Neu zugeordnete Gefährdungen

Baustein	Alt	Bausteinname	Gefährdung	Gefährdungstitel
B 1.0	(3.0)	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 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 1.2	Ausfall des IT-Systems
			G 2.7	Unerlaubte Ausübung von Rechten
			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 5.20	Missbrauch von Administratorrechten
			G 5.23	Computer-Viren
			G 5.43	Makro-Viren
			G 5.80	Hoax
B 1.6	(3.6)	Computer-Virenschutzkonzept		
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
			G 3.44	Sorglosigkeit im Umgang mit Informationen

			G 4.22	Software-Schwachstellen oder -Fehler
			G 5.127	Spyware
B 1.7	(3.7)	Kryptokonzept		
			G 4.33	Schlechte oder fehlende Authentikation
			G 5.27	Nichtanerkennung einer Nachricht
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
			G 5.85	Integritätsverlust schützenswerter Informationen
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 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen
			G 2.7	Unerlaubte Ausübung von Rechten
			G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
			G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern
			G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz
			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 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 4.31	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 5.9	Unberechtigte IT-Nutzung
			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 2.2 Unzureichende Kenntnis über Regelungen
			G 2.7 Unerlaubte Ausübung von Rechten
			G 2.67 Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten
			G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
			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 5.2 Manipulation an Daten oder Software
			G 5.9 Unberechtigte IT-Nutzung
B 2.4	(4.3.2)	Serverraum	
			G 1.16 Ausfall von Patchfeldern durch Brand
B 2.9	(4.6)	Rechenzentrum	
			G 1.16 Ausfall von Patchfeldern durch Brand
B 3.101	(6.1)	Allgemeiner Server	
			G 2.25 Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten
			G 4.13 Verlust gespeicherter Daten
			G 4.22 Software-Schwachstellen oder -Fehler
			G 4.39 Software-Konzeptionsfehler
			G 5.15 "Neugierige" Mitarbeiter
			G 5.40 Abhören von Räumen mittels Rechner mit Mikrofon
			G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
			G 5.85 Integritätsverlust schützenswerter Informationen
B 3.106	(6.9)	Server unter Windows 2000	
			G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System	
			G 5.40 Abhören von Räumen mittels Rechner mit Mikrofon
B 3.203	(5.3)	Laptop	
			G 1.15 Beeinträchtigung durch wechselnde Einsatzumgebung
			G 3.38 Konfigurations- und Bedienungsfehler
			G 3.76 Fehler bei der Synchronisation mobiler Endgeräte
			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 5.18 Systematisches Ausprobieren von Passwörtern
			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 3.207	(5.7)	Client unter Windows 2000	
			G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
			G 5.85 Integritätsverlust schützenswerter Informationen
B 3.208	(5.8)	Internet-PC	
			G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
			G 5.2 Manipulation an Daten oder Software
B 3.301	(7.3)	Sicherheitsgateway (Firewall)	
			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 2.22 Fehlende Auswertung von Protokolldaten
			G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen
			G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
			G 5.62 Missbrauch von Ressourcen über abgesetzte IT-Systeme
B 3.404	(8.6)	Mobiltelefon	
			G 5.126 Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten
B 4.1	(6.7)	Heterogene Netze	
			G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
			G 5.20 Missbrauch von Administratorrechten
B 4.2	(6.8)	Netz- und Systemmanagement	
			G 1.7 Unzulässige Temperatur und Luftfeuchte
			G 2.27 Fehlende oder unzureichende Dokumentation
			G 2.32 Unzureichende Leitungskapazitäten
			G 3.9 Fehlerhafte Administration des IT-Systems
			G 3.28 Ungeeignete Konfiguration der aktiven Netzkomponenten
			G 4.31 Ausfall oder Störung von Netzkomponenten
			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

B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN
B 5.2	(7.1)	Datenträgeraustausch

G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen
G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
G 2.1	Fehlende oder unzureichende Regelungen