G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
		G 5.83	Kompromittierung kryptographischer Schlüssel
		G 5.91	Abschalten von Sicherheitsmechanismen für den RAS-Zugang
		G 5.92	Nutzung des RAS-Clients als RAS-Server
		G 5.93	Erlauben von Fremdnutzung von RAS-Komponenten
B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN	
		G 1.2	Ausfall des IT-Systems
		G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen
		G 2.7	Unerlaubte Ausübung von Rechten
		G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
		G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung
		G 2.22	Fehlende Auswertung von Protokolldaten
		G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
		G 2.32	Unzureichende Leitungskapazitäten
		G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen
		G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
		G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
		G 3.8	Fehlerhafte Nutzung des IT-Systems
		G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
		G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten
		G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
		G 4.25	Nicht getrennte Verbindungen
		G 5.2	Manipulation an Daten oder Software
		G 5.7	Abhören von Leitungen
		G 5.8	Manipulation an Leitungen
		G 5.9	Unberechtigte IT-Nutzung
		G 5.10	Missbrauch von Fernwartungszugängen
		G 5.14	Gebührenbetrug
		G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
		G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
		G 5.18	Systematisches Ausprobieren von Passwörtern
		G 5.25	Maskerade
		G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten
		G 5.48	IP-Spoofing

			G 5.61	Missbrauch von Remote-Zugängen für Managementfunktionen von Routern
			G 5.62	Missbrauch von Ressourcen über abgesetzte IT-Systeme
			G 5.63	Manipulationen über den ISDN-D-Kanal
B 5.1	(6.3)	Peer-to-Peer-Dienste		
			G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten
			G 2.65	Komplexität der SAMBA-Konfiguration
			G 3.9	Fehlerhafte Administration des IT-Systems
			G 3.18	Freigabe von Verzeichnissen, Druckern oder der Ablagemappe
			G 3.19	Speichern von Passwörtern unter WfW und Windows 95
			G 3.20	Ungewollte Freigabe des Leserechtes bei Schedule+
			G 5.45	Ausprobieren von Passwörtern unter WfW und Windows 95
			G 5.46	Maskerade unter WfW
			G 5.47	Löschen des Post-Office unter WfW
B 5.2	(7.1)	Datenträgeraustausch		
			G 1.7	Unzulässige Temperatur und Luftfeuchte
			G 1.8	Staub, Verschmutzung
			G 1.9	Datenverlust durch starke Magnetfelder
			G 2.1	Fehlende oder unzureichende Regelungen
			G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel
			G 2.10	Nicht fristgerecht verfügbare Datenträger
			G 2.17	Mangelhafte Kennzeichnung der Datenträger
			G 2.18	Ungeordnete Zustellung der Datenträger
			G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.12	Verlust der Datenträger beim Versand
			G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
			G 4.7	Defekte Datenträger
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.2	Manipulation an Daten oder Software
			G 5.4	Diebstahl
			G 5.9	Unberechtigte IT-Nutzung
			G 5.23	Computer-Viren
			G 5.29	Unberechtigtes Kopieren der Datenträger
			G 5.43	Makro-Viren
B 5.3	(7.4)	E-Mail		
			G 2.1	Fehlende oder unzureichende Regelungen
			G 2.7	Unerlaubte Ausübung von Rechten
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung
			G 2.54	Vertraulichkeitsverlust durch Restinformationen

		G 2.55	Ungeordnete E-Mail-Nutzung
		G 2.56	Mangelhafte Beschreibung von Dateien
		G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
		G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
		G 3.8	Fehlerhafte Nutzung des IT-Systems
		G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
		G 4.13	Verlust gespeicherter Daten
		G 4.20	Datenverlust bei erschöpftem Speichermedium
		G 4.32	Nichtzustellung einer Nachricht
		G 4.37	Mangelnde Authentizität und Vertraulichkeit von E-Mail
		G 5.2	Manipulation an Daten oder Software
		G 5.7	Abhören von Leitungen
		G 5.9	Unberechtigte IT-Nutzung
		G 5.21	Trojanische Pferde
		G 5.23	Computer-Viren
		G 5.24	Wiedereinspielen von Nachrichten
		G 5.25	Maskerade
		G 5.26	Analyse des Nachrichtenflusses
		G 5.27	Nichtanerkennung einer Nachricht
		G 5.28	Verhinderung von Diensten
		G 5.43	Makro-Viren
		G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
		G 5.72	Mißbräuchliche E-Mail-Nutzung
		G 5.73	Vortäuschen eines falschen Absenders
		G 5.74	Manipulation von Alias-Dateien oder Verteilerlisten
		G 5.75	Überlastung durch eingehende E-Mails
		G 5.76	Mailbomben
		G 5.77	Mitlesen von E-Mails
		G 5.85	Integritätsverlust schützenswerter Informationen
		G 5.110	Web-Bugs
		G 5.111	Missbrauch aktiver Inhalte in E-Mails
B 5.4	(7.5) Webserver		
		G 2.1	Fehlende oder unzureichende Regelungen
		G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
		G 2.7	Unerlaubte Ausübung von Rechten
		G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
		G 2.28	Verstöße gegen das Urheberrecht
		G 2.32	Unzureichende Leitungskapazitäten
		G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen
		G 2.96	Veraltete oder falsche Informationen in einem Webangebot
		G 2.100	Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen

		G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
		G 3.37	Unproduktive Suchzeiten
		G 3.38	Konfigurations- und Bedienungsfehler
		G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
		G 4.22	Software-Schwachstellen oder -Fehler
		G 4.39	Software-Konzeptionsfehler
		G 5.2	Manipulation an Daten oder Software
		G 5.19	Missbrauch von Benutzerrechten
		G 5.20	Missbrauch von Administratorrechten
		G 5.21	Trojanische Pferde
		G 5.23	Computer-Viren
		G 5.28	Verhinderung von Diensten
		G 5.43	Makro-Viren
		G 5.48	IP-Spoofing
		G 5.78	DNS-Spoofing
		G 5.87	Web-Spoofing
		G 5.88	Missbrauch aktiver Inhalte
B 5.5	(7.7)	Lotus Notes	
		G 1.1	Personalausfall
		G 1.2	Ausfall des IT-Systems
		G 2.1	Fehlende oder unzureichende Regelungen
		G 2.2	Unzureichende Kenntnis über Regelungen
		G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
		G 2.7	Unerlaubte Ausübung von Rechten
		G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PCs
		G 2.18	Ungeordnete Zustellung der Datenträger
		G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung
		G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen
		G 2.40	Komplexität des Datenbankzugangs/-zugriffs
		G 2.49	Fehlende oder unzureichende Schulung der Telearbeiter
		G 3.9	Fehlerhafte Administration des IT-Systems
		G 3.43	Ungeeigneter Umgang mit Passwörtern
		G 3.44	Sorglosigkeit im Umgang mit Informationen
		G 3.46	Fehlkonfiguration eines Lotus Notes Servers
		G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Notes
		G 4.26	Ausfall einer Datenbank
		G 4.28	Verlust von Daten einer Datenbank
		G 4.35	Unsichere kryptographische Algorithmen
		G 5.7	Abhören von Leitungen
		G 5.8	Manipulation an Leitungen
		G 5.22	Diebstahl bei mobiler Nutzung des IT-Systems

			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
			G 5.77	Mitlesen von E-Mails
			G 5.83	Kompromittierung kryptographischer Schlüssel
			G 5.84	Gefälschte Zertifikate
			G 5.85	Integritätsverlust schützenswerter Informationen
			G 5.100	Missbrauch aktiver Inhalte beim Zugriff auf Lotus Notes
			G 5.101	"Hacking Lotus Notes"
B 5.6	(8.5)	Faxserver		
			G 2.7	Unerlaubte Ausübung von Rechten
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			G 2.22	Fehlende Auswertung von Protokolldaten
			G 2.63	Ungeordnete Faxnutzung
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 3.14	Fehleinschätzung der Rechtsverbindlichkeit eines Fax
			G 4.15	Fehlerhafte Faxübertragung
			G 4.20	Datenverlust bei erschöpftem Speichermedium
			G 5.2	Manipulation an Daten oder Software
			G 5.7	Abhören von Leitungen
			G 5.9	Unberechtigte IT-Nutzung
			G 5.24	Wiedereinspielen von Nachrichten
			G 5.25	Maskerade
			G 5.27	Nichtanerkennung einer Nachricht
			G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
			G 5.31	Unbefugtes Lesen von Faxsendungen
			G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxservern
			G 5.33	Vortäuschen eines falschen Absenders bei Faxsendungen
			G 5.35	Überlastung durch Faxsendungen
			G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten
			G 5.90	Manipulation von Adressbüchern und Verteillisten
B 5.7	(9.2)	Datenbanken		
			G 1.1	Personalausfall
			G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel
			G 2.22	Fehlende Auswertung von Protokolldaten
			G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
			G 2.38	Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen
			G 2.39	Komplexität eines DBMS
			G 2.40	Komplexität des Datenbankzugangs/-zugriffs
			G 2.41	Mangelhafte Organisation des Wechsels von Datenbank-Benutzern
			G 2.57	Nicht ausreichende Speichermedien für den Notfall
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
			G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten

		G 3.23	Fehlerhafte Administration eines DBMS
		G 3.24	Unbeabsichtigte Datenmanipulation
		G 4.26	Ausfall einer Datenbank
		G 4.27	Unterlaufen von Zugriffskontrollen über ODBC
		G 4.28	Verlust von Daten einer Datenbank
		G 4.29	Datenverlust einer Datenbank bei erschöpftem Speichermedium
		G 4.30	Verlust der Datenbankintegrität/-konsistenz
		G 5.9	Unberechtigte IT-Nutzung
		G 5.10	Missbrauch von Fernwartungszugängen
		G 5.18	Systematisches Ausprobieren von Passwörtern
		G 5.64	Manipulation an Daten oder Software bei Datenbanksystemen
		G 5.65	Verhinderung der Dienste eines Datenbanksystems
B 5.8	(9.3) Telearbeit		
		G 1.1	Personalausfall
		G 2.1	Fehlende oder unzureichende Regelungen
		G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
		G 2.5	Fehlende oder unzureichende Wartung
		G 2.7	Unerlaubte Ausübung von Rechten
		G 2.22	Fehlende Auswertung von Protokolldaten
		G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
		G 2.49	Fehlende oder unzureichende Schulung der Telearbeiter
		G 2.50	Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter
		G 2.51	Mangelhafte Einbindung des Telearbeiters in den Informationsfluss
		G 2.52	Erhöhte Reaktionszeiten bei IT-Systemausfall
		G 2.53	Unzureichende Vertretungsregelungen für Telearbeit
		G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
		G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
		G 3.9	Fehlerhafte Administration des IT-Systems
		G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
		G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten
		G 3.30	Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners
		G 4.13	Verlust gespeicherter Daten
		G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
		G 5.2	Manipulation an Daten oder Software
		G 5.7	Abhören von Leitungen
		G 5.9	Unberechtigte IT-Nutzung
		G 5.10	Missbrauch von Fernwartungszugängen
		G 5.18	Systematisches Ausprobieren von Passwörtern
		G 5.19	Missbrauch von Benutzerrechten
		G 5.20	Missbrauch von Administratorrechten
		G 5.21	Trojanische Pferde

			G 5.23	Computer-Viren
			G 5.24	Wiedereinspielen von Nachrichten
			G 5.25	Maskerade
			G 5.43	Makro-Viren
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
B 5.9	(9.4)	Novell eDirectory		
			G 1.2	Ausfall des IT-Systems
			G 2.1	Fehlende oder unzureichende Regelungen
			G 2.2	Unzureichende Kenntnis über Regelungen
			G 2.7	Unerlaubte Ausübung von Rechten
			G 2.69	Fehlende oder unzureichende Planung des Einsatzes von Novell eDirectory
			G 2.70	Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Novell eDirectory
			G 2.71	Fehlerhafte oder unzureichende Planung des LDAP-Zugriffs auf Novell eDirectory
			G 3.9	Fehlerhafte Administration des IT-Systems
			G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
			G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten
			G 3.34	Ungeeignete Konfiguration des Managementsystems
			G 3.35	Server im laufenden Betrieb ausschalten
			G 3.36	Fehlinterpretation von Ereignissen
			G 3.38	Konfigurations- und Bedienungsfehler
			G 3.43	Ungeeigneter Umgang mit Passwörtern
			G 3.50	Fehlkonfiguration von Novell eDirectory
			G 3.51	Falsche Vergabe von Zugriffsrechten im Novell eDirectory
			G 3.52	Fehlkonfiguration des Intranet-Clientzugriffs auf Novell eDirectory
			G 3.53	Fehlkonfiguration des LDAP-Zugriffs auf Novell eDirectory
			G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
			G 4.13	Verlust gespeicherter Daten
			G 4.33	Schlechte oder fehlende Authentikation
			G 4.34	Ausfall eines Kryptomoduls
			G 4.44	Ausfall von Novell eDirectory
			G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
			G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
			G 5.18	Systematisches Ausprobieren von Passwörtern
			G 5.19	Missbrauch von Benutzerrechten
			G 5.20	Missbrauch von Administratorrechten
			G 5.65	Verhinderung der Dienste eines Datenbanksystems
			G 5.78	DNS-Spoofing
			G 5.81	Unautorisierte Benutzung eines Kryptomoduls
B 5.10	(7.8)	Internet Information Server		
			G 2.1	Fehlende oder unzureichende Regelungen
			G 2.94	Unzureichende Planung des IIS-Einsatzes

			G 3.56 Fehlerhafte Einbindung des IIS in die Systemumgebung
			G 3.57 Fehlerhafte Konfiguration des Betriebssystems für den IIS
			G 3.58 Fehlkonfiguration eines IIS
			G 3.59 Unzureichende Kenntnisse über aktuelle Sicherheitslücken und Prüfwerkzeuge für den IIS
			G 4.13 Verlust gespeicherter Daten
			G 4.22 Software-Schwachstellen oder -Fehler
			G 4.39 Software-Konzeptionsfehler
			G 5.2 Manipulation an Daten oder Software
			G 5.20 Missbrauch von Administratorrechten
			G 5.28 Verhinderung von Diensten
			G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
			G 5.84 Gefälschte Zertifikate
			G 5.88 Missbrauch aktiver Inhalte
			G 5.108 Ausnutzen von systemspezifischen Schwachstellen des IIS
B 5.11	(7.9)	Apache Webserver	
			G 2.1 Fehlende oder unzureichende Regelungen
			G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			G 2.87 Verwendung unsicherer Protokolle in öffentlichen Netzen
			G 2.97 Unzureichende Notfallplanung bei einem Apache-Webserver
			G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
			G 3.9 Fehlerhafte Administration des IT-Systems
			G 3.38 Konfigurations- und Bedienungsfehler
			G 3.62 Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver
			G 3.63 Fehlerhafte Konfiguration eines Apache-Webservers
			G 4.39 Software-Konzeptionsfehler
			G 5.2 Manipulation an Daten oder Software
			G 5.7 Abhören von Leitungen
			G 5.21 Trojanische Pferde
			G 5.28 Verhinderung von Diensten
			G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
			G 5.85 Integritätsverlust schützenswerter Informationen
			G 5.109 Ausnutzen systemspezifischer Schwachstellen beim Apache-Webserver
B 5.12	(7.10)	Exchange 2000 / Outlook 2000	
			G 1.2 Ausfall des IT-Systems
			G 2.1 Fehlende oder unzureichende Regelungen
			G 2.2 Unzureichende Kenntnis über Regelungen
			G 2.7 Unerlaubte Ausübung von Rechten
			G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen
			G 2.55 Ungeordnete E-Mail-Nutzung
			G 2.91 Fehlerhafte Planung der Migration von Exchange 5.5 nach Exchange 2000
			G 2.92 Fehlerhafte Regelungen für den Browser-Zugriff auf Exchange

G 2.95	Fehlendes Konzept zur Anbindung anderer E-Mail-Systeme an Exchange/Outlook
G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
G 3.9	Fehlerhafte Administration des IT-Systems
G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten
G 3.38	Konfigurations- und Bedienungsfehler
G 3.60	Fehlkonfiguration von Exchange 2000 Servern
G 3.61	Fehlerhafte Konfiguration von Outlook 2000 Clients
G 4.22	Software-Schwachstellen oder -Fehler
G 4.32	Nichtzustellung einer Nachricht
G 5.9	Unberechtigte IT-Nutzung
G 5.19	Missbrauch von Benutzerrechten
G 5.23	Computer-Viren
G 5.77	Mitlesen von E-Mails
G 5.83	Kompromittierung kryptographischer Schlüssel
G 5.84	Gefälschte Zertifikate
G 5.85	Integritätsverlust schützenswerter Informationen