Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS®

Abschnitt 4
MITTEL ZUR BESTIMMUNG DER IT-RISIKEN

Version 2 – 5. Februar 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Dieses Dokument wurde vom Beratungsbüro der DCSSI
(SGDN / DCSSI / SDO / BCS)
in Zusammenarbeit mit dem EBIOS-Club erstellt.

Kommentare und Anmerkungen werden gerne unter Einsendung an folgende Adresse entgegengenommen:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
FRANCE

ebios.dcssi@sgdn.pm.gouv.fr

Änderungsprotokoll

Version	Gegenstand der Änderung	Stand
02/1997 (1.1)	Veröffentlichung des Leitfadens "Formalisierung von Bedürfnissen und Identifizierung von Sicherheitszielen" (EBIOS – Expression des besoins et d'identification des objectifs de sécurité).	Genehmigt
23/01/2004	Generalüberarbeitung: - Erläuterungen und Anpassung an die Internationalen Normen über Sicherheit und Risikomanagement - Hervorhebung der Basisverordnungen zur Unterscheidung von allen übrigen zu berücksichtigenden Anforderungen. - Integrierung der Konzepte "Hypothese" und "Sicherheitsvorschriften" (ISO/IEC 15408) - Übernahme der ausgewählten wesentlichen Elemente in die Zielsystemstudie - Verbesserungen bei der Festlegung der Bedarfsskala: Werte, die von der Organisation, bezogen auf ihre unmittelbaren Auswirkungen, als akzeptable Grenzen eingestuft werden. - Integrierung der für jedes Element formalisierten Bedarfe bezogen auf die nachfolgende Aktivität. - Integrierung der Bestimmung des Betriebsmodus' in die Hypothesen. - Anpassung der Konzepte an ISO/IEC 15408: Analysiert wird der Ursprung der Bedrohungen, d. h. die Angriffsmethoden und die bedrohenden Elemente, sowie deren Charakterisierung nach Art (natürlich bedingt, menschlich bedingt, umgebungsbedingt), Ursache (unbeabsichtigt, vorsätzlich bei weiterer Aufsplitterung nach Exposition, verfügbare Ressourcen, Fachkenntnissen und Motivation) und Angriffspotential. - Hervorhebung der nicht berücksichtigten Angriffsmethoden - Formalisierung der Bedrohungen im Sinne von ISO/IEC 15408 (bedrohendes Element, Angriff und Wert bezogen auf die Entitäten), bevor diese dem Sicherheitsbedarf gegenübergestellt werden. - Änderung bezüglich der Gegenüberstellung von Bedrohungen und Bedürfnissen zur Identifizierung von Risiken - Hervorhebung der nicht berücksichtigten Risiken - Integrierung der Festlegung minimaler Sicherheitsziele für die Aktivitäten "Formalisierung von Sicherheitszielen" und "Bestimmung von funktionellen Anforderungen" - Änderung bezüglich der Festlegung von Sicherheitszielen, bei der die Hypothesen, die aus der Sicherheits-Policy erwachsenen Vorschriften, die Zwänge, Basisverordnungen und Risiken berücksichtigt werden - Hinzufügen der Bestimmung von Sicherheitsniveaus, wodurch das Niveau der Sicherheitsziele bestimmt (z. B. unter Berücksichtigung des Angriffspotentials) und ein Gewährleistungsniveau ausgewählt werden kann. - Hinzufügen der Bestimmung funktioneller Sicherheitsanforderungen; dadurch können funktionelle Anforderungen bezogen auf die Sicherheitsziele bestimmt und diese Entsprechung dargestellt werden - Hinzufügen der Bestimmung von Sicherheitsgewährleistungsanforderungen, mit denen eventuelle Gewährleistungsanforderungen festgelegt werden können. Verbesserungen hinsichtlich Form, Anpassungen und geringfügiger Korrekturen (Grammatik, Rechtschreibung, Formulierungen, Gestaltung, Kohärenz usw.)	vom EBIOS-Club genehmigt
05/02/2004	Veröffentlichung der Version 2 des EBIOS-Leitfadens	Genehmigt

Inhaltsverzeichnis

1 Einleitung

Die EBIOS[1] –Methode besteht aus fünf sich ergänzenden Abschnitten

- Abschnitt 1 - Einführung
  In diesem Abschnitt werden der Kontext, der Nutzen und der Stellenwert der EBIOS-Methodik vorgestellt. Vervollständigt wird dieser Abschnitt durch ein Literaturverzeichnis, ein Glossar und ein Abkürzungsverzeichnis.

- Abschnitt 2 - Methodik
  Dieser Abschnitt beschreibt den Ablauf der verschiedenen Aktivitäten der Methode.

- Abschnitt 3 - Techniken
  In diesem Abschnitt werden Mittel zur Realisierung der Aktivitäten der Methode angeboten. Es ist ratsam, diese Techniken den Anforderungen und Praktiken der jeweiligen Institution anzupassen.

- Abschnitt 4 – Mittel zur IT-Risikobewertung
  Dieser Abschnitt entspricht dem ersten Teil der Grundkenntnisse der EBIOS-Methode (Entitätstypen, Angriffsmethoden, Schwachstellen)

- Abschnitt 5 – Mittel zur Behandlung von IT-Risiken
  Dieser Abschnitt entspricht dem zweiten Teil der Grundkenntnisse der EBIOS-Methode (Sicherheitsziele, Sicherheitsanforderungen, Tabellen zur Festlegung der funktionellen Sicherheitsziele und –anforderungen).

Das vorliegende Dokument entspricht dem vierten Abschnitt der Methode.

Es beinhaltet :
- eine Typologie der Entitätstypen und -untertypen,
- eine Typologie der Angriffsmethoden unter Berücksichtigung der bedrohenden Elemente, die sich diese Methoden zu Nutze machen können,
- eine Schwachstellendatenbank, die nach Angriffsmethoden strukturiert ist und in der die betroffenen Entitätstypen und –untertypen aufgelistet werden.

[1] EBIOS ist eine Schutzmarke des Generalsekretariats der Nationalen Verteidigung in Frankreich.

2 Einheitentypen und untertypen

2.1 MAT : Hardware

MAT: Hardware	
Typ	MAT: Hardware
Beschreibung	Beschreibung: --- Der Einheitentyp "Hardware" umfasst alle physischen Elemente eines Informationssystems. Der Einheitentyp "Hardware" umfasst alle physischen Elemente eines Informationssystems.

2.1.1 MAT_ACT : Datenverarbeitungsmittel (aktiv)

MAT_ACT: Datenverarbeitungsmittel (aktiv)	
Typ	MAT_ACT: Datenverarbeitungsmittel (aktiv)
Beschreibung	Beschreibung: --- Automatische Datenverarbeitungsanlage mit allen notwendigen Organen für einen autonomen Betrieb. Angegliederte Einheitentypen und untertypen: --- MAT: HardwareDer Einheitentyp "Hardware" umfasst alle physischen Elemente eines Informationssystems.

MAT_ACT.1: Tragbare Hardware	
Typ	MAT_ACT.1: Tragbare Hardware
Beschreibung	Beschreibung: --- Datenverarbeitungsanlagen, die von Hand transportiert und an verschiedenen Orten benutzt werden können. Beispiele: --- Laptop, PDA. Angegliederte Einheitentypen und untertypen: --- MAT: Hardware Der Einheitentyp "Hardware" umfasst alle physischen Elemente eines Informationssystems. MAT_ACT: Datenverarbeitungsmittel (aktiv) Automatische Datenverarbeitungsanlage mit allen notwendigen Organen für einen autonomen Betrieb.

MAT_ACT.2: Ortsfeste Hardware	
Typ	MAT_ACT.2: Ortsfeste Hardware
Beschreibung	Beschreibung: --- Datenverarbeitungsanlagen, die der Institution gehören oder die in den Räumen der Institution benutzt werden. Beispiele: --- Server, PC als Arbeitsstation.

	Angegliederte Einheitentypen und untertypen: --- MAT : Hardware Der Einheitentyp "Hardware" umfasst alle physischen Elemente eines Informationssystems. MAT_ACT : Datenverarbeitungsmittel (aktiv) Automatische Datenverarbeitungsanlage mit allen notwendigen Organen für einen autonomen Betrieb.
MAT_ACT.3: Verarbeitungsperipheriegerät	
Typ	MAT_ACT.3: Verarbeitungsperipheriegerät
Beschreibung	Beschreibung: --- An den Rechner über eine Schnittstelle (seriell, parallel, USB usw.) angeschlossenes Gerät für die Erfassung, den Transport und das Senden von Daten. Beispiele: --- Drucker, externes Plattenlaufwerk. Angegliederte Einheitentypen und untertypen: --- MAT: Hardware Der Einheitentyp "Hardware" umfasst alle physischen Elemente eines Informationssystems. MAT_ACT: Datenverarbeitungsmittel (aktiv) Automatische Datenverarbeitungsanlage mit allen notwendigen Organen für einen autonomen Betrieb.

2.1.2 MAT_PAS : Datenträger (passiv)

MAT_PAS: Datenträger (passiv)	
Typ	MAT_PAS: Datenträger (passiv)
Beschreibung	Beschreibung: --- Hier handelt es sich um Datenträger zur Speicherung von Informationen oder Funktionen. Angegliederte Einheitentypen und untertypen: --- MAT: Hardware Der Einheitentyp "Hardware" umfasst alle physischen Elemente eines Informationssystems.
MAT_PAS.1: Elektronischer Datenträger	
Typ	MAT_PAS.1: Elektronischer Datenträger
Beschreibung	Beschreibung: --- IT-Datenträger, der zur Speicherung von Daten an einen Rechner oder ein Rechnernetz angeschlossen werden kann. Sie sind imstande, bei kleiner Größe ein großes Datenvolumen zu speichern. Sie sind auf Standardgeräten einsetzbar. Beispiele: --- Diskette, CD-Rom, Cartridge, externe Festplatte, Speicherschlüssel, Band. Angegliederte Einheitentypen und untertypen: --- MAT: Hardware Der Einheitentyp "Hardware" umfasst alle physischen Elemente eines

	Informationssystems. MAT_PAS: Datenträger (passiv) Hier handelt es sich um Datenträger zur Speicherung von Informationen oder Funktionen.

MAT_PAS.2: Sonstige Datenträger

Typ	MAT_PAS.2: Sonstige Datenträger
Beschreibung	Beschreibung: ---------- Statischer, nicht elektronischer Datenträger. Beispiele: ---------- Papier, Diapositiv, Folie, Dokument, Fax. Angegliederte Einheitentypen und untertypen: ---------- MAT: Hardware Der Einheitentyp "Hardware" umfasst alle physischen Elemente eines Informationssystems. MAT_PAS: Datenträger (passiv) Hier handelt es sich um Datenträger zur Speicherung von Informationen oder Funktionen.

2.2 LOG : Software

LOG: Software	
Typ	LOG: Software
Beschreibung	Beschreibung: ---------- Der Einheitentyp "Software" umfasst alle Programme, die für den Betrieb einer Datenverarbeitungseinheit erforderlich sind.

2.2.1 LOG_OS : Betriebssystem

LOG_OS: Betriebssystem	
Typ	LOG_OS: Betriebssystem
Beschreibung	Beschreibung: ---------- Unter diesem Begriff werden alle Softwareprogramme eines Rechners zusammengefasst, die die operationelle Basis bilden, auf der alle weiteren Softwareprogramme aufbauen werden (Dienste und Anwendungen). Das Betriebssystem besteht aus einem Kern und aus Basisfunktionen bzw. -diensten. Je nach Architektur ist das Betriebssystem monolithisch oder es wird von einem Mikrokern plus einer Anzahl von Systemdiensten gebildet. Das Betriebssystem enthält im Wesentlichen alle Dienste zur Verwaltung der Betriebsmittel (CPU, Speicher, Platten, Peripherien und Netzschnittstellen), jene zur Verwaltung der Aufgaben oder Verfahren und jene zur Verwaltung der Benutzer und ihrer Rechte. Beispiele: ---------- GCOS, MVS, Solaris, Linux, Windows95, Windows2000, Windows XP, Palm OS, WCX, Mac OS. Angegliederte Einheitentypen und untertypen: ---------- LOG: Software Der Einheitentyp "Software" umfasst alle Programme, die für den Betrieb einer Datenverarbeitungseinheit erforderlich sind.

2.2.2 LOG_SRV : Dienst-, Wartungs- oder Administrationsprogramme

LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme	
Typ	LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
Beschreibung	Beschreibung: ---------- Softwareprogramm, das sich dadurch auszeichnet, dass es die Dienste des Betriebssystems vervollständigt und dass es nicht direkt im Dienste der Benutzer oder der Anwendungen steht (selbst wenn es meistens wesentlich oder gar unabdingbar für den globalen Betrieb des IS ist). Beispiele: ---------- GCOS, MVS, Solaris, Linux, Windows95, Windows2000, WindowsXP, PalmOS, WCX, MacOS. Angegliederte Einheitentypen und untertypen: ---------- LOG: Software Der Einheitentyp "Software" umfasst alle Programme, die für den Betrieb einer Datenverarbeitungseinheit erforderlich sind.

2.2.3 LOG_STD : Programmpaket oder Standard-Software

LOG_STD: Programmpaket oder Standard-Software	
Typ	LOG_STD: Programmpaket oder Standard-Software
Beschreibung	Beschreibung: --- Die Standard-Softwareprogramme bzw. Programmpakete werden als solche auf den Markt gebracht (d. h. es sind keine einzigartigen oder spezifischen Sonderentwicklungen), einschließlich Unterstützung, Version und Wartung. Sie erweisen den Benutzern und Anwendungen "generische" Dienste, sind jedoch nicht individuell oder speziell angefertigt wie die tätigkeitsgebundenen Anwendungen. Beispiele: --- Datenbankverwaltungsprogramm, Listserv, Groupwareprogramm, Verzeichnissoftware, Webserver-Software usw. (Oracle, DB2, IIS, Apache, Lotus Notes, Exchange, OpenLDAP...). Angegliederte Einheitentypen und untertypen: --- LOG: SoftwareDer Einheitentyp "Software" umfasst alle Programme, die für den Betrieb einer Datenverarbeitungseinheit erforderlich sind.

2.2.4 LOG_APP : Tätigkeitsgebundene Anwendung

LOG_APP: Tätigkeitsgebundene Anwendung	
Typ	LOG_APP: Tätigkeitsgebundene Anwendung
Beschreibung	Angegliederte Einheitentypen und untertypen: --- LOG: Software Der Einheitentyp "Software" umfasst alle Programme, die für den Betrieb einer Datenverarbeitungseinheit erforderlich sind.

LOG_APP.1: Tätigkeitsgebundene Standardanwendun	
Typ	LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Beschreibung	Beschreibung: --- Es handelt sich hier um marktübliche Softwareprogramme, deren Ziel es ist, den Benutzern direkt alle Dienste und Funktionen bereit zu stellen, die sie von ihrem Informationssystem im Rahmen der Ausübung ihrer Tätigkeit erwarten. Die Anwendungsbereiche sind vielfach und definitionsgemäß ohne Grenzen. Beispiele: --- Buchhaltungsprogramme, Programme zur Steuerung von Werkzeugmaschinen, "Customer-care-Software", Programme für leistungsorientierten Personaleinsatz, Programme für administrative Teleprozeduren. Angegliederte Einheitentypen und untertypen: --- LOG: Software Der Einheitentyp "Software" umfasst alle Programme, die für den Betrieb einer Datenverarbeitungseinheit erforderlich sind. LOG_APP: Tätigkeitsgebundene Anwendung

LOG_APP.2: Tätigkeitsgebundene Sonderanwendung	
Typ	LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
Beschreibung	Beschreibung: ---

Hier geht es um Sonderanwendungen (mit unmittelbarer Auswirkung auf Aspekte wie z. B. Unterstützung, Wartung oder Weiterentwicklungen), deren Ziel es ist, den Benutzern direkt alle Dienste und Funktionen bereit zu stellen, die sie von ihrem Informationssystem im Rahmen der Ausübung ihrer Tätigkeit erwarten. LDie Anwendungsbereiche sind vielfach und definitionsgemäß ohne Grenzen.

Beispiele:

Rechnungsdatenverwaltung der Kunden eines Telefon-Providers, eine Anwendung zur Verfolgung von Raketenabschüssen in Echtzeit.

Angegliederte Einheitentypen und untertypen:

LOG: Software
Der Einheitentyp "Software" umfasst alle Programme, die für den Betrieb einer Datenverarbeitungseinheit erforderlich sind.
LOG_APP: Tätigkeitsgebundene Anwendung

2.3 RES : Netzwerk

RES: Netzwerk	
Typ	RES: Netzwerk
Beschreibung	Beschreibung: ---------- Der Einheitentyp "Netzwerk" umfasst alle Telekommunikationseinrichtungen, über die mehrere ausgelagerte Rechner oder Teile des Informationssystems untereinander verbunden werden können.

2.3.1 RES_INF : Medien und Informationsträger

RES_INF: Medien und Informationsträger	
Typ	RES_INF: Medien und Informationsträger
Beschreibung	Beschreibung: ---------- Die Kommunikations- und Telekommunikationsmedien und -träger zeichnen sich v. a. durch die physischen und technischen Merkmale des Informationsträgers (Punkt-zu-Punkt, Broadcast) und durch die Kommunikationsprotokolle aus (Verbindung oder Netzwerk -Niveau 2 und 3 des OSI-Sieben-Schichten-Modells.) Beispiele: ---------- RTC, Ethernet, GigabitEthernet, Kabel, Glasfaser, Kupfer-DSL, WiFi 802.11, BlueTooth, FireWire. Angegliederte Einheitentypen und untertypen: ---------- RES: Netzwerk Der Einheitentyp "Netzwerk" umfasst alle Telekommunikationseinrichtungen, über die mehrere ausgelagerte Rechner oder Teile des Informationssystems untereinander verbunden werden können.

2.3.2 RES_REL : Passives oder aktives Relais

RES_REL: Passives oder aktives Relais	
Typ	RES_REL: Passives oder aktives Relais
Beschreibung	Beschreibung: ---------- Unter diesem Untertyp werden alle Vorrichtungen zusammengefasst, die keine logischen Kommunikationsendeinrichtungen (IS-Vision) sondern Zwischenglieder oder Relais darstellen. Diese Relais enthalten Hardwarekomponenten, häufig jedoch Ad-hoc-Software. Sie zeichnen sich durch netzwerkgestützte Kommunikationsprotokolle aus. Sie enthalten häufig neben dem einfachen Relais Aufschaltungs- und/oder Filterfunktionen und -dienste (Kommunikationssteuerung bzw. Filter in den Routern). Sie sind meistens aus der Entfernung administrierbar, und einige von ihnen sind in der Lage, Protokolldaten zu erzeugen (Journale). Beispiele: ---------- Brücke, Router, Hub, Switch, automatischer Umschalter. Angegliederte Einheitentypen und untertypen: ---------- RES: Netzwerk Der Einheitentyp "Netzwerk" umfasst alle Telekommunikationseinrichtungen, über die mehrere ausgelagerte Rechner oder Teile des Informationssystems

	untereinander verbunden werden können.

2.3.3 RES_INT : Kommunikationsschnittstelle

RES_INT: Kommunikationsschnittstelle	
Typ	RES_INT: Kommunikationsschnittstelle
Beschreibung	Beschreibung: ---------- Kommunikationsschnittstellen der Verarbeitungseinheiten. Sie sind an diese gebunden, charakterisieren sich jedoch durch die akzeptierten Medien und Protokolle, durch die eventuellen Funktionen und Filterkapazitäten, die Fähigkeit Protokolle oder Fehlerjournale zu erzeugen und durch die Möglichkeit und Notwendigkeit einer Teleadministration. Beispiele: ---------- Wifi-Adapter, GPRS, Ethernet. Angegliederte Einheitentypen und untertypen: ---------- RES: Netzwerk Der Einheitentyp "Netzwerk" umfasst alle Telekommunikationseinrichtungen, über die mehrere ausgelagerte Rechner oder Teile des Informationssystems untereinander verbunden werden können.

2.3.4 PER : Personal

PER: Personal	
Typ	PER: Personal
Beschreibung	Beschreibung: ---------- Der Einheitentyp "Personal" umfasst die Gesamtheit aller Personengruppen, die mit dem Informationssystem in Kontakt stehen.

2.3.5 PER_DEC : Entscheidungsträger

PER_DEC: Entscheidungsträger	
Typ	PER_DEC: Entscheidungsträger
Beschreibung	Beschreibung: ---------- In diese Kategorie fallen die Eigentümer wesentlicher Elemente (Informationen und Funktionen) und die hierarchisch Vorgesetzten einer Institution oder eines bestimmten Projekts. Beispiele: ---------- Generaldirektion, Projektleiter. Angegliederte Einheitentypen und untertypen: ---------- PER: Personal Der Einheitentyp "Personal" umfasst die Gesamtheit aller Personengruppen, die mit dem Informationssystem in Kontakt stehen.

2.3.6 PER_UTI : Benutzer

PER_UTI: Benutzer	
Typ	PER_UTI: Benutzer
Beschreibung	Beschreibung: ---------- In diese Kategorie fallen alle Personen, die im Rahmen ihrer Tätigkeit sensitive Elemente bearbeiten und auf Grund dessen eine besondere Verantwortung tragen. Sie können zur Ausübung ihrer täglichen Arbeiten über besondere Zugriffsprivilegien auf das Informationssystem verfügen. Beispiele: ---------- Human-Ressource-Direktion, Direktion für das Finanzwesen, Risiko-Manager. Angegliederte Einheitentypen und untertypen: ---------- PER: Personal Der Einheitentyp "Personal" umfasst die Gesamtheit aller Personengruppen, die mit dem Informationssystem in Kontakt stehen.

2.3.7 PER_EXP : Betreiber / Wartung

PER_EXP: Betreiber / Wartung	
Typ	PER_EXP: Betreiber / Wartung
Beschreibung	Beschreibung: ---------- In diese Kategorie fallen alle Personen, die mit dem Betrieb und der Wartung des Informationssystems beauftragt sind. Sie verfügen zur Ausübung ihrer täglichen

	Arbeiten über besondere Zugriffsprivilegien auf das Informationssystem. Beispiele: ---------- Systemadministrator, Datenadministrator, Sicherungsoperator, Help Desk, Anwendungsdemonstrator, Sicherheitspersonal. Angegliederte Einheitentypen und untertypen: ---------- PER: Personal Der Einheitentyp "Personal" umfasst die Gesamtheit aller Personengruppen, die mit dem Informationssystem in Kontakt stehen.

2.3.8 PER_DEV : Entwickler

PER_DEV: Entwickler	
Typ	PER_DEV: Entwickler
Beschreibung	Beschreibung: ---------- In diese Kategorie fallen alle Personen, die innerhalb der Institution mit der Entwicklung von Anwendungen beauftragt sind. Sie haben auf einen Teil des Informationssystems Zugriff mit fortgeschrittenen Benutzerprivilegien, wirken jedoch nicht auf die Produktionsdaten ein.* Beispiele: ---------- Entwickler von tätigkeitsgebundenen Anwendungen. Angegliederte Einheitentypen und untertypen: ---------- PER: Personal Der Einheitentyp "Personal" umfasst die Gesamtheit aller Personengruppen, die mit dem Informationssystem in Kontakt stehen.

2.4 PHY : Standort

PHY: Standort	
Typ	PHY: Standort
Beschreibung	Beschreibung: ---------- Der Einheitentyp "Standort" umfasst alle Orte, an denen das System, Teile des Systems oder sonstige zum Betrieb notwendigen physischen Mittel untergebracht sind.

2.4.1 PHY_LIE : Orte

PHY_LIE: Orte	
Typ	PHY_LIE: Orte
Beschreibung	Beschreibung: ---------- Perimeter, physische Einzäunungen.

PHY_LIE.1: Äußere Umgebung	
Typ	PHY_LIE.1: Äußere Umgebung
Beschreibung	Beschreibung: ---------- Hier geht es um die Orte, an denen die Sicherheitsmaßnahmen der Institution nicht angewendet werden können. Beispiele: ---------- Wohnsitze des Personals, Räumlichkeiten einer anderen Institution, die äußere Umgebung rund um den Standort (Stadtgebiet, Risikogebiet). Angegliederte Einheitentypen und untertypen: ---------- PHY : Standort Der Einheitentyp "Standort" umfasst alle Orte, an denen das System, Teile des Systems oder sonstige zum Betrieb notwendigen physischen Mittel untergebracht sind. PHY_LIE: Ort Perimeter, physische Einzäunungen.

PHY_LIE.2: Räumlichkeiten	
Typ	PHY_LIE.2: Räumlichkeiten
Beschreibung	Beschreibung: ---------- Die Räumlichkeiten werden durch den Perimeter der Institution abgegrenzt, der unmittelbar an die äußere Umgebung anschließt. Dabei kann es sich um einen Perimeter physischer Schutzeinrichtungen (z. B. durch Aufstellen von Barrieren) oder um Überwachungsvorrichtungen rund um die Gebäude handeln. Beispiele: ---------- Einrichtung, Gebäude. Angegliederte Einheitentypen und untertypen: ---------- PHY: Standort Der Einheitentyp "Standort" umfasst alle Orte, an denen das System, Teile des Systems oder sonstige zum Betrieb notwendigen physischen Mittel untergebracht sind. PHY_LIE: Ort

	Perimeter, physische Einzäunungen.

PHY_LIE.3: Zone	
Typ	PHY_LIE.3: Zone
Beschreibung	Beschreibung: ---------- Hierbei handelt es sich um einen physischen Schutzperimeter, der eine Abtrennung der Räumlichkeiten innerhalb der Institution ermöglicht. Er wird durch das Aufstellen physischer Barrieren rund um die Infrastrukturen zur Informationsverarbeitung innerhalb der Institution realisiert. Beispiele: ---------- Büros, Zonen mit eingeschränktem Zugang, Sicherheitszonen. Angegliederte Einheitentypen und untertypen: ---------- PHY: Standort Der Einheitentyp "Standort" umfasst alle Orte, an denen das System, Teile des Systems oder sonstige zum Betrieb notwendigen physischen Mittel untergebracht sind. PHY_LIE: Ort Perimeter, physische Einzäunungen.

2.4.2 PHY_SRV : Wesentlicher Dienst

PHY_SRV: Wesentlicher Dienst	
Typ	PHY_SRV: Wesentlicher Dienst
Beschreibung	Beschreibung: ---------- Gesamtheit aller Dienste, die für den geordneten Betrieb der Betriebsmittel der Institution erforderlich sind. Angegliederte Einheitentypen und untertypen: ---------- PHY: Standort Der Einheitentyp "Standort" umfasst alle Orte, an denen das System, Teile des Systems oder sonstige zum Betrieb notwendigen physischen Mittel untergebracht sind.

PHY_SRV.1: Kommunikation	
Typ	PHY_SRV.1: Kommunikation
Beschreibung	Beschreibung: ---------- Durch einen Provider bereitgestellte Telekommunikationsdienste und -geräte. Beispiele: ---------- Fernsprechleitung, PABX, interne Fernsprechnetze. Angegliederte Einheitentypen und untertypen: ---------- PHY: Standort Der Einheitentyp "Standort" umfasst alle Orte, an denen das System, Teile des Systems oder sonstige zum Betrieb notwendigen physischen Mittel untergebracht sind. PHY_SRV: Wesentlicher Dienst Gesamtheit aller Dienste, die für den geordneten Betrieb der Betriebsmittel der Institution erforderlich sind.

PHY_SRV.2: Energie

Typ	PHY_SRV.2: Energie
Beschreibung	Beschreibung: ---------- Zur Stromspeisung der IT- und Peripheriegeräte erforderliche Dienste und Mittel (Quellen und Verkabelung). Beispiele: ---------- Niederspannungsversorgung, Wechselrichter, elektrische Kopfstation. Angegliederte Einheitentypen und untertypen: ---------- PHY: Standort Der Einheitentyp "Standort" umfasst alle Orte, an denen das System, Teile des Systems oder sonstige zum Betrieb notwendigen physischen Mittel untergebracht sind. PHY_SRV: Wesentlicher Dienst Gesamtheit aller Dienste, die für den geordneten Betrieb der Betriebsmittel der Institution erforderlich sind.

PHY_SRV.3: Abkühlung / Verschmutzung

Typ	PHY_SRV.3: Abkühlung / Verschmutzung
Beschreibung	Beschreibung: ---------- Zur Abkühlung und Luftaufbereitung erforderliche Dienste und Mittel (Material, Leitungen). Beispiele: ---------- Kühlwasserleitungen, Klimatisierungssysteme. Angegliederte Einheitentypen und untertypen: ---------- PHY: Standort Der Einheitentyp "Standort" umfasst alle Orte, an denen das System, Teile des Systems oder sonstige, zum Betrieb notwendigen physischen Mittel untergebracht sind. PHY_SRV: Wesentlicher Dienst Gesamtheit aller Dienste, die für den geordneten Betrieb der Betriebsmittel der Institution erforderlich sind.

2.5 ORG : Organisation

ORG: Organisation	
Typ	ORG: Organisation
Beschreibung	Beschreibung: ---------- Der Einheitentyp "Organisation" beschreibt den organisatorischen Rahmen. Er umfasst sämtliche Strukturen der Personal-Aufgaben-Zuordnung sowie alle Prozeduren zur Regelung dieser Strukturen.

2.5.1 ORG_DEP : Organisation, von der die Institution abhängt

ORG_DEP: Organisation, von der die Institution abhängt	
Typ	ORG_DEP: Organisation, von der die Institution abhängt
Beschreibung	Beschreibung: ---------- Es geht hierbei um die Organisationen, von denen die untersuchte Institution abhängig ist, egal ob diese Abhängigkeit im juristischen Sinne besteht oder nicht. Die untersuchte Institution ist gebunden, was die Vorschriften, Entscheidungen, Aktionen und auch den Informationsfluss anbelangt. Beispiele: ---------- Vormundschaftsinstitution, Sitz einer Institution, Rechnungshof. Angegliederte Einheitentypen und untertypen: ---------- ORG Der Einheitentyp "Organisation" beschreibt den organisatorischen Rahmen. Er umfasst sämtliche Strukturen der Personal-Aufgaben-Zuordnung sowie alle Prozeduren zur Regelung dieser Strukturen.

2.5.2 ORG_GEN : Organisation der Institution

ORG_GEN: Organisation der Institution	
Typ	ORG_GEN: Organisation der Institution
Beschreibung	Beschreibung: ---------- Hier geht es um die verschiedenen Zweige der Institution, die einer gemeinsamen Direktion untergeordnet sind; transversale Aktivitäten sind ebenso inbegriffen. Beispiele: ---------- Human-Ressource-Direktion, Direktion Datenverarbeitung, Direktion Einkauf, Direktionen der einzelnen Tätigkeitsbereiche, Abteilung Gebäudeschutz, Abteilung Brandschutz, Audit-Direktion. Angegliederte Einheitentypen und untertypen: ---------- ORG Der Einheitentyp "Organisation" beschreibt den organisatorischen Rahmen. Er umfasst sämtliche Strukturen der Personal-Aufgaben-Zuordnung sowie alle Prozeduren zur Regelung dieser Strukturen.

2.5.3 ORG_PRO : Organisation eines Projekts oder eines Systems

ORG_PRO: Organisation eines Projekts oder eines Systems

Typ	ORG_PRO: Organisation eines Projekts oder eines Systems
Beschreibung	Beschreibung: ---------- Dabei geht es um die Organisation, die speziell für ein bestimmtes Projekt oder einen bestimmten Dienst eingerichtet wurde. Beispiele: ---------- Projektorganisation für die Entwicklung einer neuen Anwendung, Projekt zur Migration eines Informationssystems. Angegliederte Einheitentypen und untertypen: ---------- ORG Der Einheitentyp "Organisation" beschreibt den organisatorischen Rahmen. Er umfasst sämtliche Strukturen der Personal-Aufgaben-Zuordnung sowie alle Prozeduren zur Regelung dieser Strukturen.

2.5.4 ORG_EXT : Unterauftragnehmer / Lieferanten / Industrielle

ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle	
Typ	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Beschreibung	Beschreibung: ---------- Organisation, die der Institution Dienste oder Mittel bereitstellt und die vertraglich an sie gebunden ist. Beispiele: ---------- Facilities Management-, Outsourcing-, Consulting-Services. Angegliederte Einheitentypen und untertypen: ---------- ORG Der Einheitentyp "Organisation" beschreibt den organisatorischen Rahmen. Er umfasst sämtliche Strukturen der Personal-Aufgaben-Zuordnung sowie alle Prozeduren zur Regelung dieser Strukturen.

2.6 SYS : System

SYS: System	
Typ	SYS: System
Beschreibung	Beschreibung: ---------- Der Einheitentyp "System" umfasst alle klar definierten IT-Installationen einschließlich ihrer operationellen Umgebung. Er umfasst verschiedene Einheiten, die anderen zuvor genannten Einheitentypen angehören.

2.6.1 SYS_INT : Einrichtung für Internetzugang

SYS_INT: Einrichtung für Internetzugang	
Typ	SYS_INT: Einrichtung für Internetzugang
Beschreibung	Beschreibung: ---------- Einrichtung zum Anschluss des institutionseigenen Netzes an das Internet einschließlich Zugangsdienste zum und vom Internet. Beispiele: ---------- Filtereinrichtung, DMZ, Gateways. Angegliederte Einheitentypen und untertypen: ---------- SYS: System Der Einheitentyp "System" umfasst alle klar definierten IT-Installationen einschließlich ihrer operationellen Umgebung. Er umfasst verschiedene Einheiten, die anderen zuvor genannten Einheitentypen angehören.

2.6.2 SYS_MES : Nachrichtenübermittlung

SYS_MES: Nachrichtenübermittlung	
Typ	SYS_MES: Nachrichtenübermittlung
Beschreibung	Beschreibung: ---------- Einrichtung, die es den dazu ermächtigten Benutzern ermöglicht, über an das Netz angeschlossene Rechner elektronische Daten oder Mitteilungen zu erfassen, zu einem späteren Zeitpunkt abzurufen und zu übertragen. Beispiele: ---------- Interne Nachrichtenübermitteilung, Web-Nachrichtenübermittlung. Angegliederte Einheitentypen und untertypen: ---------- SYS: System Der Einheitentyp "System" umfasst alle klar definierten IT-Installationen einschließlich ihrer operationellen Umgebung. Er umfasst verschiedene Einheiten, die anderen zuvor genannten Einheitentypen angehören.

2.6.3 SYS_ITR : Intranet

SYS_ITR: Intranet	
Typ	SYS_ITR: Intranet
Beschreibung	Beschreibung: ---------- Geteilte Daten und Datendienste und privates Netz, das einheitliche

	Kommunikationsprotokolle und Technologien benutzt (z. B. die Internettechnologie). Beispiele: ---------- Internes Informationssystem. Angegliederte Einheitentypen und untertypen: ---------- SYS: System Der Einheitentyp "System" umfasst alle klar definierten IT-Installationen einschließlich ihrer operationellen Umgebung. Er umfasst verschiedene Einheiten, die anderen zuvor genannten Einheitentypen angehören.

2.6.4 SYS_ANU : Unternehmensverzeichnis

SYS_ANU: Unternehmensverzeichnis	
Typ	SYS_ANU: Unternehmensverzeichnis
Beschreibung	Beschreibung: ---------- Eine Einrichtung für die Verwaltung und den Zugriff auf eine Datenbank, in der die Mitarbeiter des Unternehmens sowie deren persönliche Daten verzeichnet sind. Beispiele: ---------- Verwaltung von Anwendungsrechten. Angegliederte Einheitentypen und untertypen: ---------- SYS: System Der Einheitentyp "System" umfasst alle klar definierten IT-Installationen einschließlich ihrer operationellen Umgebung. Er umfasst verschiedene Einheiten, die anderen zuvor genannten Einheitentypen angehören.

2.6.5 SYS_WEB : Externes Portal

SYS_WEB: Externes Portal	
Typ	SYS_WEB: Externes Portal
Beschreibung	Beschreibung: ---------- Bei einem externen Portal handelt es sich um einen Zugriffspunkt, den ein Benutzer aufsucht bzw. benutzt, wenn er eine Auskunft einholen oder einen Dienst der Institution in Anspruch nehmen möchte. Die Portale bieten eine große Auswahl an Ressourcen und Diensten an. Beispiele: ---------- Informationsportal, Teleprozedurportal, E-Commerce-Website. Angegliederte Einheitentypen und untertypen: ---------- SYS: System Der Einheitentyp "System" umfasst alle klar definierten IT-Installationen einschließlich ihrer operationellen Umgebung. Er umfasst verschiedene Einheiten, die anderen zuvor genannten Einheitentypen angehören.

3 Allgemeine Angriffsmethoden und allgemeine bedrohende Elemente

In der folgenden Tabelle werden die Angriffsmethoden mit ihren wesentlichen Auswirkungen auf die Sicherheitsgrundwerte dargestellt. Die Angriffsmethoden werden nach repräsentativen Themen sortiert (sie können aber durchaus mehreren Themen zugeordnet werden).

Angriffsmethode	Integrität	Verfügbarkeit	Vertraulichkeit
1 - Physische Schadensfälle			
01 - BRAND	X	X	
02 - WASSERSCHÄDEN	X	X	
03 - VERSCHMUTZUNG	X	X	
04 - GRÖSSERER SCHADENSFALL	X	X	
05 - ZERSTÖRUNG VON BETRIEBSMITTELN ODER DATENTRÄGERN	X	X	
2 - Natürliche Ereignisse			
06 - KLIMATISCHES PHÄNOMEN	X	X	
07 - SEISMISCHES PHÄNOMEN	X	X	
08 - VULKANISCHES PHÄNOMEN	X	X	
09 - METEOROLOGISCHES PHÄNOMEN	X	X	
10 - HOCHWASSER	X	X	
3 - Ausfall wesentlicher Dienste			
11 - AUSFALL DER KLIMATISIERUNGSSYSTEME		X	
12 - AUSFALL DER ENERGIEVERSORGUNG		X	
13 - AUSFALL DER TELEKOMMUNIKATIONSMITTEL		X	
4 - Störungen durch Strahlung			
14 - ELEKTROMAGNETISCHE STRAHLUNG	X	X	
15 - THERMISCHE STRAHLUNG	X	X	
16 - ELEKTROMAGNETISCHE IMPULSE	X	X	
5 - Infragestellung von Informationen			
17 - ABFANGEN VON KOMPROMITTIERENDEN STÖRSIGNALEN			X
18 - FERN-SPIONAGE	X	X	X
19 - PASSIVES MITHÖREN			X
20 - DIEBSTAHL VON DATENTRÄGERN ODER UNTERLAGEN			X
21 - DIEBSTAHL VON BETRIEBSMITTELN		X	X
22 - ÜBERNAHME RECYCELTER ODER AUSGEMUSTERTER DATENTRÄGER			X
23 - VERBREITUNG			X
24 - INFORMATIONEN OHNE HERKUNFTSGARANTIE	X	X	
25 - SABOTIEREN DER HARDWARE			X
26 - SABOTIEREN DER SOFTWARE	X	X	X
27 - GEOLOKALISATION			X
6 - Technische Störungen			
28 - AUSFALL VON BETRIEBSMITTELN		X	

29 - FEHLERHAFTER BETRIEB VON BETRIEBSMITTELN		X	
30 - ÜBERLASTUNG DES INFORMATIONSSYSTEMS		X	
31 - FEHLERHAFTER BETRIEB VON SOFTWAREPROGRAMMEN	X	X	
32 - BEEINTRÄCHTIGUNG DER WARTBARKEIT DES INFORMATIONSSYSTEMS		X	
7 - Widerrechtliche Aktionen			
33 - UNZULÄSSIGE BENUTZUNG DER BETRIEBSMITTEL	X	X	X
34 - BETRÜGERISCHE KOPIE VON SOFTWAREPROGRAMMEN			X
35 - BENUTZUNG GEFÄLSCHTER ODER KOPIERTER SOFTWAREPROGRAMME		X	
36 - DATENMANIPULATION	X		X
37 - UNZULÄSSIGE VERARBEITUNG VON DATEN			X
8 - Infragestellung von Funktionen			
38 - BENUTZUNGSFEHLER	X	X	X
39 - RECHTSMISSBRAUCH	X	X	X
40 - RECHTSANMASSUNG	X	X	X
41 - VERLEUGNUNG VON AKTIONEN	X		
42 - BEEINTRÄCHTIGUNG DER PERSONALVERFÜGBARKEIT		X	

Die Beschreibung der Angriffsmethoden erfolgt in Abhängigkeit von den bedrohenden Elementen, die diese Methoden ausnutzen können.

Thema 1 – Physische Schadensfälle

01 - BRAND

Beschreibung

Typ

Natürlich bedingt / Menschlich bedingt / Umgebungsbedingt.

Unabsichtliche Ursache

Anhäufung brennbarer oder explosionsgefährdeter Stoffe in einer geschlossenen Umgebung, die durch ein externes Ereignis oder einen internen Unfall entzündet werden.

Beispiele:

Blitz, Papierkorbbrand, Kurzschluss.

Absichtliche Ursache

Terroristen, Rowdys verschaffen sich Zugang zu den Gütern, um brennbare oder explosionsgefährdete Stoffe direkt oder indirekt in Brand zu setzen (Brandbomben, Zerstörung der Belüftungsanlagen usw.).

Beispiele:

Ein Streikender verschafft sich Zugang zu den Büroräumen (z. B. durch die Fenster des IT-Zentrums), um dort einen Brandkörper zu werfen.

Mögliche Konsequenzen

Zerstörung des Gutes.Gefährdung der Sicherheit von Personen. Finanzielle VerlusteStörung des internen Betriebs.

Verletzungen

Integrität
Verfügbarkeit

02 - WASSERSCHÄDEN

Beschreibung

Typ

Natürlich bedingt / Menschlich bedingt / Umgebungsbedingt.

Unabsichtliche Ursache

Überschwemmung auf Grund einer undichten Stelle oder eines Rohrbruchs.

Beispiele:

Undichte Klimatisierungssysteme; Wasser sickert aus einem Waschraum einer oberen Etage durch; offenes Strahlrohr.

Absichtliche Ursache

Terroristen, Rowdys verschaffen sich Zugang zum Gut, um eine Überschwemmung der Räume auszulösen.

Beispiele:

Absichtlicher Rohrbruch, Auslösung der Löschsysteme oder einfach Bespritzen der Einrichtung.

Mögliche Konsequenzen

	---------- Zerstörung oder vorübergehende Nicht-Verfügbarkeit eines Gutes. Finanzielle Verluste. Störung des internen Betriebs.
Verletzungen	Integrität Verfügbarkeit

03 - VERSCHMUTZUNG

Beschreibung	Typ ------ Natürlich bedingt / Menschlich bedingt / Umgebungsbedingt. Unabsichtliche Ursache ---------- Vorhandensein von Staub, Dämpfen, korrosiven oder giftigen Gasen in der Umgebungsluft. Beispiele: ---------- Auspuffgase in einem Bereich dichten Verkehrs. Absichtliche Ursache ---------- Absichtliche Luftverschmutzung durch Beschädigung der Klimatisierungssysteme oder durch Hinterlassen einer Verschmutzungsquelle in den Räumen. Beispiele: ---------- Böswilliger Zugang und Hinterlassen eines Schadstoffs in den Kanälen zur Belüftung, Heizung oder Klimatisierung. Mögliche Konsequenzen ---------- Zerstörung eines Gutes. Gefährdung der Sicherheit von Personen. Verfügbarkeit von operationellem Personal.
Verletzungen	Integrität Verfügbarkeit

04 - GRÖSSERER SCHADENSFALL

Beschreibung	Typ ------ Natürlich bedingt / Umgebungsbedingt. Unabsichtliche Ursache ---------- Äußeres Ereignis oder Schadensfall, der auf die natürliche bzw. industrielle Umgebung der Güter zurückzuführen ist und diese physisch gesehen gravierend beeinträchtigen kann. Beispiele: ---------- Explosion nah liegender Industriestandorte, Erdrutsche, Flutwellen, Flugzeugabstürze, beschädigtes bzw. zerstörtes Mobilfahrzeug infolge eines Zusammenstoßes. Absichtliche Ursache ---------- Äußeres Ereignis oder Schadensfall, der auf Rowdytum oder einen Terrorakt in unmittelbarer Umgebung der Güter zurückzuführen ist und diese physisch gesehen gravierend beeinträchtigen kann.

	Beispiele: --- Explosion nah liegender Industriestandorte, Erdrutsche, Flugzeugabstürze, beschädigtes bzw. zerstörtes Mobilfahrzeug infolge eines Zusammenstoßes. Mögliche Konsequenzen --- Zerstörung eines Gutes. Gefährdung der Sicherheit von Personen. Finanzielle Verluste. Betriebsstillstand.
Verletzungen	Integrität Verfügbarkeit

05 - ZERSTÖRUNG VON BETRIEBSMITTELN ODER DATENTRÄGERN

Beschreibung	Typ --- Menschlich bedingt. Unabsichtliche Ursache --- Nachlässigkeit oder unabsichtliches Ereignis, das die Zerstörung eines Betriebsmittels oder Datenträgers zur Folge hat. Beispiele: --- Nachlässigkeit beim Transport der Hardware. Lagerung archivierter Datenträger unter schlechten Umgebungsbedingungen. Durch Tiere verursachte Schäden. Verschütten von Nahrung oder Getränken auf Betriebsmittel. Absichtliche Ursache --- Jemand verschafft sich Zugang zu den Betriebsmitteln und verursacht deren Zerstörung. Beispiele --- Zerstörung eines Rechners einschließlich Sicherungskopien (Cartridges). Mögliche Konsequenzen --- Datenverlust. Finanzielle Verluste in Höhe des Wertes des zerstörten Betriebsmittels. Nicht-Verfügbarkeit des Gerätes.
Verletzungen	Integrität Verfügbarkeit

Thema 2 – Natürliche Ereignisse

06 - KLIMATISCHES PHÄNOMEN

Beschreibung	Typ --- Natürlich bedingt. Unabsichtliche Ursache --- Besondere klimatische Bedingungen (an der Grenze der tolerierten Betriebsbedingungen der Betriebsmittel). Beispiele --- Standort in einer geografischen Lage, in der extreme Hitze, Kälte, Feuchtigkeit, Wind und Trockenheit zu erwarten sind. Mögliche Konsequenzen --- Zerstörung oder vorübergehender Stillstand eines Gutes.
Verletzungen	Integrität Verfügbarkeit

07 - SEISMISCHES PHÄNOMEN

Beschreibung	Typ --- Natürlich bedingt. Unabsichtliche Ursache --- Ein Erdstoß oder Erdbeben verursacht extreme Vibrationen oder löst ein Katastrophenereignis aus (Flutwelle). Beispiele --- Standort in einer geografischen Lage, in der häufig Erdstöße verzeichnet werden. Mögliche Konsequenzen --- Zerstörung eines Gutes. Gefährdung der Sicherheit von Personen.
Verletzungen	Integrität Verfügbarkeit

08 - VULKANISCHES PHÄNOMEN

Beschreibung	Typ --- Natürlich bedingt. Unabsichtliche Ursache --- Ein Vulkanausbruch verursacht extreme Vibrationen oder löst ein weiteres Katastrophenereignis aus (Flutwelle). Beispiele --- Das Informationssystem wird an einem Standort untergebracht, dessen geografische Lage für vulkanische Aktivität bekannt ist (zeitweilig aussetzendes Phänomen, bei dem die Emissionsphasen mit z. T. sehr langen Ruhephasen

	abwechseln). Mögliche Konsequenzen --- Zerstörung eines Gutes. Gefährdung der Sicherheit von Personen.
Verletzungen	Integrität Verfügbarkeit

09 - METEOROLOGISCHES PHÄNOMEN

Beschreibung	Typ --- Natürlich bedingt / Menschlich bedingt. Unabsichtliche Ursache --- Punktuelle atmosphärische Störung verursacht extreme klimatische Bedingungen. Beispiele --- Unwetter, Orkane, Zyklone, Hagel, Blitz, Lawine. Absichtliche Ursache --- Ein Saboteur verschafft sich Zugang zu den Schutzeinrichtungen gegen Blitzschlag. Beispiele --- Beseitigung des Erdungsschutzes, Kurzschließung der Überspannungsableiter, Verstellung der Schutzeinrichtungen. Mögliche Konsequenzen --- Zerstörung eines Gutes. Gefährdung der Sicherheit von Personen.
Verletzungen	Integrität Verfügbarkeit

10 - HOCHWASSER

Beschreibung	Typ --- Natürlich bedingt. Unabsichtliche Ursache --- Fluss, Wasserlauf oder Grundwasser verursachen regelmäßig oder ausnahmsweise eine Überschwemmung der umliegenden Landstriche. Beispiele --- Der Standort kann sich im Überflutungsbereich eines nahe liegenden Flusses befinden und die Folgen einer Überschwemmung erleiden oder weiter entfernt liegen, aber die Konsequenzen dieser Überschwemmung zu spüren bekommen (Erdrutsch). Mögliche Konsequenzen --- Zerstörung eines Gutes. Gefährdung der Sicherheit von Personen.

	Finanzielle Verluste.
Verletzungen	Integrität Verfügbarkeit

Thema 3 – Ausfall wesentlicher Dienste

11 - AUSFALL DER KLIMATISIERUNGSSYSTEME

Beschreibung	Typ ------ Menschlich bedingt / Umgebungsbedingt. Unabsichtliche Ursache ---------- Ein Ausfall, Stillstand oder eine Störung der Klimatisierung kann bei Gütern, die eine Abkühlung und Belüftung benötigen, zu deren Stillstand, Fehlbetrieb oder gar Ausfall führen. Beispiele ---------- Fehlende Wartung der Klimatisierungssysteme, schlechte Dimensionierung der Anlage, Unterbrechung der Wasserzufuhr durch den Versorgungsbetrieb. Absichtliche Ursache ---------- Jemand sabotiert die Elemente, die zum Betrieb der Klimatisierungssysteme erforderlich sind (Unterbrechung der Wasser- oder Energiezufuhr, Zerstörung der Anlage). Beispiele ---------- Unterbrechung der Klimatisierung, Unterbrechung der Wasserzufuhr. Mögliche Konsequenzen ---------- Beschädigung von Gütern.
Verletzungen	Verfügbarkeit

12 - AUSFALL DER ENERGIEVERSORGUNG

Beschreibung	Typ ------- Menschlich bedingt / Umgebungsbedingt. Unabsichtliche Ursache ---------- Ausfall, Stillstand oder schlechte Dimensionierung der Energieversorgung der Güter, wobei die Energie entweder vom Versorgungsbetrieb oder durch interne Verteilungsvorrichtungen bereitgestellt wird. Beispiele ---------- Unterbrechung der Energieversorgung durch den frz. Versorgungsbetrieb EDF wegen Streik, Störungen oder Instandsetzungsarbeiten. Fehler oder schlechte Dimensionierung der internen elektrischen Zentrale bzw. des unterstützten Stromnetzes, vorausgesetzt solche Einrichtungen sind vorhanden. Anschluss nicht vorgesehener leistungsstarker Geräte an das Unterstützungsnetz, so dass die Notversorgungseinrichtung nicht ausreicht. Wartungsfehler oder Veralterung der Batterien des Wechselrichters. Unabsichtliche Unterbrechung der internen oder externen Kabel. Unterbrechung der Wasserversorgung (Fehler des Versorgerbetriebs, interne Anomalie durch Nachlässigkeit). Absichtliche Ursache

	--- Sabotage oder Störung der elektrischen Einrichtung durch jemanden, der sich Zugang zu den Gerätschaften verschafft hat (Kopfstation, Niederspannungsschalttafel, Wechselrichter usw.). Beispiele --- Absichtliche Unterbrechung der Stromkabel, absichtliche Unterbrechung der Wasserversorgung. Mögliche Konsequenzen --- Vorübergehende Unterbrechung der Stromversorgung, der Klimatisierung.
Verletzungen	Verfügbarkeit

13 - AUSFALL DER TELEKOMMUNIKATIONSMITTEL

Beschreibung	Typ --- Menschlich bedingt / Umgebungsbedingt. Unabsichtliche Ursache --- Störung, Stillstand oder schlechte Dimensionierung der Telekommunikationsdienste (Telefon, Internetzugang, Internet-Netz). Beispiele --- Streiks, außergewöhnliche externe Ereignisse, die eine Überlastung der Kommunikationen zur Folge haben. Absichtliche Ursache --- Sabotage oder Störung der Telekom-Einrichtung durch jemanden, der sich Zugang zur den Telekommunikationseinrichtungen verschafft hat (Kopfstation, PABX, Verteiler, Außenkabel usw.). Beispiele --- Absichtliche Unterbrechung der Telekom-Kabel, Zerstörung einer Telekom-Zentrale, absichtliche Überlastung der Telekom-Bandbreite. Mögliche Konsequenzen --- Kurze oder langfristige Unterbrechung der Telekom-Dienste. Finanzielle Verluste.
Verletzungen	Verfügbarkeit

Thema 4 – Störungen durch Strahlung

14 - ELEKTROMAGNETISCHE STRAHLUNG

Beschreibung

Typ

Menschlich bedingt / Umgebungsbedingt.

Unabsichtliche Ursache

Elektromagnetische Störungen auf Grund eines internen oder externen Gerätes.

Beispiele

Radar, Funkantenne, elektrische Zentrale, Werkzeugmaschine.

Absichtliche Ursache

Aussenden unerwünschter Strahlung zur Verhinderung oder Überlastung von Kommunikationen oder zur Störung des ordnungsgemäßen Betriebs von Gerätschaften.

Beispiele

Störende Beeinflussung von Wifi-Kommunikationen.

Mögliche Konsequenzen

Gestörte Anzeige auf Kathodenstrahl-Bildschirmgeräten, gestörte Kommunikationen.
Beeinträchtigungen, Betriebsstörungen.

Verletzungen

Integrität
Verfügbarkeit

15 - THERMISCHE STRAHLUNG

Beschreibung

Typ

Menschlich bedingt / Natürlich bedingt / Umgebungsbedingt.

Unabsichtliche Ursache

Thermischer Effekt infolge eines Schadensfalls oder außergewöhnlicher meteorologischer Bedingungen.

Beispiele

Auf Grund eines Waldbrandes befinden sich die Betriebsmittel außerhalb der tolerierten Betriebsbedingungen.

Absichtliche Ursache

Ein Gerät zur Erzeugung eines thermischen Effekts provoziert einen fehlerhaften Betrieb oder die Zerstörung von Betriebsmitteln.

Beispiele

Hinterlassen radioaktiver Abfälle in unmittelbarer Nähe des Betriebssystems, thermonukleare Explosion.

Mögliche Konsequenzen

	Fehlerhafter Betrieb oder Zerstörung von Betriebsmitteln. Gefährdung der Sicherheit von Personen. Finanzielle Verluste.
Verletzungen	Integrität Verfügbarkeit

16 - ELEKTROMAGNETISCHE IMPULSE

Beschreibung	Typ ------- Umgebungsbedingt. Unabsichtliche Ursache ---------- Ein Schadensfall bewirkt einen außergewöhnlichen elektromagnetischen Effekt. Beispiele ---------- Industrieunfall in unmittelbarer Nähe zum Standort. Absichtliche Ursache ---------- Elektromagnetische Impulse nuklearer Herkunft. Beispiele ---------- Bomben. Mögliche Konsequenzen ---------- Zerstörung des Gutes. Finanzielle Verluste.
Verletzungen	Integrität Verfügbarkeit

Thema 5 – Infragestellung von Informationen

17 - ABFANGEN VON KOMPROMITTIERENDEN STÖRSIGNALEN

Beschreibung

Typ

Menschlich bedingt.

Absichtliche Ursache

Aussendung elektromagnetischer Störsignale (durch Übertragung über elektrische Leitungen oder über Masseleiter oder durch Strahlung im freien Raum). Der Einfang dieser Signale hängt von der Entfernung zum anvisierten Gerät oder von der Möglichkeit ab, sich an die Verkabelung oder sonstige Leiter anzuschalten, die in unmittelbarer Nähe des Gerätes entlang laufen (Kopplungseffekt).

Beispiele

Ein Spion oder Hacker fängt elektromagnetische Signale mit Hilfe von Sensoren und elektronischem Material über die Rohrleitungen ab und zeichnet sie auf.
Ein Spion oder Hacker fängt elektromagnetische Signale ab, die von der Video-Strahlung einer IT-Arbeitsstation stammen und zeichnet sie auf.

Mögliche Konsequenzen

Weitergabe von Kommunikationen und Daten.

Verletzungen

Vertraulichkeit

18 - FERN-SPIONAGE

Beschreibung

Typ

Menschlich bedingt.

Absichtliche Ursache

Beobachtung aus der Entfernung von Aktionen, die von Mitarbeitern ausgeführt werden.

Beispiele

Visuelle Beobachtung ohne optische Mittel, z. B. Beobachtung eines Benutzers, der über Tastatur einen Code oder ein Passwort eingibt.

Mögliche Konsequenzen

Intrusion.
Benutzung einer fremden Identität

Verletzungen

Integrität
Vertraulichkeit
Verfügbarkeit

19 - PASSIVES MITHÖREN

Beschreibung

Typ

Menschlich bedingt.

Absichtliche Ursache

Jemand zapft Kommunikationsgeräte oder -träger an oder befindet sich im

	Sendebereich einer Kommunikation.In diesem Fall werden kostengünstige Mittel eingesetzt, um umlaufende Informationen (Stimme oder Daten) abzuhören, abzuspeichern und auszuwerten. Beispiele ---------- Sowohl über Funk als auch über Leitungen gesendete Signale können abgefangen werden. Das Abfangen geschieht dann über Sensoren (oder bei Funksignalen über eine Antenne). Auch Infrarot-Kommunikationen können abgefangen werden. Bei einem angeschlossenen Datenträger kann das bereits an das Netz angeschlossene Gerät (z. B. eine an ein lokales Netz angeschlossene Arbeitsstation) zur Abspeicherung und Analyse umlaufender Informationen benutzt werden (z. B. mit einem Server ausgetauschte Informationen). Zahlreiche handelsübliche Apparate erleichtern die Analyse und ermöglichen es, die Datenübertragungsblöcke unabhängig vom benutzten Kommunikationsprotokoll in Echtzeit zu interpretieren. Mögliche Konsequenzen ---------- Verbreitung einer auf einem Kommunikationsträger umlaufenden Information.
Verletzungen	Vertraulichkeit

20 - DIEBSTAHL VON DATENTRÄGERN ODER UNTERLAGEN

Beschreibung	Typ ------- Menschlich bedingt. Absichtliche Ursache ---------- Eine institutionsinterne oder externe Person verschafft sich Zugang zu den digitalen Datenträgern oder zu gedruckten Dokumenten, mit dem Ziel, diese zu entwenden und die darauf befindlichen Informationen auszuwerten. Beispiele ---------- Diebstahl von Disketten, CD-Roms, Cartridges, Speicherkassetten. Diebstahl von Akten, Notizen, Plänen, Berichten. Diebstahl von Ausgaben, die eine Weile im Drucker z. B. eines Großraumbüros gelegen haben. Durchsuchen von Papierkörben oder auf der Straße abgestellten Mülltonnen. Mögliche Konsequenzen ---------- Verbreitung von Informationen (Informationsbestand, Passwörter).
Verletzungen	Vertraulichkeit

21 - DIEBSTAHL VON BETRIEBSMITTELN

Beschreibung	Typ ------ Menschlich bedingt. Absichtliche Ursache ---------- Eine institutionsinterne oder externe Person verschafft sich aus Habgier oder aus strategischen Beweggründen Zugang zu Betriebsmitteln, die sich innerhalb oder außerhalb der Institution befinden. Beispiele ---------- Diebstahl eines Laptops für den Wiederverkauf, Diebstahl eines PDA zur

	Auswertung des Inhalts. Mögliche Konsequenzen --- Nicht-Verfügbarkeit von Informationen und/oder Funktionen (z. B. tragbares Gerät für Wartungszwecke). Verbreitung von im Gerät gespeicherten Informationen (z. B.: Passwörter, Auszüge des Informationsbestandes). Finanzielle Verluste.
Verletzungen	Vertraulichkeit Verfügbarkeit

22 - ÜBERNAHME RECYCELTER ODER AUSGEMUSTERTER DATENTRÄGER

Beschreibung	Typ --- Menschlich bedingt. Unabsichtliche Ursache --- Übernahme von elektronischen Informationsträgern (Festplatten, Disketten, Speicherkassetten, USB-Schlüssel, ZIP-Disketten, externen Festplatten usw.) oder von Papier (Listen, unvollständige Textausgaben, Nachrichten usw.), die zum Recycling bestimmt sind und wieder verwendbare Informationen enthalten. Beispiel --- Weitergabe ausgemusterter Rechner an andere Benutzer der gleichen Institution, an Schulen oder an andere Institutionen, ohne dass die Festplatten formatiert wurden. Wiederverwendung von Papier als Konzeptpapier innerhalb oder außerhalb der Institution. Absichtliche Ursache --- Eintreibung von elektronischen Informationsträgern (Festplatten, Disketten, Speicherkassetten, USB-Schlüssel, ZIP-Disketten, externen Festplatten usw.) oder von Papier (Listen, unvollständige Textausgaben, Nachrichten usw.), die zum Recycling bestimmt sind und wieder verwendbare Informationen enthalten.Beispiel----------Durchsuchen von Papierkörben oder auf der Straße abgestellten Mülltonnen. Mögliche Konsequenzen --- Imageverlust. Verbreitung von Informationen.
Verletzungen	Vertraulichkeit

23 - VERBREITUNG

Beschreibung	Typ --- Menschlich bedingt. Unabsichtliche Ursache --- Eine institutionsinterne Person gibt durch Nachlässigkeit eine Information an andere, von dieser Information nicht betroffene institutionsinterne Personen oder an Außenstehende weiter (wobei die Konsequenzen bei Außenstehenden in der Regel schlimmer sind). Beispiele ---

	Falsch eingegebene Empfängeradressen bei Übermittlung von Nachrichten. Nachkommen von Aufforderungen ohne Überprüfung ihrer Herkunft (Abfrage von Passwörtern in böswilliger Absicht). Unkenntnis der in der Institution geltenden Vorschriften zur Verbreitung von Informationen. Nachlässigkeit bei der Definition von Vorschriften bezüglich der Zugriffskontrolle gemeinsam genutzter Informationen. Nicht-Einhaltung elementarer Grundregeln der Zurückhaltung (Gespräche oder Lesen von Dokumenten in der Öffentlichkeit). Absichtliche Ursache --- Jemand gibt absichtlich eine Information innerhalb der Institution an andere, von dieser Information nicht betroffene Personen oder an Außenstehende weiter (wobei die Konsequenzen bei Außenstehenden in der Regel schlimmer sind). Beispiele --- Jemand verbreitet aus Rache vertrauliche Informationen per E-Mail. Jemand verbreitet Informationen, weil ihm seiner Meinung nach die Kenntnis sensitiver Informationen eine gewisse Macht über andere verleiht. Verbreitung von Informationen an Dritte unter dem Druck einer Erpressung. Finanzielle Ausnutzung industrieller oder kommerzieller Informationen (Industrie-Spionage). Mögliche Konsequenzen --- Verletzung der Privatsphäre der Benutzer. Verbreitung des Informationsbestandes. Finanzielle Verluste.
Verletzungen	Vertraulichkeit

24 - INFORMATIONEN OHNE HERKUNFTSGARANTIE

Beschreibung	Typ --- Menschlich bedingt. Unabsichtliche Ursache --- Empfang und Nutzung im Informationssystem der Institution von externen fehlerhaften Daten oder nicht angepassten Betriebsmitteln. Beispiele --- Informationen, die von einem Diskussionsforum stammen. Herunterladen von Updates über fremde Webseiten außerhalb des Verantwortungsbereichs des jeweiligen Herausgebers. Erhalt einer Information ohne Identifikation, Authentifizierung des Absenders, z. B. Empfang einer elektronischen Mitteilung, die mit einer allgemeinen Firmenidentifikation versandt wurde (Unterlage@Firma.com). Absichtliche Ursache --- Jemand übermittelt falsche Informationen, die dazu bestimmt sind, in das Informationssystem eingeschleust zu werden, um dem Empfänger eine falsche Information zuzuspielen und die Zuverlässigkeit des Systems bzw. die Gültigkeit der enthaltenen Informationen zu beeinträchtigen. Beispiele --- Übertragung einer Falschmeldung ("Hoax") via elektronische Nachrichtenübermittlung.

	Jemand übermittelt Daten und weist sich als legitime Quelle aus. Mögliche Konsequenzen --- Manipulation von Daten bzw. Datenverarbeitungen. Unnötige Inanspruchnahme von Arbeitskraft. Imageverlust
Verletzungen	Integrität Verfügbarkeit

25 - SABOTIEREN DER HARDWARE

Beschreibung	Typ --- Menschlich bedingt. Absichtliche Ursache --- Jemand verschafft sich Zugang zu einem Kommunikationsträger oder Gerät, um dort einen Schnüffel- oder Zerstörungsmechanismus zu installieren. Beispiele --- Einschieben einer Karte in einen Laptop während des Transports. Einbau eines Mikrofons in ein Gerät. Abzweigung von Kommunikationskanälen (Stimme oder Daten). Sabotage einer Schutzvorrichtungsfunktion, um diese außer Kraft setzen und einen Angriff durchführen zu können. Mögliche Konsequenzen --- Verbreitung von Informationen außerhalb der Institution. Zerstörung von Betriebsmitteln während einer kritischen Phase. Unwirksamkeit einer Schutzfunktion.
Verletzungen	Vertraulichkeit

26 - SABOTIEREN DER SOFTWARE

Beschreibung	Typ --- Menschlich bedingt / Umgebungsbedingt. Unabsichtliche Ursache --- Unabsichtliche Aktion, die innerhalb oder außerhalb der Institution mit Software-Mitteln eingeleitet wurde und eine Beeinträchtigung bzw. Zerstörung von Programmen oder Daten zur Folge hat, den korrekten Betrieb des Betriebsmittels verhindert oder gar Befehle im Namen der Benutzer ausführt, ohne dass diese davon Kenntnis haben. Beispiele --- Ein Benutzer schließt an das Netz einen mit einem Virus infizierten Laptop an, wobei sich der Virus bei einem Austausch mit einer anderen Institution eingeschlichen hat. Ein Benutzer des Informationssystems empfängt einem Wurm von außen und verbreitet diesen, ohne sein Wissen, innerhalb der Institution. Absichtliche Ursache --- Ein Hacker schleust ein Programm bzw. Befehle ein, die das Verhalten eines Softwareprogramms verändern oder dem Betriebssystem einen unerlaubten Dienst hinzufügen sollen. Dieses bedrohende Element kann während allen

	Phasen vom Entwurf über die Vorserie, die Serienfertigung, den Betrieb, den Transport bis hin zur Wartung des Informationssystems zum Einsatz kommen. Beispiele --- Jemand lässt unter Vortäuschung einer zulässigen Aktion einen Benutzer ein Programm ausführen, das versteckte Funktionen enthält, die in der Lage sind, die Sicherheitspolitik zu durchkreuzen (Trojanisches Pferd). Zur Einschleusung eines Befehls koppelt ein Programmierer zur Ausführung einer unzulässigen Aktion eine logische Bombe an ein Programm, wobei der Befehl i. d. R. an ein auslösendes Ereignis (Datum, kontextuelles Ereignis) gebunden ist. Mögliche Konsequenzen --- Intrusion. Störung des geordneten Betriebs. Zerstörung von Daten. Manipulation der Software.
Verletzungen	Integrität Vertraulichkeit Verfügbarkeit

27 - GEOLOKALISATION

Beschreibung	Typ --- Menschlich bedingt. Absichtliche Ursache --- Jemand verschafft sich Zugang zu Mitteln, mit denen er einen Benutzer eines Informationssystems lokalisieren kann. Beispiele --- Zugang zu Eingangs-/Ausgangsregistern. Zugang zu Ticketbestellungen. Benutzung von Mobilfunkantennen zur Lokalisierung einer bestimmten Person. Mögliche Konsequenzen --- Ausnutzung von Informationen, um gezielte Angriffe durchzuführen.
Verletzungen	Vertraulichkeit

Thema 6 – Technische Störungen

28 - AUSFALL VON BETRIEBSMITTELN

Beschreibung

Typ

Menschlich bedingt / Natürlich bedingt.

Unabsichtliche Ursache

Ein Ereignis bewirkt den Ausfall eines Betriebsmittels.

Beispiele

Verschleiß, Alterung, Wartungsfehler oder unsachgemäßer Gebrauch (z. B. schlechte Dimensionierung, Betrieb außerhalb der tolerierten Betriebsbedingungen) bewirken einen Ausfall.

Mögliche Konsequenzen

Nicht-Verfügbarkeit eines Gerätes.
Beeinträchtigung oder Verlust von Informationen.

Verletzungen

Verfügbarkeit

29 - FEHLERHAFTER BETRIEB VON BETRIEBSMITTELN

Beschreibung

Typ

Menschlich bedingt / Natürlich bedingt.

Unabsichtliche Ursache

Ein logisches oder physisches Ereignis bewirkt einen fehlerhaften Betrieb des Betriebsmittels.

Beispiele

Nicht-Einhalten der Qualifikationsprozeduren für ein Gerät in Folge von Weiterentwicklungen oder Nacharbeiten.
Unabsichtliche Beschädigung eines Gerätes.
Benutzung des Gerätes unter Bedingungen jenseits der tolerierten Grenzbedingungen (Temperatur, Feuchtigkeit).
Verschleiß, Alterung des Materials.

Mögliche Konsequenzen

Unterbrechung des Betriebs eines Gerätes, was durch Seiteneffekt die Nicht-Verfügbarkeit des gesamten Informationssystems bewirken kann.

Verletzungen

Verfügbarkeit

30 - ÜBERLASTUNG DES INFORMATIONSSYSTEMS

Beschreibung

Typ

Menschlich bedingt.

Unabsichtliche Ursache

Die Betriebsmittel (Hardware, Software, Netzwerk) reichen nicht mehr aus, um den Anforderungen der Benutzer gerecht zu werden.

Beispiele

	---------- Überschreitung der Speicherkapazitäten (z. B. Speicherplatzbedarf, Mailbox-Speicher, Arbeitsspeicher usw.); beispielsweise Überlastung der Mailbox bei längerer Abwesenheit des Inhabers. Überlastung auf Grund intensiver Inanspruchnahme der Anlage (zahlreiche Anfragen zur gleichen Zeit). Schlechte Dimensionierung der Geräte (Wechselrichter, Kommunikationskanäle usw.). Absichtliche Ursache ---------- Jemand gibt einen intensiven Bedarf an einem Betriebsmittel vor und provoziert dadurch eine intensive und dauerhafte Störung des Betriebsmittels. Beispiele ---------- Aufgabe einer sehr großen Anzahl gleichzeitiger Bestellungen. Absichtliche Überlastung der Speicher zur Speicherung der Aktivitäten- oder Anwendungsprotokolle des Systems mit dem Ziel, die Realisierung unzulässiger Operationen zu verschleiern. Mögliche Konsequenzen ---------- Stillstand mit vorübergehender Nicht-Verfügbarkeit des Dienstes. Informationsverlust.
Verletzungen	Verfügbarkeit

31 - FEHLERHAFTER BETRIEB VON SOFTWAREPROGRAMMEN

Beschreibung	Typ ------- Menschlich bedingt / Umgebungsbedingt. Unabsichtliche Ursache ---------- Ein Konzeptionsfehler, Installationsfehler oder eine Nachlässigkeit bei Durchführung einer Änderung verhindern einen konformen Betrieb. Beispiele ---------- Ein Implementierungsfehler bewirkt eine fehlerhafte Verarbeitung der Daten. Die Installation von Softwareprogrammen verursacht Seiteneffekte. Nicht-Einhalten der Installations- oder Betriebsprozeduren. Nachlässigkeit bei Wartungsaktionen. Mögliche Konsequenzen ---------- Dienstunterbrechung. Betriebsstörungen. Störungen bei der Datenerzeugung.
Verletzungen	Integrität Verfügbarkeit

32 - BEEINTRÄCHTIGUNG DER WARTBARKEIT DES INFORMATIONSSYSTEMS

Beschreibung	Typ ------ Menschlich bedingt / Umgebungsbedingt. Unabsichtliche Ursache ---------- Eine fehlende Systembeherrschung macht jegliche Aktualisierung oder Weiterentwicklung unmöglich, z. B. um eine Anomalie beseitigen oder um neuen

	Bedürfnissen gerecht werden zu können. Beispiele --- Ausfall der Hard-/Software-Lieferanten. Ausfall von mit der Software- und Hardware-Wartung beauftragten Drittfirmen, Auslaufen eines Dienstleistungsvertrages mit der Folge, dass die Kompetenzen oder Mittel fehlen, um die Weiterentwicklung des Systems gewährleisten zu können. Zahlreiche, am System durchgeführte Änderungen machen die Instandhaltung schwierig oder sogar unmöglich, es wird ständig Gefahr gelaufen, Seiteneffekte infolge einer Modifikation zu provozieren. Absichtliche Ursache --- Jemand erschwert oder verhindert jegliche Aktualisierung des Systems. Beispiele --- Jemand hinterlässt aus Rache keinerlei Spuren oder Hilfen zur Instandhaltung des Systems (gewollte Undurchsichtigkeit). Mögliche Konsequenzen --- Längere Dienstunterbrechung. Beeinträchtigung der Betriebssicherheit. Finanzielle Verluste durch Austausch der Betriebsmittel bzw. der Lieferanten.
Verletzungen	Verfügbarkeit

Thema 7 – Widerrechtliche Aktionen

33 - UNZULÄSSIGE BENUTZUNG DER BETRIEBSMITTEL

Beschreibung

Typ

Menschlich bedingt.

Absichtliche Ursache

Eine institutionsinterne oder externe Person verschafft sich Zugang zum Informationssystem, indem sie einen der angebotenen Dienste in Anspruch nimmt, um sich einzuschleichen, Aktionen auszuführen oder Informationen zu entwenden.

Beispiele

Entwendung von Identifikations-/Authentifizierungsdaten eines autorisierten Benutzers, um sich dessen Rechte anzueignen; Umgehung der Zugangskontrollen; autorisierter Zugang zu den geschützten Bereichen durch Ausnutzung von Schwachstellen der installierten Schutzmechanismen.
Untersuchung und Suche nach Informationen mit Hilfe von residuellen Daten auf elektronischen Datenträgern (Datei im Cache-Speicher, Datenreste auf Festplatten, Kontextspeicherungen - Rücksetzpunkt nach Zwischenfällen - mit Informationen über den Zustand des Systems, die von einem erfahrenen Hacker ausgewertet werden können).
Simulation des Verhaltens einer Maschine, um einen legitimen Benutzer zu täuschen und sich dessen Namen und Passwort anzueignen.
Absichtliche Änderung oder Zerstörung von Daten.

Mögliche Konsequenzen

Intrusion in das Informationssystem.
Verbreitung von Informationen.

Verletzungen

Integrität
Vertraulichkeit
Verfügbarkeit

34 - BETRÜGERISCHE KOPIE VON SOFTWAREPROGRAMMEN

Beschreibung

Typ

Menschlich bedingt.

Absichtliche Ursache

Institutionsinterne Person fertigen Piratenkopien (auch sklavische Kopien genannt) von "hauseigenen" Softwareprogrammen und Programmpaketen an.

Beispiele

Kopie institutionseigener Software aus Spielerei, Rache (Verbreitung über das Internet) oder Habgier (Verkauf).

Mögliche Konsequenzen

Finanzielle Verluste.
Imageverlust.

Verletzungen

Vertraulichkeit

35 - BENUTZUNG GEFÄLSCHTER ODER KOPIERTER SOFTWAREPROGRAMME

Beschreibung	Typ ------ Menschlich bedingt / Umgebungsbedingt. Unabsichtliche Ursache ---------- Verlust oder Vernichtung von Lizenz-Belegen oder Nachlässigkeit beim Einsatz von Softwareprogrammen (fehlende Quittierung bestimmter Rechte). Beispiele ---------- Ein Schadensfall hat die Vernichtung der Kaufbelege verursacht. Eine Zusammenstellung aller benutzten Lizenzen erweist sich als unmöglich. Absichtliche Ursache ---------- Ein institutionsinterne Person benutzt auf unzulässige Art ein kopiertes Softwareprogramm. Beispiele ---------- Kopie von Programmen ohne Lizenz, um innerhalb der Institution zulässige Arbeiten auszuführen. Mögliche Konsequenzen ---------- Nicht-Einhalten der Rechtsvorschriften. Imageverlust.
Verletzungen	Verfügbarkeit

36 - DATENMANIPULATION

Beschreibung	Typ ------- Menschlich bedingt. Absichtliche Ursache ---------- Jemand verschafft sich Zugang zu den Kommunikationsmitteln des Informationssystems und manipuliert die Datenübertragung (durch Abfangen, Einschleusen, Beseitigen) oder erprobt solange die Zugänge, bis er einen autorisierten Zugang gefunden hat. Beispiele ---------- Beseitigung, Einschleusung, Änderung von Mitteilungen (Abänderung einer Information, Umgestaltung der Information innerhalb einer Mitteilung oder Umgestaltung der Reihenfolge der Mitteilungen). Dienstverweigerung (zeitliche Verlegung einer Mitteilung). Abtasten der IP-Adressen von außen, bis eine Adresse gefunden wird, die Zugang zum Informationssystem verschafft. Mögliche Konsequenzen ---------- Intrusion. Manipulation von Kommunikationen.
Verletzungen	Integrität Vertraulichkeit

37 - UNZULÄSSIGE VERARBEITUNG VON DATEN

Beschreibung	Typ -------

	Menschlich bedingt. Absichtliche Ursache --- Jemand bearbeitet Informationen auf eine Art, die durch gesetzliche Verordnung oder durch Vorschriften untersagt ist. Beispiele --- Einrichtung oder Nutzung nicht deklarierter personenbezogener Dateien (unzulässige Protokolldatenauswertung). Durchführung unzulässiger Operationen in deklarierten personenbezogenen Dateien wie z. B. das Zusammenstellen mehrerer Dateien. Verschlüsselung von Daten aus Gründen der Vertraulichkeit unter Benutzung langer Schlüssel ohne vorherige Autorisierung. Unzulässige Manipulation von Daten eines recycelten Rechners. Mögliche Konsequenzen --- Verletzung der Privatsphäre der Benutzer. Gerichtliche Verfolgung und (Geld-)Strafen
Verletzungen	Vertraulichkeit

Thema 8 – Infragestellung von Funktionen

38 - BENUTZUNGSFEHLER

Beschreibung

Typ

Menschlich bedingt.

Unabsichtliche Ursache

Jemand begeht einen Bedienungs-, Eingabe- oder Benutzungsfehler (Hard- oder Software).

Beispiele

Datenverlust infolge eines Fehlers bei der Abspeicherung.
Nicht-Einhalten der Installations- oder Betriebsprozeduren.
Eingabe zahlreicher verschlüsselter Daten durch Operatoren.
Nachlässigkeit bei der Parametrierung eines Schutzprogramms.
Fehlerhafte Eingabe einer Empfängeradresse einer elektronischen Nachricht.

Mögliche Konsequenzen

Dienstunterbrechung.
Datenverfälschung.
Fehlerhafter Betrieb, Leistungsverlust der Schutzvorrichtungen, Hinzufügen zusätzlicher Schwachstellen.
Unabsichtliche Verbreitung von Daten.

Verletzungen

Integrität
Vertraulichkeit
Verfügbarkeit

39 - RECHTSMISSBRAUCH

Beschreibung

Typ

Menschlich bedingt.

Unabsichtliche Ursache

Jemand mit privilegierten Zugriffsrechten (Netzadministrator, Informatiker) kann Betriebsparameter ändern, ohne die Benutzer davon in Kenntnis zu setzen.

Beispiele

Anlegen neuer Systemzugriffe ohne Berücksichtigung der Datenschutzbedürfnisse der von den Benutzern gespeicherten Daten.
Unterbrechung der Speicherprozedur ohne Benachrichtigung der Benutzer.
Änderung von Konfigurationsparametern der Server, wodurch Seiteneffekte und ein fehlerhafter Betrieb verursacht werden.

Absichtliche Ursache

Jemand verschafft sich Zugang zum System, um Betriebsparameter zu ändern, zu löschen oder hinzuzufügen oder um eine beliebig andere unzulässige Aktion durchzuführen, zu der er auf Grund seiner Zugriffsrechte in der Lage ist.

Beispiele

Ein Administrator ändert die Passwörter der Benutzer.
Ein Wartungstechniker verändert die Funktionsweise von Sicherheitsmechanismen, um sich Zugang zu geschützten Informationen zu

	verschaffen. Löschung der Ereignisprotokolle auf den Anwendungsservern. Mögliche Konsequenzen ---------- Betriebsstörungen. Verbreitung von Informationen. Informationsverlust.
Verletzungen	Integrität Vertraulichkeit Verfügbarkeit

40 - RECHTSANMASSUNG

Beschreibung	Typ ------- Menschlich bedingt. Absichtliche Ursache ---------- Jemand gibt sich als jemand anderes aus, um sich mit dessen Zugriffsprivilegien Zugang zum Informationssystem zu verschaffen, den Empfänger falsch zu informieren, eine betrügerische Tat auszuführen usw.. Beispiele ---------- Jemand gibt sich als Benutzer aus und bittet den Administrator um Freigabe des Zugangs infolge eines verlorenen Passwortes. Jemand nimmt den Platz eines Benutzers ein und profitiert von der offen gelassenen Sitzung. Mögliche Konsequenzen ---------- Intrusion.
Verletzungen	Integrität Vertraulichkeit Verfügbarkeit

41 - VERLEUGNUNG VON AKTIONEN

Beschreibung	Typ ------- Menschlich bedingt. Absichtliche Ursache ---------- Eine Einzelperson oder eine Einheit leugnet die Teilnahme an einem Austausch mit einem Dritten oder an der Realisierung einer bestimmten Aktion. Beispiele ---------- Jemand leugnet, eine bestimmte Nachricht empfangen oder gesendet zu haben oder gibt vor, eine andere Nachricht (Datei) gesendet (empfangen) zu haben oder gibt an, eine bestimmte Aktion niemals durchgeführt zu haben. Mögliche Konsequenzen ---------- Mangelnde Beweise.
Verletzungen	Integrität

42 - BEEINTRÄCHTIGUNG DER PERSONALVERFÜGBARKEIT

Beschreibung	Typ

	------ Menschlich bedingt / Umgebungsbedingt. Unabsichtliche Ursache ---------- Mangel an qualifiziertem oder befugtem Personal auf Grund einer Verhinderung, die außerhalb des Verantwortungsbereichs der betroffenen Personen liegt. Beispiele ---------- Krankheit, Todesfall, Streik der Verkehrsbetriebe. Absichtliche Ursache ---------- Absichtliches Fernbleiben qualifizierter bzw. ermächtigter Mitarbeiter. Beispiele ---------- Durch die Institution nicht genehmigter Streik, nicht genehmigter Urlaub. Mögliche Konsequenzen ---------- Stillstand, Störung der Dienstleistung.
Verletzungen	Verfügbarkeit

4 Schwachstellen Vorspanne

Die Schwachstellen werden nach Angriffsmethoden sortiert, die betroffenen Entitätstypen und untertypen werden vorgestellt. Die Entitätsuntertypen sind den gleichen Schwachstellen ausgesetzt, wie die entsprechenden Entitätstypen.

4.1 BRAND

Einzelexemplar der Lizenzverträge	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Intern entwickelte Einzelanwendungen	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
Benutzungsbedingungen außerhalb der tolerierten Betriebsbedingungen der Betriebsmittel	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware
Fehlende Ersatz-Betriebsmittel	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Betriebsmittel in Kontakt mit brennbaren Stoffen (z. B. stauberzeugende Massendrucker)	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Datensicherung auf Datenträgern	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Original-Datenträger	
Entitätstypen	MAT_PAS.2: Sonstige Datenträger
Fehlender Versicherungsschutz bei schweren Schadensfällen	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation
Fehlende Standorterkundung durch die Rettungsdienste (Feuerwehr)	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Normen beim Einrichten institutionseigener Standorte	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln zur Sicherstellung der Aktivitäten bei Krisensituationen beim Lieferanten	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Weitergabe von Sicherheitsanweisungen an externes Personal	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle

Fehlende Verwaltung der Prüfberichte, die die Sicherheitsausrüstung betreffen	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Aushängung gültiger Anweisungen zur Benachrichtigung der Rettungsdienste	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Brandschutzorganisation (Festlegung der Rollen, Verantwortungen)	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Aktualisierung der Verträge zur Wartung der Brandschutzeinrichtungen	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Krisenmanagementorganisation	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfal	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Sensibilisierung für den Schutz von Sicherheitseinrichtungen	
Entitätstypen	PER_DEC: Entscheidungsträger
Konfliktgeladenes soziales Klima	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Bestehende Öffnungen zur Straße hin (Fenster)	
Entitätstypen	PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Veraltete Räumlichkeiten	
Entitätstypen	PHY_LIE.2: Räumlichkeiten
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten	
Entitätstypen	PHY_LIE.2: Räumlichkeiten
Fehlende Brandschutz-Zwischenwände	
Entitätstypen	PHY_LIE.2: Räumlichkeiten
Während der Installationsphase, fehlende Berücksichtigung der besonderen, an die vorhandene Ausstattung gebundenen Brandrisiken	
Entitätstypen	PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE.3: Zone
Fehlende, falsch dimensionierte oder unangepasste automatische Brandlöscheinrichtung	
Entitätstypen	PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE.3: Zone
Fehlende Wartung der Klimatisierungssysteme	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung

DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 01 - BRAND

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.2 WASSERSCHÄDEN

Einzelexemplar der Lizenzverträge	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Intern entwickelte Einzelanwendungen	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
Fehlende Ersatz-Betriebsmittel	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Datensicherung auf Datenträgern	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Original-Datenträger	
Entitätstypen	MAT_PAS.2: Sonstige Datenträger
Fehlender Versicherungsschutz bei schweren Schadensfällen	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation
Fehlende Normen beim Einrichten institutionseigener Standorte	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Weitergabe von Sicherheitsanweisungen an externes Personal	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Verwaltung der Prüfberichte, die die Sicherheitsausrüstung betreffen	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Aushängung gültiger Anweisungen zur Benachrichtigung der Rettungsdienste	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Anweisungen bezüglich der Alarmierung, des Verhaltens und der Unterrichtung bei Wasserschäden (fehlende Ausweisung der Sperrventile usw.)	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Garantie für den korrekten Betrieb der Wasserdetektoren	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Krisenmanagementorganisation	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfall	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Kenntnis der Sicherheitsmaßnahmen	

Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Sensibilisierung für den Schutz von Sicherheitseinrichtungen	
Entitätstypen	PER_DEC: Entscheidungsträger
Konfliktgeladenes soziales Klima	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Standort in einem Überflutungsbereich	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Fehlende physische Zugangskontrolle zu den Räumlichkeiten	
Entitätstypen	PHY_LIE.2: Räumlichkeiten
Undichte Öffnungen nach außen	
Entitätstypen	PHY_LIE.2: Räumlichkeiten
Vorhandensein einer Wasserlöscheinrichtung	
Entitätstypen	PHY_LIE.2: Räumlichkeiten
Undichte Decke oder Öffnungen nach außen	
Entitätstypen	PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE.3: Zone
Fehlende Ausweisung der Wasserabsperrventile	
Entitätstypen	PHY_LIE.3: Zone
Ungeschützter Zugang	
Entitätstypen	PHY_LIE.3: Zone
Wasserleitung in unmittelbarer Nähe der Systemausstattung	
Entitätstypen	PHY_LIE.3: Zone
Vorhandensein einer Wasserlöscheinrichtung	
Entitätstypen	PHY_LIE.3: Zone
Wasserleitung in unmittelbarer Nähe der Endgeräte	
Entitätstypen	PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE.3: Zone
Fehlende Abfallschächte	
Entitätstypen	PHY_LIE.3: Zone
Ungeschützter Zugang zu den Räumlichkeiten, in denen sich die Einrichtungen zur Produktion bzw. zur Erbringung der wesentlichen Dienste befinden	
Entitätstypen	PHY_SRV.2: Energie PHY_SRV.1: Kommunikation
Unter-Boden-Verkabelung	
Entitätstypen	PHY_SRV.2: Energie PHY_SRV.1: Kommunikation
Veraltete Kühlkanäle	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung
Fehlende Wartung der Klimatisierungssysteme	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung
Fehlendes Wasserabsperrventil	

Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung

DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 02 - WASSERSCHÄDEN

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.3 VERSCHMUTZUNG

Einzelexemplar der Lizenzverträge	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Intern entwickelte Einzelanwendungen	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
Empfindlichkeit des Datenträgers bei schlechten Aufbewahrungsbedingungen	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Fehlende Normen beim Einrichten institutionseigener Standorte	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Aktualisierung der Wartungsverträge	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Maßnahmen bei Ausfall der Klimatisierungssysteme	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfall	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Sensibilisierung für den Schutz von Sicherheitseinrichtungen	
Entitätstypen	PER_DEC: Entscheidungsträger
Konfliktgeladenes soziales Klima	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Unmittelbare Nähe zu Verschmutzungsquellen (akustische Quelle, Rauch, Dampf usw.)	
Entitätstypen	PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung
Verschmutzte Atmosphäre (Lagerhalle, Werkstatt usw.)	
Entitätstypen	PHY_LIE.2: Räumlichkeiten
Fehlende Wartung der Klimatisierungssysteme	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung
Fehlendes, ausreichend bemessenes redundantes Material	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung
Veraltete Filter der Klimatisierungssysteme	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung
Ungeschützter Zugang zur Systemausstattung	

Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung

DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 03 - VERSCHMUTZUNG

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.4 GRÖSSERER SCHADENSFALL

Einzelexemplar der Lizenzverträge	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Intern entwickelte Einzelanwendungen	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
Fehlende Ersatz-Betriebsmittel	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Datensicherung auf Datenträgern	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Original-Datenträger	
Entitätstypen	MAT_PAS.2: Sonstige Datenträger
Fehlender Notdienst in unmittelbarer Umgebung der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Normen beim Einrichten institutionseigener Standorte	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Aushängung gültiger Anweisungen zur Benachrichtigung der Rettungsdienste	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlender Versicherungsschutz bei schweren Schadensfällen	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Krisenmanagementorganisation	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Prozeduren zum Management von Notsituationen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung
Mögliche Zerstörung infolge eines externen Ereignisses (Kollisionen, Attentate)	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Unmittelbare Nähe zu einem Gebiet mit industrieller Tätigkeit oder zu einem Risikogebiet	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Räumlichkeiten ohne Berücksichtigung der Explosions-/Implosionsgefahr	

Entitätstypen	PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten

DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 04 - GRÖSSERER SCHADENSFALL

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.5 ZERSTÖRUNG VON BETRIEBSMITTELN ODER DATENTRÄGER

Einzelexemplar der Lizenzverträge	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Intern entwickelte Einzelanwendungen	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
Fehlende Ersatz-Betriebsmittel	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Empfindlichkeit der Betriebsmittel	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Zugänglichkeit der Betriebsmittel durch Fremde (Nicht-Eigentümer) (z. B. Unterbringung an einem Ort mit Publikumsverkehr)	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Zugänglichkeit der Datenträger durch Fremde (Nicht-Eigentümer)	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Fehlende Prozedur zur Archivierung	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Empfindlichkeit der Datenträger	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Fehlende Maßnahmen zur Konservierung der Archive unter Berücksichtigung der Aufbewahrungsfristen (Alterung der Bänder, Abnutzung der CD-Roms usw.)	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Fehlende Datensicherung auf Datenträgern	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Original-Datenträger	
Entitätstypen	MAT_PAS.2: Sonstige Datenträger
Fehlende Weitergabe von Sicherheitsanweisungen an externes Personal	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlender Versicherungsschutz bei Zerstörung von Betriebsmitteln	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Vorschriften über Gebrauch und Aufbewahrung von Betriebsmitteln und Datenträgern (Schutzmaßnahmen beim Transport, Rauchverbot usw.)	

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Konfliktgeladenes soziales Klima	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Fehlende Sensibilisierung für den physischen Schutz der Systemausstattung	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten oder Eindringen über indirekte Zugänge möglich	
Entitätstypen	PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung
Ungeschützter physischer Zugang zu den Räumlichkeiten, in denen sich die Betriebsmittel oder Datenträger befinden	
Entitätstypen	PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE.3: Zone
Datenträger sind unbefugten Personen zugänglich	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
Unter Boden verlegte, nicht gekennzeichnete Informationsträger	
Entitätstypen	RES_INF: Medien und Informationsträger
Zugänglichkeit der Systemausstattung durch unbefugte Personen	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Empfindlichkeit der Systemausstattung	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 05 – ZERSTÖRUNG VON BETRIEBSMITTELN ODER DATENTRÄGERN	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie

	PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.6 KLIMATISCHES PHÄNOMEN

Fehlende Normen beim Einrichten institutionseigener Standorte	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlender Notdienst in unmittelbarer Umgebung der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfall	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Fehlende Belüftungs- oder Klimatisierungsmittel bei exzessiver Sommerhitze	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Keine Berücksichtigung der klimatischen Bedingungen bei Konstruktion der Räumlichkeiten	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Nicht für Extrembedingungen ausgelegte Informationsträger oder Ausstattung (extreme Feuchtigkeit, Temperaturen oder physische Störungen)	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 06 - KLIMATISCHES PHÄNOMEN	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten

	PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.7 SEISMISCHES PHÄNOMEN

Vibrationsempfindliche Hardware	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Normen beim Einrichten institutionseigener Standorte	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlender Notdienst in unmittelbarer Umgebung der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfall	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Keine Berücksichtigung der seismischen Risiken bei Konstruktion der Räumlichkeiten	
Entitätstypen	PHY_LIE.2: Räumlichkeiten
Nicht für Extrembedingungen ausgelegte Informationsträger oder Ausstattung (extreme Feuchtigkeit, Temperaturen oder physische Störungen)	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 07 - SEISMISCHES PHÄNOMEN	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten

	PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.8 VULKANISCHES PHÄNOMEN

Fehlende Normen beim Einrichten institutionseigener Standorte	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlender Notdienst in unmittelbarer Umgebung der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfall	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Als gefährdetes Gebiet eingestufter Standort	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Keine Berücksichtigung der seismischen Risiken bei Konstruktion der Räumlichkeiten	
Entitätstypen	PHY_LIE.2: Räumlichkeiten
Nicht für Extrembedingungen ausgelegte Informationsträger oder Ausstattung (extreme Feuchtigkeit, Temperaturen oder physische Störungen)	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 08 - VULKANISCHES PHÄNOMEN	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer

	PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.9 METEOROLOGISCHES PHÄNOMEN

Benutzungsbedingungen außerhalb der tolerierten Betriebsbedingungen der Betriebsmittel	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware
Fehlender Notdienst in unmittelbarer Umgebung der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Normen beim Einrichten institutionseigener Standorte	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Tests zur Überprüfung der Reaktions- und Unterrichtungsprozeduren im Schadensfall	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Standort mit regelmäßigen extremen meteorologischen Phänomenen (Unwetter, Orkan, Zyklon usw.)	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Fehlender Blitzschutz	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Nicht für Extrembedingungen ausgelegte Informationsträger oder Ausstattung (extreme Feuchtigkeit, Temperaturen oder physische Störungen)	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 09 – METEOROLOGISCHES PHÄNOMEN	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle

RES_INF: Medien und Informationsträger
RES: Netzwerk
PHY_SRV: Wesentlicher Dienst
PHY_SRV.3: Abkühlung / Verschmutzung
PHY_SRV.2: Energie
PHY_SRV.1: Kommunikation
PHY_LIE: Orte
PHY_LIE.3: Zone
PHY_LIE.2: Räumlichkeiten
PHY_LIE.1: Äußere Umgebung
PER_UTI: Benutzer
PER_EXP: Betreiber / Wartung
PER_DEV: Entwickler
PER_DEC: Entscheidungsträger
PER: Personal
ORG_PRO: Organisation eines Projekts oder eines Systems
ORG_GEN: Organisation der Institution
ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
ORG_DEP: Organisation, von der die Institution abhängt
ORG: Organisation
MAT_PAS: Datenträger (passiv)
MAT_PAS.2: Sonstige Datenträger
MAT_PAS.1: Elektronischer Datenträger
MAT_ACT: Datenverarbeitungsmittel (aktiv)
MAT_ACT.3: Verarbeitungsperipheriegerät
MAT_ACT.2: Ortsfeste Hardware
MAT_ACT.1: Tragbare Hardware
MAT: Hardware
LOG_STD: Programmpaket oder Standard-Software
LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
LOG_OS: Betriebssystem
LOG_APP: Tätigkeitsgebundene Anwendung
LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
LOG_APP.1: Tätigkeitsgebundene Standardanwendun
LOG: Software

4.10 HOCHWASSER

Fehlender Notdienst in unmittelbarer Umgebung der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Normen beim Einrichten institutionseigener Standorte	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln im Hinblick auf Krisensituationen bei Unterauftragnehmern oder Lieferanten	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Standort in einem Überflutungsbereich	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Fehlender Schutz gegen Wasserspiegelanstieg	
Entitätstypen	PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Nicht für Extrembedingungen ausgelegte Informationsträger oder Ausstattung (extreme Feuchtigkeit, Temperaturen oder physische Störungen)	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 10 - HOCHWASSER	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt

	ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.11 AUSFALL DER KLIMATISIERUNGSSYSTEME

Zu klimatisierende Betriebsmittel	
Entitätstypen	MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware
Zu klimatisierende Archive	
Entitätstypen	MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Fehlende Normen beim Einrichten institutionseigener Standorte	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln über die maximal zulässige Unterbrechungsdauer bei Erbringung eines wesentlichen Dienstes	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Vertragsklauseln über Schadensersatz bei Nicht-Erbringung eines wesentlichen Dienstes	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Nachkontrolle der Klimatisierungsbedürfnisse nach Umbau oder Hinzufügung von Betriebsmitteln	
Entitätstypen	PHY_LIE.3: Zone
Von Kaltwasserzufuhr oder Nahrungsmittelbelieferung abhängiges Gerät	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung
Den Bedürfnissen nicht angepasste Einrichtung	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung
Fehlende Wartung der Klimatisierungssysteme	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung
Fehlendes, ausreichend bemessenes redundantes Material	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung
Ungeschützter Zugang zu den Wasser- und Stromversorgungseinrichtungen	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 11 – AUSFALL DER KLIMATISIERUNG	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung

PHY_SRV.2: Energie
PHY_SRV.1: Kommunikation
PHY_LIE: Orte
PHY_LIE.3: Zone
PHY_LIE.2: Räumlichkeiten
PHY_LIE.1: Äußere Umgebung
PER_UTI: Benutzer
PER_EXP: Betreiber / Wartung
PER_DEV: Entwickler
PER_DEC: Entscheidungsträger
PER: Personal
ORG_PRO: Organisation eines Projekts oder eines Systems
ORG_GEN: Organisation der Institution
ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
ORG_DEP: Organisation, von der die Institution abhängt
ORG: Organisation
MAT_PAS: Datenträger (passiv)
MAT_PAS.2: Sonstige Datenträger
MAT_PAS.1: Elektronischer Datenträger
MAT_ACT: Datenverarbeitungsmittel (aktiv)
MAT_ACT.3: Verarbeitungsperipheriegerät
MAT_ACT.2: Ortsfeste Hardware
MAT_ACT.1: Tragbare Hardware
MAT: Hardware
LOG_STD: Programmpaket oder Standard-Software
LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
LOG_OS: Betriebssystem
LOG_APP: Tätigkeitsgebundene Anwendung
LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
LOG_APP.1: Tätigkeitsgebundene Standardanwendun
LOG: Software

4.12 AUSFALL DER ENERGIEVERSORGUNG

Störempfindliches Material (Spannungsabfälle, Überspannungen, Mikrounterbrechungen)	
Entitätstypen	RES_REL: Passives oder aktives Relais MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Normen beim Einrichten institutionseigener Standorte	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln über Schadensersatz bei Nicht-Erbringung eines wesentlichen Dienstes	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Vertragsklauseln über die maximal zulässige Unterbrechungsdauer bei Erbringung eines wesentlichen Dienstes	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Auskunft über die Benutzungsbedingungen der Notstrom-Versorgungspunkte	
Entitätstypen	PER_UTI: Benutzer
Kommunikationsendgerät ohne Notstromversorgung	
Entitätstypen	PHY_SRV.1: Kommunikation
Keine spezielle, getrennte Unterbringung säurehaltiger Batterien, sie befinden sich in den gleichen Räumlichkeiten wie das Material, an das sie angeschlossen sind	
Entitätstypen	PHY_SRV.2: Energie
Schlechte Dimensionierung der Notversorgungseinheiten (Wechselrichter, Batterien usw.)	
Entitätstypen	PHY_SRV.2: Energie
Ungeschützter physischer Zugang zu den Räumlichkeiten, in denen die Einrichtungen zur Stromversorgung und Elektrizitätsverteilung untergebracht sind	
Entitätstypen	PHY_SRV.2: Energie
Die Räumlichkeiten mit säurehaltigen Batterien werden weder mechanisch belüftet noch sind sie aus elektrischer Sicht explosionsgeschützt ausgelegt	
Entitätstypen	PHY_SRV.2: Energie
Die verschiedenen Boden- oder Wandbeläge sind nicht antistatisch	
Entitätstypen	PHY_SRV.2: Energie
Die Niederspannungsschalttafel ist nicht zugänglich	
Entitätstypen	PHY_SRV.2: Energie
Die Umspannanlage Mittelspannung / Niederspannung befindet sich außerhalb des Standorts (mit Zugangskontrolle durch den Lieferanten)	
Entitätstypen	PHY_SRV.2: Energie
Fehlende Notversorgungsleistungsanalyse, die bei Hinzufügen von Betriebsmitteln durchzuführen ist	
Entitätstypen	PHY_SRV.2: Energie
Massen und Erdungen sind nicht vorschriftsmäßig	
Entitätstypen	PHY_SRV.2: Energie

DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 12 – AUSFALL DER ENERGIEVERSORGUNG

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.13 AUSFALL DER TELEKOMMUNIKATIONSMITTEL

Über Telekommunikationsmittel ausgelagertes Material	
Entitätstypen	RES_REL: Passives oder aktives Relais MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Normen beim Einrichten institutionseigener Standorte	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln über Schadensersatz bei Nicht-Erbringung eines wesentlichen Dienstes	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Vertragsklauseln über die maximal zulässige Unterbrechungsdauer bei Erbringung eines wesentlichen Dienstes	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Anweisungen (hinsichtlich Alarmierung, Vorbeugung, Verhalten usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Wartung der Endgeräte und Verteilungseinrichtungen	
Entitätstypen	PHY_SRV.1: Kommunikation
Unsachgemäßer Betrieb des internen Telefonnetzes	
Entitätstypen	PHY_SRV.1: Kommunikation
Bereits festgestellte Funktionsstörung bei Erbringung des Telekommunikationsdienstes	
Entitätstypen	PHY_SRV.1: Kommunikation
Ungeschützter physischer Zugang zu den Räumlichkeiten, in denen die Einrichtungen zur Stromversorgung und Elektrizitätsverteilung bzw. die Telekommunikationsmittel untergebracht sind	
Entitätstypen	PHY_SRV.2: Energie PHY_SRV.1: Kommunikation
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 13 – AUSFALL DER TELEKOMMUNIKATIONSMITTEL	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung

	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.14 ELEKTROMAGNETISCHE STRAHLUNG

Elektromagnetischer oder thermischer Strahlung gegenüber empfindliche Medien und Informationsträger	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware
Fehlende Vertragsklausel bezüglich der elektromagnetischen Verträglichkeit	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Berücksichtigung der Gefahr elektromagnetischer oder thermischer Strahlung bei der Konzeption	
Entitätstypen	PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung
Unmittelbare Nähe zu einer Quelle elektromagnetischer oder thermischer Strahlung	
Entitätstypen	PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung
Keine Berücksichtigung der Risiken, die mit der Nähe einer elektromagnetischen Quelle verbunden sind	
Entitätstypen	PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation
Elektromagnetischer oder thermischer Strahlung gegenüber empfindliche Medien und Informationsträger	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 14 - ELEKTROMAGNETISCHE STRAHLUNG	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle

	ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.15 THERMISCHE STRAHLUNG

Elektromagnetischer oder thermischer Strahlung gegenüber empfindliches Material	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware
Unmittelbare Nähe zu einer Quelle elektromagnetischer oder thermischer Strahlung	
Entitätstypen	PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung
Fehlende Berücksichtigung der Gefahr elektromagnetischer oder thermischer Strahlung bei der Konzeption	
Entitätstypen	PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung
Keine Berücksichtigung der Risiken, die mit der Nähe einer elektromagnetischen Quelle verbunden sind	
Entitätstypen	PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation
Elektromagnetischer oder thermischer Strahlung gegenüber empfindliche Medien und Informationsträger	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 15 - THERMISCHE STRAHLUNG	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger

	MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.16 ELEKTROMAGNETISCHE IMPULSE

Elektromagnetischer oder thermischer Strahlung gegenüber empfindliches Material	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware
Unmittelbare Nähe zu einer Quelle elektromagnetischer oder thermischer Strahlung	
Entitätstypen	PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung
Fehlende Berücksichtigung der Gefahr elektromagnetischer oder thermischer Strahlung bei der Konzeption	
Entitätstypen	PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung
Keine Berücksichtigung der Risiken, die mit der Nähe einer elektromagnetischen Quelle verbunden sind	
Entitätstypen	PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation
Elektromagnetischer oder thermischer Strahlung gegenüber empfindliche Medien und Informationsträger	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 16 - ELEKTROMAGNETISCHE IMPULSE	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger

	MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.17 ABFANGEN VON KOMPROMITTIERENDEN STÖRSIGNALEN

Fehlende Berücksichtigung der Installationsvorschriften

Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV.2: Energie PHY_SRV.1: Kommunikation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware

Fehlende Berücksichtigung der Zoneneinteilung des Materials

Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware

Material, das möglicherweise kompromittierende Störsignale aussendet

Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware

Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten

Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt

Fehlende Vorschriften über die Anwendungspflicht von Normen

Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt

Fehlende Vertragsklauseln über von Unterauftragnehmern und Lieferanten einzuhaltende Sicherheitsmaßnahmen

Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle

Fehlende Prozedur zur Überprüfung der Betriebsmittel vor dem Kauf oder nach einer Instandsetzung

Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle

Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik

Entitätstypen	ORG_GEN: Organisation der Institution

Fehlende Datenschutzpolitik

Entitätstypen	ORG_GEN: Organisation der Institution

Die Sicherheitspolitik wird nicht angewendet

Entitätstypen	ORG_GEN: Organisation der Institution

Fehlende TEMPEST-Zoneneinteilung

Entitätstypen	PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung
Besuchereingang in unmittelbarer Gebäudenähe	
Entitätstypen	PHY_LIE.2: Räumlichkeiten
Unmittelbare Nähe zur Straße	
Entitätstypen	PHY_LIE.3: Zone
Trägermaterial fördert das Abfangen von kompromittierenden Störsignalen (elektrische Kabel, Rohrleitungen usw.)	
Entitätstypen	PHY_SRV.2: Energie PHY_SRV.1: Kommunikation
Fehlender Zugangsschutz zu den Einrichtungen	
Entitätstypen	PHY_SRV.2: Energie PHY_SRV.1: Kommunikation
Medien und Informationsträger senden möglicherweise kompromittierende Störsignale aus	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 17 – ABFANGEN VON KOMPROMITTIERENDEN STÖRSIGNALEN	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme

	LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.18 FERN-SPIONAGE

Fehlende Bildschirmschutzvorrichtungen bei Nichtbenutzung	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Benutzung leicht zu beobachtender Passwörter für den Zugriff auf das System oder auf Systemanwendungen (Form auf einer Tastatur, kurzes Passwort)	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Keine oder seltene Passwortänderung für den Zugriff auf das System oder die Anwendung	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Von außen einsehbarer Bildschirm	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Lesen von sensitiven Unterlagen in der Öffentlichkeit (Beobachten der Unterlagen durch externe Personen)	
Entitätstypen	MAT_PAS.2: Sonstige Datenträger
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Schutzvorschriften für den Austausch vertraulich eingestufter Informationen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln über von Unterauftragnehmern und Lieferanten einzuhaltende Sicherheitsmaßnahmen	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Die Sicherheitspolitik wird nicht angewendet	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Identifizierung sensitiver Güter	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Die Sicherheitsverantwortungen bezüglich der Ermächtigungsverwaltung sind nicht formalisiert	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Datenschutzpolitik	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems

Fehlende Identifizierung der Sicherheitsbedürfnisse eines Projekts	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Geringe Sensibilisierung für den Schutz von Informationen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Vorhandensein von Beobachtungspunkten außerhalb des Standorts	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Zone mit Öffnungen zur Straße hin	
Entitätstypen	PHY_LIE.3: Zone
Zone, die von einem Gebiet mit Publikumsverkehr aus beobachtet werden kann	
Entitätstypen	PHY_LIE.3: Zone
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 18 - FERN-SPIONAGE	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger

	MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.19 PASSIVES MITHÖREN

Fehlende Zugriffskontrollvorrichtung bei Nichtbenutzung	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Möglichkeit zur Installation einer Abhörsoftware (z. B. Trojanisches Pferd)	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Fehlender Schutz der Journale mit den Protokolldaten der jeweiligen Aktivitäten	
Entitätstypen	SYS_WEB: Externes Portal SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang LOG_STD: Programmpaket oder Standard-Software LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Keine oder seltene Passwortänderung für den Zugriff auf das System oder die Anwendung	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_OS: Betriebssystem LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Fehlender Schutz gegen den Gebrauch fortgeschrittener Zugriffsprivilegien	
Entitätstypen	LOG_OS: Betriebssystem
Keine oder seltene Passwortänderung für den Zugriff auf die Unterstützungssoftware	
Entitätstypen	LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
Logischer Zugriff auf Betriebsmittel, der die Installation einer Abhörsoftware ermöglicht	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Betriebsmittel mit abhörbarer Kommunikationsschnittstelle (Infrarot, 802.11, Bluetooth usw.)	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Schutzvorschriften für den Austausch vertraulich eingestufter Informationen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln über von Unterauftragnehmern und Lieferanten einzuhaltende Sicherheitsmaßnahmen	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	

Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Identifizierung sensitiver Güter	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Die Sicherheitsverantwortungen bezüglich der Ermächtigungsverwaltung sind nicht formalisiert	
Entitätstypen	ORG_GEN: Organisation der Institution
Die Sicherheitspolitik wird nicht angewendet	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Datenschutzpolitik	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Fehlende Identifizierung der Sicherheitsbedürfnisse eines Projekts	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Fehlende Ausbildung über Schutzmaßnahmen und –mittel bei externem und internem Informationsaustausch	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Manipulierbares Personal	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Geringe Sensibilisierung für einen geschützten Informationsaustausch bei vertraulichen Informationen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Verschaffung eines Vorteils beim Abfangen einer Information	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Möglichkeit, Übertragungen außerhalb des Standorts abzufangen	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten oder Eindringen über indirekte Zugänge möglich	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlender Zugangsschutz zu den Telekommunikationsendgeräten	
Entitätstypen	PHY_SRV.1: Kommunikation
Medien und Informationsträger besitzen Eigenschaften, die ein passives Mithören erlauben (z. B.	

Ethernet, kabelloses Kommunikationssystem usw.)	
Entitätstypen	RES_INF: Medien und Informationsträger
Informationsträger oder Kommunikationsausstattung zur Installation einer Abhöreinrichtung physisch zugänglich	
Entitätstypen	RES_INF: Medien und Informationsträger
Fehlende Authentifizierung der an das Netz angeschlossenen Betriebsmittel	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Physischer oder logischer Zugang zu einem Relais ermöglicht die Installation einer Abhöreinrichtung	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Kommunikation im Broadcastmodus	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Komplexe Leitweglenkung zwischen den Nebennetzen	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Schnittstelle mit Funktion, die ein Abhören ermöglicht	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Unverschlüsselter Informationsaustausch	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Fehlende Abtrennung der Kommunikationsnetze	
Entitätstypen	SYS_ITR: Intranet
Möglichkeit zum Mithören der mit den Authentifizierungsservern ausgetauschten Informationen	
Entitätstypen	SYS_ITR: Intranet
Möglichkeit zum Mithören der mit den Anwendungsservern ausgetauschten Informationen	
Entitätstypen	SYS_ITR: Intranet
Möglichkeit zum Einschleusen eines Abhörprogramms über die Clients	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Möglichkeit zur Installation einer logischen Abhöreinrichtung über die Mailbox-Gateways	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Lücken bei der Verwaltung der Zugriffsprivilegien an den Mailbox-Gateways	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 19 - PASSIVES MITHÖREN	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation

	PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.20 DIEBSTAHL VON DATENTRÄGERN ODER UNTERLAGEN

Intern entwickelte Einzelanwendungen	
Entitätstypen	LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
Fehlende Materialbestandsaufnahme	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Attraktive Betriebsmittel (Marktwert und technologische und strategische Werte)	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Diebstahlsicherung der Betriebsmittel (Kabelschloss)	
Entitätstypen	MAT_ACT.1: Tragbare Hardware
Festplatte leicht ausbaubar	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Betriebsmittel, das einer Gruppe von Personen frei zugänglich ist	
Entitätstypen	MAT_ACT.1: Tragbare Hardware
Fehlender Zugangsschutz zu den Speichereinrichtungen	
Entitätstypen	MAT_ACT.3: Verarbeitungsperipheriegerät
Vorhandensein eines Druckers in Bereichen mit Publikumsverkehr	
Entitätstypen	MAT_ACT.3: Verarbeitungsperipheriegerät
Datenträger allgemein zugänglich	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Weitergabe von Datenträgern über Postdienste (externe Lieferanten, interne Post usw.)	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Fehlender Schutz bei der Datenträgeraufbewahrung	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Fehlende Bestandsaufnahme der benutzten Datenträger	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Fehlende Datensicherung auf Datenträgern	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Leicht transportierbare Datenträger (z. B. herausnehmbare Festplatte, Speicherkassette)	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Original-Datenträger	
Entitätstypen	MAT_PAS.2: Sonstige Datenträger
Fehlende Datenschutz-Sicherheitspolitik an den verschiedenen Standorten der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln über von Unterauftragnehmern und Lieferanten einzuhaltende Sicherheitsmaßnahmen	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle

Die Sicherheitsverantwortungen bezüglich der Klassifizierung von Informationen sind weder formalisiert noch allgemein bekannt	
Entitätstypen	ORG_GEN: Organisation der Institution
Die Sicherheitspolitik wird nicht angewendet	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Organisation zur Verwaltung von Sicherheitszwischenfällen	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Identifizierung sensitiver Güter	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Kontrolle sensitiver Güter	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Identifizierung der Sicherheitsbedürfnisse eines Projekts	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Fehlende Datenschutzpolitik	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Manipulierbares Personal	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Nicht-Einhalten der Vorschriften bezüglich der Klassifizierung von Informationen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Sensibilisierung für den Schutz vertraulicher Unterlagen bewirkt mangelnde Wachsamkeit	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Verschaffung eines Vorteils bei Verbreitung einer Information	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_DEC: Entscheidungsträger
Fehlender persönlicher Einsatz beim Schutz vertraulicher Unterlagen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Außerhalb des Standorts vorhandene bzw. weitergereichte Datenträger oder Unterlagen	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten oder Eindringen über indirekte Zugänge möglich	

Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten

DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 20 - DIEBSTAHL VON DATENTRÄGERN ODER UNTERLAGEN

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.21 DIEBSTAHL VON BETRIEBSMITTELN

Fehlende Ersatz-Betriebsmittel	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Materialbestandsaufnahme	
Entitätstypen	MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.1: Tragbare Hardware
Betriebsmittel, das einer Gruppe von Personen frei zugänglich ist	
Entitätstypen	MAT_ACT.1: Tragbare Hardware
Attraktive Betriebsmittel (Marktwert und technologische und strategische Werte)	
Entitätstypen	MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.1: Tragbare Hardware
Möglichkeit zum Wiederverkauf des Gerätes (Fehlende Markierung, Benutzung ohne Passwort)	
Entitätstypen	MAT_ACT.1: Tragbare Hardware
Leicht zerlegbares Gerät	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln über von Unterauftragnehmern und Lieferanten einzuhaltende Sicherheitsmaßnahmen	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Organisation zur Verwaltung und Handhabung von Sicherheitszwischenfällen bei Diebstahl	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Kontrollvorschriften für ein- und ausgelieferte Betriebsmittel	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Identifizierung sensitiver Güter	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Identifizierung der Sicherheitsbedürfnisse eines Projekts	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Geringe Sensibilisierung für den Schutz der Betriebsmittel außerhalb der Institution	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Manipulierbares Personal	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung

	PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Nicht-Einhalten der physischen Schutzvorschriften für transportfähige Betriebsmittel	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Verschaffung eines Vorteils bei Wiederverkauf eines Gerätes	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Benutzung von Betriebsmitteln außerhalb der Institution (am Wohnsitz der Mitarbeiter, in einer anderen Institution usw.)	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten oder Eindringen über indirekte Zugänge möglich	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 21 - DIEBSTAHL VON BETRIEBSMITTELN	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware

MAT_ACT.1: Tragbare Hardware
MAT: Hardware
LOG_STD: Programmpaket oder Standard-Software
LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
LOG_OS: Betriebssystem
LOG_APP: Tätigkeitsgebundene Anwendung
LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
LOG_APP.1: Tätigkeitsgebundene Standardanwendun
LOG: Software

4.22 ÜBERNAHME RECYCELTER ODER AUSGEMUSTERTER DATENTRÄGER

Vorhandensein von Restdaten der Softwareprogramme

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Vorhandensein von Restdaten ohne Wissen des Benutzers auf weitergegebenen oder ausgemusterten Betriebsmitteln

Entitätstypen	MAT_PAS.1: Elektronischer Datenträger MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware

Fehlende Mittel zur Vernichtung von Datenträger

Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger

Fehlende Identifizierung sensitiver Güter

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt

Fehlende Kontrolle sensitiver Güter

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt

Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt

Fehlende Anwendung einer Datenschutzpolitik im Hinblick auf Recycling und Ausmusterung

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt

Fehlende Vertragsklauseln über von Unterauftragnehmern und Lieferanten einzuhaltende Sicherheitsmaßnahmen

Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle

Manipulierbares Personal

Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal

Nicht-Einhalten der Vorschriften zur Vernichtung von Datenträgern mit klassifizierten Informationen

Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal

Fehlende Aufklärung und Sensibilisierung hinsichtlich der Remanenz von maschinenlesbaren Daten auf den Datenträgern

Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal

Verschaffung eines Vorteils bei Verbreitung einer Information

Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal

Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert

Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal

Vorhandensein ausgemusterter Datenträger außerhalb des Standorts

Entitätstypen	PHY_LIE.1: Äußere Umgebung

Vorhandensein ausgemusterter Datenträger in Räumlichkeiten mit Publikumsverkehr

Entitätstypen	PHY_LIE.2: Räumlichkeiten

Vorhandensein ausgemusterter Datenträger in Zonen, die dienstlich nicht betroffenen Personen zugänglich sind

Entitätstypen	PHY_LIE.3: Zone

DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 22 - ÜBERNAHME RECYCELTER ODER AUSGEMUSTERTER DATENTRÄGER

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv)

	MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.23 VERBREITUNG

Fehlende Überprüfung der bewilligten Mehrbenutzerzugriffe	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Verfahren zur Verwaltung der Zugriffsprivilegien zu schwerfällig zu handhaben	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Funktionen zur Verwaltung der Benutzerrechte zu kompliziert in der Anwendung; mögliche Quelle von Fehlern	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware
Vorhandensein eines gemeinsamen Verzeichnisses zur Datenspeicherung	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware
Datenträger zum Austausch sensitiver Informationen befähigt	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Fehlen einer verantwortlichen Organisation zur Definition, Vergabe und Kontrolle von Zugriffsprivilegien	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Identifizierung sensitiver Güter	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Die Sicherheitspolitik wird nicht angewendet	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Fehlender persönlicher Einsatz zum Schutz der Vertraulichkeit	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Verfahren zur Verwaltung und Anwendung der Ermächtigungen zu schwerfällig zu handhaben	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Die Sicherheitsverantwortungen bezüglich der Klassifizierung von Informationen sind weder formalisiert noch allgemein bekannt	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems

	ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Kontrolle sensitiver Güter	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Datenschutzpolitik	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Nicht-Einhalten der Vorschriften zur Klassifizierung der Informationen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Manipulierbares Personal	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Sensibilisierung für den Schutz sensitiver Informationen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Nicht-Einhalten der Zurückhaltungspflicht	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Verschaffung eines Vorteils bei Verbreitung einer Information	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Kontrolle (oder fehlende Protokollierung) des Informationsaustauschs nach außen	
Entitätstypen	PHY_SRV.1: Kommunikation PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Vorhandensein eines Kommunikationsnetzes für den Informationsaustausch nach außen	
Entitätstypen	RES_INF: Medien und Informationsträger
Fichiers d'imputation complexes ou peu ergonomiques	
Entitätstypen	RES_INT: Kommunikationsschnittstelle

Standardschnittstelle für den Informationsaustausch (z. B. Bluetooth-Schnittstelle mit standardmäßiger Akzeptanz von Kommunikationen aller Art)	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Möglichkeit zur Benutzung von Betriebsmitteln ohne Hinterlassen von Spuren	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Fehlende Benachrichtigung der Benutzer	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Komplexe Leitweglenkung zwischen den Nebennetzen	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Fehlende straffe Leitweglenkung zwischen den Nebennetzen	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Fehlende Filterung und Protokollierung an den Kommunikationsrelais zwischen den einzelnen Netzen	
Entitätstypen	RES_REL: Passives oder aktives Relais
Anschluss des Systems an externe Netzwerk	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Fehlende Zugriffskontrolle zu den im Unternehmensverzeichnis gespeicherten Informationen	
Entitätstypen	SYS_ANU: Unternehmensverzeichnis
Fehlende Protokollierung der Zugriffe	
Entitätstypen	SYS_INT: Einrichtung für Internetzugang
Fehlende Filtereinrichtung	
Entitätstypen	SYS_INT: Einrichtung für Internetzugang
Fehlende oder schwierige Verwaltung der Privilegien für den Zugriff auf gemeinsame Informationen (Definition, Vergabe, Kontrolle)	
Entitätstypen	SYS_ITR: Intranet
Fehlende Abtrennung der Kommunikationsnetze	
Entitätstypen	SYS_ITR: Intranet
Fehlende Maßnahmen zur Vermeidung von Nachlässigkeiten beim Senden von Informationen	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Das System ist von allen Mitarbeitern benutzbar	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Das System kann Informationen im Anhang übermitteln	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Kein wirksamer und operationeller Anti-Virenschutz	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Fehlende Verwaltung der Privilegien für den Zugriff auf Informationen (Möglichkeit der Beeinträchtigung öffentlicher Informationen)	
Entitätstypen	SYS_WEB: Externes Portal
Das System vereinfacht die Verbreitung von Informationen nach außen	
Entitätstypen	SYS_WEB: Externes Portal
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 23 - VERBREITUNG	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung

SYS_ITR: Intranet
SYS_INT: Einrichtung für Internetzugang
SYS_ANU: Unternehmensverzeichnis
SYS: System
RES_REL: Passives oder aktives Relais
RES_INT: Kommunikationsschnittstelle
RES_INF: Medien und Informationsträger
RES: Netzwerk
PHY_SRV: Wesentlicher Dienst
PHY_SRV.3: Abkühlung / Verschmutzung
PHY_SRV.2: Energie
PHY_SRV.1: Kommunikation
PHY_LIE: Orte
PHY_LIE.3: Zone
PHY_LIE.2: Räumlichkeiten
PHY_LIE.1: Äußere Umgebung
PER_UTI: Benutzer
PER_EXP: Betreiber / Wartung
PER_DEV: Entwickler
PER_DEC: Entscheidungsträger
PER: Personal
ORG_PRO: Organisation eines Projekts oder eines Systems
ORG_GEN: Organisation der Institution
ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
ORG_DEP: Organisation, von der die Institution abhängt
ORG: Organisation
MAT_PAS: Datenträger (passiv)
MAT_PAS.2: Sonstige Datenträger
MAT_PAS.1: Elektronischer Datenträger
MAT_ACT: Datenverarbeitungsmittel (aktiv)
MAT_ACT.3: Verarbeitungsperipheriegerät
MAT_ACT.2: Ortsfeste Hardware
MAT_ACT.1: Tragbare Hardware
MAT: Hardware
LOG_STD: Programmpaket oder Standard-Software
LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
LOG_OS: Betriebssystem
LOG_APP: Tätigkeitsgebundene Anwendung
LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
LOG_APP.1: Tätigkeitsgebundene Standardanwendun
LOG: Software

4.24 INFORMATIONEN OHNE HERKUNFTSGARANTIE

Übernahme von Softwareprogrammen über nicht authentifizierte Sammelstellen	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Möglichkeit zur Installation von Korrekturmaßnahmen, Updates, Patches, Hotfixes usw.	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Fehlende sichere Mittel zur Identifikation	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Fehlende Aufbewahrung von Protokolldaten, die Aufschluss über die Aktivitäten geben	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Fehlende Vorkehrungen zur Garantie der Herkunft eines Betriebsmittels	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Datenschutz-Sicherheitspolitik an den verschiedenen Standorten der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vorkehrungen zur Garantie der Herkunft gelieferter Waren	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Politik zur Aufbewahrung und Analyse aktivitätsspezifischer Protokolldaten	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Information bezüglich der Aufteilung der Verantwortungen und der Mittel zur Garantie der Berechtigung einer Anfrage	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Organisation zur garantierten Identifikation einer Person innerhalb der Institution oder eines Projekts	

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Sensibilisierung für Risiken bei Benutzung einer fremden Identität (falsche Benutzung von Mitteln, die eine Authentifizierung garantieren wie z. B. Passwörter)	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Leichtgläubigkeit	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Unkenntnis der Bedeutung der Qualifikation einer Information	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Manipulierbares Personal	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Konfliktgeladenes soziales Klima	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Verschaffen eines Vorteils bei Fehlinformation	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Fehlende Mittel zur Garantie der Authentizität von Codes	
Entitätstypen	PER_DEV: Entwickler
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_DEV: Entwickler
Möglichkeit der Beeinträchtigung einer Kommunikation	
Entitätstypen	RES_INF: Medien und Informationsträger
Über das Protokoll kann der Geber einer Kommunikation nicht eindeutig authentifiziert werden	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Möglichkeit zur Benutzung von Betriebsmitteln ohne Hinterlassen von Spuren	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Komplexe bzw. wenig ergonomische Dateien	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Die Relais identifizieren weder die Quellen noch die Ziele (mögliche Auswirkungen: Anfälligkeit des Systems für Spoofing-Angriffe)	
Entitätstypen	RES_REL: Passives oder aktives Relais
Möglichkeit, sich widerrechtlich Funktion des Unternehmensverzeichnisses anzueignen	

Entitätstypen	SYS_ANU: Unternehmensverzeichnis
Das System kann den Autor einer Änderung nicht identifizieren	
Entitätstypen	SYS_ANU: Unternehmensverzeichnis
Über die Einrichtung besteht Zugriff auf nicht authentifizierbare Daten (z. B. Hoax)	
Entitätstypen	SYS_INT: Einrichtung für Internetzugang
Das System verfügt über keine Mittel zur Aufbewahrung aktivitätsspezifischer Journale	
Entitätstypen	SYS_WEB: Externes Portal SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang
Das System ermöglicht die Speicherung oder Änderung von Informationen ohne Authentifizierung der Autoren	
Entitätstypen	SYS_ITR: Intranet
Das System ermöglicht das Senden und Empfangen von Informationen ohne Authentifizierung der Sender bzw. Empfänger	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Das System verfügt über keine Filter zur Verhinderung des Empfangs von außen kommender Falschmeldungen	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Das System gestattet die Relayfunktion	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Das System kann die Person, die eine Anfrage gesendet hat, nicht identifizieren	
Entitätstypen	SYS_WEB: Externes Portal
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 24 – INFORMATIONEN OHNE HERKUNFTSGARANTIE	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger

	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.25 SABOTIEREN DER HARDWARE

Möglichkeit zum Hinzufügen zusätzlicher Hardwarekomponenten zum Speichern, Übertragen oder Manipulieren (z. B. physisches Keyloggen)	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Prozedur zur Kontrolle bei Eingriffen an der Systemausstattung der Institution durch externes Personal	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	
Entitätstypen	ORG_GEN: Organisation der Institution
Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Prozeduren zur operationellen Qualifikation	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Kontrolle sensitiver Güter	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Identifizierung sensitiver Güter	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Prozedur zur Validierung der Hardwarekomponenten bei Lieferung oder nach Instandsetzung	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Unzureichende Abnahmeprüfung der Software, insbesondere hinsichtlich der Grenzwerte	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Manipulierbares Personal	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Wachsamkeit bei Eingriff eines Wartungstechnikers an einer Arbeitsstation oder am Server	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Geringe Sensibilisierung für den Schutz von Betriebsmitteln außerhalb der Institution	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung

	PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Verschaffen eines Vorteils bei Fehlinformation	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Benutzung von Betriebsmitteln außerhalb der Institution (am Wohnsitz der Mitarbeiter, in einer anderen Institution usw.)	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten oder Eindringen über indirekte Zugänge möglich	
Entitätstypen	PHY_SRV.1: Kommunikation PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Möglichkeit zur Installation einer Leitungsabzweigung	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 25 - SABOTIEREN DER HARDWARE	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware

	MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.26 SABOTIEREN DER SOFTWARE

Die Hotline zur Telewartung ist permanent aktiviert

Entitätstypen	SYS_MES: Nachrichtenübermittlung RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Möglichkeit des Vorhandenseins versteckter Funktionen, die während der Entwurfs- oder Entwicklungsphase eingeschleust wurden

Entitätstypen	SYS_WEB: Externes Portal SYS_ANU: Unternehmensverzeichnis LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Möglichkeit zur Änderung oder Manipulation der Software

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Fehlender Schutz gegen den Gebrauch fortgeschrittener Zugriffsprivilegien

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Benutzung ungeprüfter Softwareprogramme

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Fehlender Einsatz von Basis-Sicherheitsregeln, die bezüglich des Betriebssystems und der Softwareprogramme anzuwenden sind

Entitätstypen	SYS_MES: Nachrichtenübermittlung LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Möglichkeit zur Erzeugung oder Änderung von Systembefehlen

Entitätstypen	SYS_WEB: Externes Portal LOG_OS: Betriebssystem

Übernahme von Softwareprogrammen über nicht authentifizierte Sammelstellen

Entitätstypen	LOG_OS: Betriebssystem

Möglichkeit zur Systemadministration aus der Entfernung mit nicht verschlüsselten Administrationstools	
Entitätstypen	SYS_MES: Nachrichtenübermittlung RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_OS: Betriebssystem
Unzureichende Komplexität der Zugangspasswörter	
Entitätstypen	SYS_MES: Nachrichtenübermittlung LOG_OS: Betriebssystem
Möglichkeit zur Installation von Korrekturmaßnahmen, Updates, Patches, Hotfixes usw.	
Entitätstypen	LOG_OS: Betriebssystem
Möglichkeit zur Fern-Systemadministration von jeder beliebigen Arbeitsstation aus	
Entitätstypen	SYS_MES: Nachrichtenübermittlung RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_OS: Betriebssystem
Benutzung eines Standard-Betriebssystems, auf das bereits Softwareangriffe durchgeführt wurden	
Entitätstypen	LOG_OS: Betriebssystem
Möglichkeit zur Fern-Systemadministration von jeder beliebigen Arbeitsstation aus	
Entitätstypen	SYS_MES: Nachrichtenübermittlung RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_OS: Betriebssystem
Möglichkeit zum Löschen, Ändern oder Installieren neuer Programme	
Entitätstypen	LOG_OS: Betriebssystem
Die SNMP-Schicht ist aktiviert	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_OS: Betriebssystem
Die Hardware kann von jedermann von einem beliebigen Peripheriegerät aus gebootet werden (z. B. Diskette, CD-ROM)	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Mittel zur Kontrolle der Unschädlichkeit von Datenträgern beim Eintreffen in der Institution	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Prozedur zur Kontrolle bei Eingriffen an der Systemausstattung der Institution durch externes Personal	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Vertragsklauseln über die Unschädlichkeitsgarantie von Lieferungen durch Unterauftragnehmer oder Lieferanten	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Globalpolitik zum Kampf gegen maligne Codes	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Identifizierung sensitiver Güter	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems

	ORG_GEN: Organisation der Institution
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Kontrolle sensitiver Güter	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Politik zum Schutze der Arbeitsstationen	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Politik zur Aufbewahrung und Analyse aktivitätsspezifischer Protokolldaten	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Maßnahmen zur Kontrolle der Entwicklungen	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Fehlende Maßnahmen zum Schutze der Integrität von Codes während der Entwurfs-, Installations- und Betriebsphasen	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Benutzung von Softwareprogrammen ohne Herkunftsgarantie	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Konfliktgeladenes soziales Klima	
Entitätstypen	PER_UTI: Benutzer PER_DEC: Entscheidungsträger
Fehlende Sensibilisierung für maligne Codes	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Unkenntnis der anzuwendenden Reflexe bei Detektion einer Anomalie	
Entitätstypen	PER_UTI: Benutzer PER_DEC: Entscheidungsträger
Nicht-Einhalten der Vorschriften zur Aktualisierung der Anti-Virenprogramme	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Manipulierbares Personal	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Verschaffung eines Vorteils bei Störung des IT-Systems	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Konfliktgeladenes Klima	
Entitätstypen	PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_DEV: Entwickler
Fehlende Mittel zur Garantie der Authentizität von Entwicklungen	
Entitätstypen	PER_DEV: Entwickler

Betreiber oder Inhaber verfügen über erweiterte Zugriffsprivilegien	
Entitätstypen	PER_EXP: Betreiber / Wartung
Unkenntnis der einzuleitenden Prozeduren bei Detektion einer Anomalie	
Entitätstypen	PER_EXP: Betreiber / Wartung
Benutzung von Betriebsmitteln außerhalb der Institution (am Wohnsitz der Mitarbeiter, in einer anderen Institution usw.)	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Fehlende Zugangskontrolle zum Standort oder zu den Räumlichkeiten oder Eindringen über indirekte Zugänge möglich	
Entitätstypen	PHY_SRV.1: Kommunikation PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Das Netzwerk vereinfacht die Nutzung von Ressourcen durch Unbefugte	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Komplexe bzw. wenig ergonomische Dateien	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Möglichkeit zum Hinzufügen von Softwareabzweigungen	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Das Netzwerk lässt es zu, Systemressourcen zu ändern oder auf sie einzuwirken	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Möglichkeit zum Hinzufügen zusätzlicher Softwarekomponenten zum Speichern, Übertragen oder Manipulieren (z. B. Keyloggen)	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Möglichkeit zur Benutzung von Betriebsmitteln ohne Hinterlassen von Spuren	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Möglichkeit zur Änderung bzw. zum Austausch von Anwendungsprogrammen	
Entitätstypen	SYS_WEB: Externes Portal SYS_ANU: Unternehmensverzeichnis
Möglichkeit zum Löschen oder Ändern von Systemprogrammen oder -dateien	
Entitätstypen	SYS_WEB: Externes Portal SYS_ANU: Unternehmensverzeichnis
Fehlende Sensibilisierung für die Risiken beim Herunterladen von Softwareprogrammen	
Entitätstypen	SYS_INT: Einrichtung für Internetzugang
Fehlende Antivirenkontrolle beim Informationsaustausch	
Entitätstypen	SYS_INT: Einrichtung für Internetzugang
Die Einrichtung ermöglicht eine Ausnutzung des Asynchronbetriebs bestimmter Bereiche oder Befehle des Betriebssystems (z. B. Javascript-Komponenten zur Erkundung des Inhalts der Festplatte)	
Entitätstypen	SYS_INT: Einrichtung für Internetzugang
Vorhandene Einrichtung zur Änderung oder Installation von Anwendungen aus der Entfernung	
Entitätstypen	SYS_ITR: Intranet
Gemeinsam genutzter Speicherplatz	
Entitätstypen	SYS_ITR: Intranet
Verwendung einer veralteten Version des Mailboxservers	

Entitätstypen	SYS_MES: Nachrichtenübermittlung
Verwendung einer Verteilungsliste, auf der eine Großteil aller Mitarbeiter verzeichnet ist	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Verwendung eines Protokolls ohne Authentifizierungsfunktion	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Möglichkeit zum automatischen Versenden von Mitteilungen	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Fehlende Sensibilisierung für die Risiken beim Versand von Anhängen	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Die Mailfunktion ermöglicht eine Ausnutzung des Asynchronbetriebs bestimmter Bereiche oder Befehle des Betriebssystems (z. B. automatischer Start von Anhängen)	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Fehlende Überprüfung der Anwendungsprogramme vor der Installation	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Über die Mailfunktion können Software-Updates installiert werden (z. B. Patches, Antivirenprogramme usw.)	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Fehlende Mittel zur Antivirenfilterung	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Möglichkeit zur Installation von Piratenprogrammen	
Entitätstypen	SYS_WEB: Externes Portal
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 26 - SABOTIEREN DER SOFTWARE	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv)

	MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.27 GEOLOKALISATION

Lokalisierbares Material (z. B. Triangulation)	
Entitätstypen	MAT_ACT.1: Tragbare Hardware
Fehlende Datenschutz-Sicherheitspolitik an den verschiedenen Standorten der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Schutzvorschriften hinsichtlich der Vertraulichkeit von Informationen, die zur Lokalisierung von Mitarbeitern genutzt werden könnten (Auskünfte über Tickets, Verzeichnis über Ein- und Ausgänge usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Zurückhaltung und Wachsamkeit	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 27 - GEOLOKALISATION	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle

	ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.28 AUSFALL VON BETRIEBSMITTELN

Fehlende Diagnosefunktion zur Vorbeugung gegen den Ausfall von Betriebsmitteln	
Entitätstypen	LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem
Fehlender Schutz gegen elektrische Störungen	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware
Schlechte Nutzungsbedingungen	
Entitätstypen	RES_INF: Medien und Informationsträger MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware
Wartungsfehler	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Schlechte Zuverlässigkeit der Betriebsmittel	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Veralterung des Materials	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Datenträger nicht an die Lebensdauer der zu archivierenden Daten angepasst	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Schlechte Lagerungsbedingungen	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Fehlende Klausel über die Fristen zum Eingreifen oder Austauschen bei Ausfall eines Betriebsmittels	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Organisation zur Aktualisierung der Wartungsverträge	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Aktualisierung der Wartungs- und Unterstützungsverträge mit den Lieferanten	

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlendes Ausfallreporting (Volumen, Kosten der Zwischenfälle, Dauer)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Vorschriften über die Anwendungsbedingungen der Infrastrukturen zur Informationsverarbeitung (in Räumlichkeiten mit IT-Material ist Rauchen, Essen und Trinken verboten)	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlender Plan zur Wiederaufnahme der wesentlichen Aktivitäten innerhalb der Institution	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Anweisungen über Sofortmaßnahmen zum Schutz der Betriebsmittel bei Wasserschäden oder Brand	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Organisation einer Analyse, ob die Kapazitäten der Betriebsmittel den Bedürfnissen angepasst sind	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Vorschriften über die Anwendungsbedingungen der Infrastrukturen zur Informationsverarbeitung (in Räumlichkeiten mit IT-Material ist Rauchen, Essen und Trinken verboten)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Ausfälle oder Überlastungen (Kontrollschemen)	
Entitätstypen	PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Keine Informationsweitergabe zur Gewährleistung einer zentralisierten Ausfallanalyse	
Entitätstypen	PER_UTI: Benutzer
Unkenntnis der Anwendungsvorschriften der Betriebsmittel	
Entitätstypen	PER_UTI: Benutzer
Fehlende Berücksichtigung der spezifischen, das Fehler- und Ausfallrisiko erhöhenden Umgebung (überhitzte Atmosphäre, industrielle Umgebung usw.)	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Funktionsprüfung der Ersatz-Betriebsmittel	
Entitätstypen	PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation
Manuelles Auslösen der Notlösung	
Entitätstypen	PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation
Schlechte Zuverlässigkeit der Informationsträger	
Entitätstypen	RES_INF: Medien und Informationsträger
Veralterung des Informationsträgers	
Entitätstypen	RES_INF: Medien und Informationsträger
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 28 - AUSFALL VON BETRIEBSMITTELN	
Entitätstypen	SYS_WEB: Externes Portal

SYS_MES: Nachrichtenübermittlung
SYS_ITR: Intranet
SYS_INT: Einrichtung für Internetzugang
SYS_ANU: Unternehmensverzeichnis
SYS: System
RES_REL: Passives oder aktives Relais
RES_INT: Kommunikationsschnittstelle
RES_INF: Medien und Informationsträger
RES: Netzwerk
PHY_SRV: Wesentlicher Dienst
PHY_SRV.3: Abkühlung / Verschmutzung
PHY_SRV.2: Energie
PHY_SRV.1: Kommunikation
PHY_LIE: Orte
PHY_LIE.3: Zone
PHY_LIE.2: Räumlichkeiten
PHY_LIE.1: Äußere Umgebung
PER_UTI: Benutzer
PER_EXP: Betreiber / Wartung
PER_DEV: Entwickler
PER_DEC: Entscheidungsträger
PER: Personal
ORG_PRO: Organisation eines Projekts oder eines Systems
ORG_GEN: Organisation der Institution
ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
ORG_DEP: Organisation, von der die Institution abhängt
ORG: Organisation
MAT_PAS: Datenträger (passiv)
MAT_PAS.2: Sonstige Datenträger
MAT_PAS.1: Elektronischer Datenträger
MAT_ACT: Datenverarbeitungsmittel (aktiv)
MAT_ACT.3: Verarbeitungsperipheriegerät
MAT_ACT.2: Ortsfeste Hardware
MAT_ACT.1: Tragbare Hardware
MAT: Hardware
LOG_STD: Programmpaket oder Standard-Software
LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
LOG_OS: Betriebssystem
LOG_APP: Tätigkeitsgebundene Anwendung
LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
LOG_APP.1: Tätigkeitsgebundene Standardanwendun
LOG: Software

4.29 FEHLERHAFTER BETRIEB VON BETRIEBSMITTELN

Fehlende Diagnosefunktion zur Vorbeugung von Ausfällen der Betriebsmittel	
Entitätstypen	LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem
Fehlender Schutz gegen elektrische Störungen	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware
Schlechte Nutzungsbedingungen	
Entitätstypen	RES_INF: Medien und Informationsträger MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware
Schlechte Zuverlässigkeit der Betriebsmittel	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Mögliche Inkompatibilität zwischen den einzelnen Betriebsmitteln	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Datenträger nicht an die Lebensdauer der zu archivierenden Daten angepasst	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Schlechte Lagerungsbedingungen	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Ausfälle oder Überlastungen (Kontrollschemen)	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vorschriften über die Anwendungspflicht von Normen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Klausel über die Fristen zum Eingreifen oder Austauschen bei fehlerhaftem Betrieb eines Betriebsmittels	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlendes Fehlerreporting	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlender Plan zur Wiederaufnahme der wesentlichen Aktivitäten innerhalb der Institution	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution

Fehlende Prozeduren zur operationellen Qualifikation	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Vorschriften über die Betriebsumgebung der Infrastrukturen zur Informationsverarbeitung (Temperatur, Hygrometrie usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Organisation einer Analyse, ob die Kapazitäten der Betriebsmittel den Bedürfnissen angepasst sind	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Ausfälle oder Überlastungen (Kontrollschemen)	
Entitätstypen	PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Unkenntnis der Anwendungsvorschriften der Betriebsmittel	
Entitätstypen	PER_UTI: Benutzer
Keine Informationsweitergabe zur Gewährleistung einer zentralisierten Ausfallanalyse	
Entitätstypen	PER_UTI: Benutzer
Fehlende Berücksichtigung der spezifischen, das Fehler- und Ausfallrisiko erhöhenden Umgebung (überhitzte Atmosphäre, industrielle Umgebung usw.)	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Funktionsprüfung der Ersatz-Betriebsmittel	
Entitätstypen	PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation
Manuelles Auslösen der Notlösung	
Entitätstypen	PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation
Veralterung des Informationsträgers	
Entitätstypen	RES_INF: Medien und Informationsträger
Mögliche Inkompatibilität zwischen den Informationsträgern und anderen Komponenten	
Entitätstypen	RES_INF: Medien und Informationsträger
Medien und Informationsträger enthalten technische Merkmale, die sie lokalisierbar machen (z. B. verschiedene ADSl-Konfigurationsparameter zwischen Frankreich und Großbritannien)	
Entitätstypen	RES_INF: Medien und Informationsträger
Schlechte Zuverlässigkeit der Informationsträger	
Entitätstypen	RES_INF: Medien und Informationsträger
Wartungsfehler	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger
Schnittstelle enthält landesspezifische technische Merkmale (z. B. verschiedene Telefonsteckertypen zwischen Frankreich und Großbritannien)	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Möglichkeit zur fehlerhaften Konfiguration, Installation oder Modifikation der Relais	
Entitätstypen	RES_REL: Passives oder aktives Relais

	RES_INT: Kommunikationsschnittstelle
Veralterung des Materials	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Mögliche Inkompatibilität zwischen den einzelnen Betriebsmitteln	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 29 - FEHLERHAFTER BETRIEB VON BETRIEBSMITTELN	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.30 ÜBERLASTUNG DES INFORMATIONSSYSTEMS

Fehlender Filter zum Schutz des Systems gegen Überlauf

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Unnötiger Einsatz von Betriebsmitteln

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Anwendung erfordert IT-Ressourcen, die der Hardware nicht angepasst ist (z. B. unzureichender Arbeitsspeicher)

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Bei Definition der Projektanforderungen fehlende Berücksichtigung von Ausnahmesituationen, bei denen das System die Grenzbedingungen erreicht

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Qualifikation der Entwicklungen in einem betriebsähnlichen Kontext

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Schlechte Dimensionierung der Ressourcen (z. B. unzureichende Autonomie einer Laptop-Batterie)

Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware

Unerwünschtes Fortbestehen von Daten auf den Datenträgern

Entitätstypen	MAT_PAS.1: Elektronischer Datenträger

Fehlende Vorschriften über die Anwendungspflicht von Normen

Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Ausfälle oder Überlastungen (Kontrollschemen)	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklausel über die Qualität der von den Systemen am Rande der Grenzbedingungen zu erbringenden Dienste (intensive Inanspruchnahme des Systems, Eingabe nicht konformer Daten, Dateneingabe bei extremen Betriebsbedingungen)	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Politik zur Nachkontrolle der angemessenen Dimensionierung der Informationsverarbeitungsinfrastruktur einschließlich der Ersatz-Betriebsmittel	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Anweisungen bezüglich der korrekten Benutzung der IT-Ressourcen zur Vermeidung von Verhalten, die eine Überlastung der Speicherkapazitäten oder Verarbeitungsressourcen hervorrufen	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Anweisungen zum Verhalten bei Zwischenfällen (Detektion, Aktion usw.)	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Entscheidung zur Neudimensionierung bei Erkennung einer signifikanten Erhöhung der Inanspruchnahme der IT-Ressourcen	
Entitätstypen	PER_DEC: Entscheidungsträger
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Ausfälle oder Überlastungen (Kontrollschemen)	
Entitätstypen	PER_EXP: Betreiber / Wartung
Ausbildungsmangel hinsichtlich der korrekten Anwendung der IT-Mittel (Störung des Systems, Installation nicht kompatibler Software usw.)	
Entitätstypen	PER_UTI: Benutzer
Verschaffung eines Vorteils bei Störung des IT-Systems	
Entitätstypen	PER_UTI: Benutzer
Fehlende Sensibilisierung für das Bedürfnis, mit den IT-Ressourcen der Institution sparsam umzugehen (schlechte Nutzung des Speicherplatzes u. ä.)	
Entitätstypen	PER_UTI: Benutzer
Schlechte Dimensionierung z. B der Telekom-Ressourcen, indem täglich auch die Ressourcen benutzt werden, die als Reservelösung vorgesehen sind	
Entitätstypen	PHY_SRV.1: Kommunikation
Schlechte Dimensionierung der Reserve-Ressourcen	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie
Möglicherweise sind die Relais einer zu großen Anzahl an Anfragen oder einer intensiven Störung ausgesetzt (z. B. Denial-of-service-Attacke vom Typ "smurf" oder "SYN flood")	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Möglichkeit zur fehlerhaften Konfiguration, Installation oder Modifikation der Relais	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Schlechte Dimensionierung (z. B. zu viele Daten bezogen auf die maximale Bandbreite)	
Entitätstypen	RES_REL: Passives oder aktives Relais
Schlechte Dimensionierung der Ressourcen (z. B. zu viele Benutzer bezogen auf die maximale Kapazität des Verzeichnisses)	
Entitätstypen	SYS_ANU: Unternehmensverzeichnis

Möglichkeit, die Einrichtung einer zu großen Anzahl an Anfragen ohne Beschränkung auszusetzen	
Entitätstypen	SYS_WEB: Externes Portal SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis
Vorhandensein eines Zeitraums oder eines Ereignisses mit ausgesprochen signifikanter Erhöhung der Inanspruchnahme des Systems	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ANU: Unternehmensverzeichnis
Schlechte Dimensionierung der Ressourcen (z. B. zu viele gleichzeitige Anschaltungen)	
Entitätstypen	SYS_INT: Einrichtung für Internetzugang
Fehlende Verwaltung der Schreibzugriffsrechte auf gemeinsame Speicherbereiche	
Entitätstypen	SYS_ITR: Intranet
Schlechte Dimensionierung der Betriebs- oder Wartungs-Ressourcen	
Entitätstypen	SYS_ITR: Intranet
Fehlende Abtrennung der Kommunikationsnetze	
Entitätstypen	SYS_ITR: Intranet
Benutzung interner Verteilungslisten, die allen zugänglich sind	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Schlechte Dimensionierung der Speicherbereiche für erhaltene Mitteilungen	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Möglichkeit zum automatischen Versenden von Mitteilungen	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Fehlender Spam-Schutz	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Fehlende Größenbegrenzung der Anhänge	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Schlechte Benutzungsgewohnheiten des Nachrichtenübermittlungsdienstes durch die Benutzer (Benutzung der Mailboxen als Archivierbereich)	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Publikumszugang zum Portal	
Entitätstypen	SYS_WEB: Externes Portal
Schlechte Dimensionierung der Ressourcen (z. B. zu viele gleichzeitige Anschaltungen)	
Entitätstypen	SYS_WEB: Externes Portal
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 30 - ÜBERLASTUNG DES INFORMATIONSSYSTEMS	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation

	PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.31 FEHLERHAFTER BETRIEB VON SOFTWAREPROGRAMMEN

Mögliche Seiteneffekte infolge der Aktualisierung einer Softwarekomponente	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Aufbewahrung von Protokolldaten, die Aufschluss über die Verarbeitungen geben	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Schulung bezüglich der Nutzung oder Wartung neuer Softwareprogramme	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Wartungsprozedur	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Qualifikationsprozedur vor Installation oder Aktualisierung	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Prozedur zur Synchronisierung der Zeitgeber	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Keine Informationsweitergabe zur Gewährleistung einer zentralisierten Bearbeitung von Betriebsstörungen	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme

	LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Möglichkeit zur fehlerhaften Konfiguration, Installation oder Modifikation des Betriebssystems	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Fehlende Protokollierung der Wartungsoperationen	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Fehlende oder fehlerhafte Konfigurationsverwaltung der Softwarekomponenten (z. B. Benutzung eines UK-Patches, der für die französische Version nicht angemessen ist)	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Die Unterlagen sind nicht auf neuestem Stand	
Entitätstypen	LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Fehlende Überprüfung der Anwendungsprogramme vor der Installation	
Entitätstypen	SYS_MES: Nachrichtenübermittlung LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem
Verwendung einer veralteten Version des Betriebssystems oder der Anwendungsprogramme	
Entitätstypen	SYS_MES: Nachrichtenübermittlung LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem
Fehlende Vorschriften über die Anwendungspflicht von Normen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Ausfälle oder Überlastungen (Kontrollschemen)	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln bezüglich der Unterstützungs- und Eingriffsbedingungen	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Politik zur räumlichen Abtrennung von Benutzerumgebungen, um eine Autorisierung von Berechtigungen zur Änderung von Systemen oder Anwendungen zu vermeiden	
Entitätstypen	ORG_GEN: Organisation der Institution

Fehlende Anweisungen bezüglich der korrekten Benutzung der IT-Ressourcen zur Vermeidung risikoträchtigen Verhaltens	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Anweisungen zum Verhalten bei Zwischenfällen (Detektion, Aktion usw.)	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlender Plan zur Wiederaufnahme der wesentlichen Aktivitäten innerhalb der Institution	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Homogenität der IT-Ausstattung	
Entitätstypen	ORG_GEN: Organisation der Institution
Unzureichende Abnahmeprüfung der Software (die Testserien decken nicht alle Betriebsbedingungen ab – intensive Inanspruchnahme des Systems, Eingabe nicht konformer Daten, Dateneingabe bei extremen Betriebsbedingungen)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Fehlende Weiterverfolgung der Zwischenfälle zur Verhinderung eventueller Betriebsstörungen (Kontrollschemen)	
Entitätstypen	PER_DEC: Entscheidungsträger
Fehlende Schulung	
Entitätstypen	PER_DEV: Entwickler
Fehlende Sicherheitsvorschriften bei den Entwicklungen	
Entitätstypen	PER_DEV: Entwickler
Ausbildungsmangel hinsichtlich Wartung und Betrieb neuer Betriebsmittel	
Entitätstypen	PER_EXP: Betreiber / Wartung
Schlechte Dimensionierung der Betriebs- oder Wartungs-Ressourcen	
Entitätstypen	PER_EXP: Betreiber / Wartung
Nicht-Einhalten der einzuleitenden Eingriffsprozeduren	
Entitätstypen	PER_EXP: Betreiber / Wartung
Ausbildungsmangel hinsichtlich der korrekten Anwendung der IT-Mittel (Störung des Systems, Installation nicht kompatibler Software usw.)	
Entitätstypen	PER_UTI: Benutzer
Möglichkeit zur fehlerhaften Konfiguration, Installation oder Modifikation der Relais	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Schlechte Verwaltung der einzelnen Versionen und der Driverkonfigurationen	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Seiteneffekte der Schnittstellen (z. B Kompatibilitätsprobleme zwischen den einzelnen Protokollen)	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Möglicherweise wird die Einrichtung mit unkorrekten Anfragen bzw. Daten konfrontiert (z. B. Buffer overflow, Dienstverweigerung am LDAP-Server, SMTP, POP3, IMAP)	
Entitätstypen	SYS_ITR: Intranet SYS_ANU: Unternehmensverzeichnis
Nicht-Einhalten der Installations- oder Wartungsprozeduren	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis
Möglichkeit, die Einrichtung einer zu großen Anzahl an Anfragen ohne Beschränkung auszusetzen	

Entitätstypen	SYS_INT: Einrichtung für Internetzugang
Inkompatibilität der Softwareprogramme (z. B. Seiteneffekt eines Antivirenprogramms zur Filterung der Nachrichten)	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Möglicherweise wird die Einrichtung mit unkorrekten Anfragen bzw. Daten konfrontiert (z. B. Buffer overflow, Dienstverweigerung am LDAP-Server, SMTP, POP3, IMAP)	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung
Verwendung einer veralteten Version des Mailboxservers	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 31 - FEHLERHAFTER BETRIEB VON SOFTWAREPROGRAMMEN	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.32 BEEINTRÄCHTIGUNG DER WARTBARKEIT DES INFORMATIONSSYSTEMS

Fehlende Überprüfung der Anwendungsprogramme vor der Installation

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Ersatzprozedur bei Notfällen

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Prozedur zum Rücksetzen im Fall einer Anomalie infolge einer Modifikation

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Wartungsprozedur

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Die Unterlagen sind nicht auf neuestem Stand

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Protokollierung der Wartungsoperationen

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Aufbewahrung von Protokolldaten, die Aufschluss über die Bearbeitungen und Modifikationen geben

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem

	LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Spezifische Softwareprogramme	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Fehlende Schulung bezüglich der Nutzung oder Wartung neuer Softwareprogramme	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Veraltete Softwareprogramme	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Softwareprogramme ohne weiterentwicklungsfähige Konfigurationen	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Von außen (außerhalb der Institution) oder vom Ausland (Länder mit großem Zeitunterschied) nicht zugängliche Unterstützungsmittel	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Hardware ohne weiterentwicklungsfähige Konfigurationen	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Veraltete Betriebsmittel	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Spezifische Hardware	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle

	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Änderung der Betriebsmittel, Softwareprogramme oder Speicherprozeduren ohne Berücksichtigung der alten Abspeicherungen oder Archivierungen	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Veralteter Datenträger	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Verlust oder schlechte Verwaltung von Original-Unterlagen (Unterstützungsverträge, Lizenzen usw.)	
Entitätstypen	MAT_PAS.2: Sonstige Datenträger
Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklausel zur Sicherstellung der Aktivität (bei Einstellen der Aktivität, bei Konkurs eines Lieferanten usw.)	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Garantie hinsichtlich der Beständigkeit der Institution	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Aktualisierung der Wartungs- und Unterstützungsverträge mit den Lieferanten	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Anweisungen zum Verhalten bei Zwischenfällen (Detektion, Aktion usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlendes Qualitätssicherungshandbuch	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Organisation zum Schutz der Systemunterlagen und -Wartungsmittel	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlender Plan zur Wiederaufnahme der wesentlichen Aktivitäten innerhalb der Institution	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Prozeduren zur Verwaltung der Systemkonfigurationen	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Nicht-Beachtung der Normen oder Standards bei Entwicklung des Informationssystems	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlender Ausbildungsplan bezüglich der Wartung neuer Systeme	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Auswahl von Technologien ohne Gewährleistung ihrer Beständigkeit	
Entitätstypen	PER_DEC: Entscheidungsträger
Geringes Wartungsbudget	
Entitätstypen	PER_DEC: Entscheidungsträger
Vorhandensein veralteter Komponenten innerhalb der Informationsverarbeitungsinfrastruktur (Entwicklungen in nicht mehr benutzten Programmiersprachen)	
Entitätstypen	PER_DEC: Entscheidungsträger

Nicht-Einhalten der Qualitätsvorschriften	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Fehlende Standards oder Normen	
Entitätstypen	PER_DEV: Entwickler
Nicht-Einhalten der Entwicklungsvorschriften	
Entitätstypen	PER_DEV: Entwickler
Ausbildungsmangel hinsichtlich der korrekten Anwendung der IT-Mittel (Störung des Systems, Installation nicht kompatibler Software usw.)	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung
Benutzung von Softwareprogrammen oder Entwicklungen, die nicht den Institutionsnormen und -standards entsprechen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung
Wartungsfehler	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger
Fehlender Verkabelungsplan	
Entitätstypen	RES_INF: Medien und Informationsträger
Wartung oder Betrieb der Betriebsmittel erfordert die Verfügbarkeit der Netzunterstützungen	
Entitätstypen	RES_INF: Medien und Informationsträger
Wartung oder Betrieb des Systems erfolgt über das Netz	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Fehlende Höchstfristen bei der Unterstützungsgarantie	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Verwendung einer veralteten Version des Betriebssystems oder der Anwendungsprogramme	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Verwendung einer veralteten Version des Mailboxservers	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Verwendung eines veralteten Systems	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Verwendung eines nicht standardmäßigen Systems	
Entitätstypen	SYS_WEB: Externes Portal

	SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Fehlende Nachkontrolle der Installations- und Wartungsprozeduren (Konfigurations- und Parametrierhefte)	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Fehlendes internes Unterstützungsmittel	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 32 - BEEINTRÄCHTIGUNG DER WARTBARKEIT DES INFORMATIONSSYSTEMS	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme

	LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.33 UNZULÄSSIGE BENUTZUNG DER BETRIEBSMITTEL

Fehlende Verwaltung der Lizenzen und der Eintragungs- bzw. Aktiviereinrichtung

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Möglichkeit zur Benutzung einer Backdoor oder eines Trojanischen Pferdes im Betriebssystem

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Gemeinsame Nutzung der Benutzeridentifikation

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Durch die gemeinsame Nutzung der Ressourcen wird der Systemzugriff durch Unbefugte vereinfacht

Entitätstypen	LOG_OS: Betriebssystem

Anschluss des Betriebsmittels an externe Netzwerke

Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware

Das verwendete Betriebsmittel kann zu anderen, ursprünglich nicht vorgesehenen Zwecken eingesetzt werden (z. B. Entwicklung von Software, die nicht für die Institution bestimmt ist)

Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware

Datenträger allgemein zugänglich

Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger

In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen

Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt

Fehlende Sicherheitspolitik zum Schutz der Informationsverarbeitungsinfrastruktur an den verschiedenen Standorten der Institution

Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt

Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten

Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt

Fehlende Sensibilisierung über die Risiken von Sanktionen

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle

Fehlende Vertragsklauseln über die Benutzung von IT-Material

Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Anweisungen hinsichtlich der Benutzung von IT-Material	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Möglichkeit zur freien Benutzung der Ressourcen der Institution (Selbstbedienung)	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Überwachungsprozedur	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Die Sicherheitspolitik wird nicht angewendet	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Informatik-Charta, in der die Benutzungsanforderungen definiert werden	
Entitätstypen	PER_EXP: Betreiber / Wartung PER_DEV: Entwickler ORG_GEN: Organisation der Institution
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Sensibilisierung des Personals über die Risiken von Sanktionen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Die zugestandenen Rechte gehen über den gerechtfertigten Bedarf hinaus	
Entitätstypen	PER_UTI: Benutzer PER_DEC: Entscheidungsträger
Verschaffung eines Vorteils	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Nicht-Einhalten der Informatik-Charta, in der die Benutzungsanforderungen definiert werden	
Entitätstypen	PER_UTI: Benutzer PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Fehlende Kontrolle der materiellen Bedürfnisse bei Entwicklung einer Anwendung	
Entitätstypen	PER_DEV: Entwickler
Fehlende moralische oder ethische Vorschriften	
Entitätstypen	PER_DEV: Entwickler
Fehlende Verwaltung des Betriebsmittelausstattung	
Entitätstypen	PER_EXP: Betreiber / Wartung
Fehlende Prozeduren zur Kontrolle der Ermächtigungen beim Zugang des Personals zum Standort oder zu den Räumlichkeiten	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Prozeduren zur Identitätskontrolle beim Zugang von Personen zu den Räumlichkeiten oder Zonen	
Entitätstypen	PHY_LIE.3: Zone

	PHY_LIE.2: Räumlichkeiten
Fehlende Protokollierung der Personenzugänge	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Sicherung der Kommunikationsleitungen und -ausstattung	
Entitätstypen	PHY_SRV.1: Kommunikation
Die Systemausstattung ermöglicht eine Benutzung der Systemressourcen von außen	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
Die Systemausstattung ist allgemein zugänglich	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
Die Systemausstattung ist an externe Netzwerke angeschlossen	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
Die Systemausstattung kann für andere Zwecke benutzt werden als ursprünglich vorgesehen	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
Die jeweilige Einrichtung kann für andere Zwecke benutzt werden als ursprünglich vorgesehen	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Fehlende Auditierung bzw. Überwachung der Zugänge (v. a. Bestandsaufnahme der Zugänge von außen in die Institution und Typologie der Personenströme)	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Fehlende Zugangsvorschriften	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Anschluss der Einrichtung an externe Netzwerke	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System

Die Einrichtung ist allgemein zugänglich	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System

DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 33 - UNZULÄSSIGE BENUTZUNG DER BETRIEBSMITTEL	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.34 BETRÜGERISCHE KOPIE VON SOFTWAREPROGRAMMEN

Fehlende Verwaltung der Zugriffsprivilegien der einzelnen Profile (Administratoren, Anwender, Gäste usw.)

Entitätstypen	MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Verwaltung der Lizenzen und der Eintragungs- oder Aktiviereinrichtung

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Attraktive Softwareprogramme oder Programme für ein breites Publikum

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Möglichkeit zur problemlosen Kopie von Softwareprogrammen oder Programmpaketen

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Möglichkeit zur problemlosen Kopie von betriebssytemeigenen Distributionen

Entitätstypen	LOG_OS: Betriebssystem

Attraktives Betriebssystem oder Betriebssystem für ein breites Publikum

Entitätstypen	LOG_OS: Betriebssystem

Hardware zur Aufzeichnung von Daten auf Datenträgern (Diskette, ZIP, CD/DVD-Brenner)

Entitätstypen	MAT_ACT.1: Tragbare Hardware

Hardware zur Aufzeichnung von Daten auf Datenträgern (Diskette, ZIP, CD-ROM/DVD-Brenner)

Entitätstypen	MAT_ACT.2: Ortsfeste Hardware

Fehlende Informationen über die für die Informationsverarbeitung spezifischen Gesetze und Vorschriften

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation

In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen

Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt

Fehlende, an den Standorten der Institution vorgeschriebene Politik zur Kontrolle der Lizenzen

Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt

Fehlende Vertragsklausel über die Benutzung von betrügerischen Softwarekopien	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Informatik-Charta, in der die Benutzungsanforderungen definiert werden	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Sensibilisierung über die Risiken von Sanktionen	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Sensibilisierung oder Aufklärung über die Gesetzgebung hinsichtlich der Urheberrechte	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Überwachungsprozedur	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Die Sicherheitspolitik wird nicht angewendet	
Entitätstypen	ORG_GEN: Organisation der Institution
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Verschaffung eines Vorteils	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Nicht-Einhalten der Informatik-Charta, in der die Benutzungsanforderungen definiert werden	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Fehlende Sensibilisierung des Personals über die Risiken von Sanktionen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEC: Entscheidungsträger
Fehlende Prozeduren zur Identitätskontrolle beim Zugang von Personen zu den Räumlichkeiten oder Zonen	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Prozeduren zur Kontrolle der Ermächtigungen beim Zugang des Personals zum Standort oder zu den Räumlichkeiten	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Protokollierung der Personenzugänge	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten

Fehlende Herkunftskontrolle der Anwendungsprogramme vor der Installation

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System

Die Zugangseinrichtung ermöglicht die Speicherung von Softwareprogrammen

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System

Die Zugangseinrichtung ermöglicht das Herunterladen von Softwareprogrammen

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System

DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 34 - BETRÜGERISCHE KOPIE VON SOFTWAREPROGRAMMEN

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software

	LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.35 BENUTZUNG GEFÄLSCHTER ODER KOPIERTER SOFTWAREPROGRAMME

Fehlende Verwaltung der Lizenzen und der Eintragungs- bzw. Aktiviereinrichtung	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Möglichkeit zur problemlosen Kopie von Softwareprogrammen oder Programmpaketen	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Attraktive Softwareprogramme oder Programme für ein breites Publikum	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Möglicherweise funktionieren die Systeme mit unzulässig kopierten oder gefälschten Betriebssystemen	
Entitätstypen	LOG_OS: Betriebssystem
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende, an den Standorten der Institution vorgeschriebene Politik zur Kontrolle der Lizenzen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklausel über die Identifizierung und Überprüfung der Herkunft von Softwareprogrammen	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Sensibilisierung oder Aufklärung über die Gesetzgebung hinsichtlich der Urheberrechte	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Kontrolle der Zertifizierung von Produkten	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Kontrolle der Herkunft von Produkten	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Informatik-Charta, in der die Benutzungsanforderungen definiert werden	
Entitätstypen	ORG_GEN: Organisation der Institution
Die Sicherheitspolitik weist nicht ausdrücklich auf die zivilen, strafrechtlichen und vorschriftsmäßigen Pflichten und Verantwortungen eines jeden hin	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Definition von Zugriffsprivilegien zur Einschränkung der Installationsmöglichkeiten an den Arbeitsstationen	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Fehlende Sensibilisierung des Personals über die Risiken von Sanktionen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung

	PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Nicht-Einhalten der Informatik-Charta, in der die Benutzungsanforderungen definiert werden	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Keine Zertifizierung der Produkte	
Entitätstypen	PER_DEV: Entwickler
Keine Prozedur zur Evaluierung der Produkte	
Entitätstypen	PER_DEV: Entwickler
Fehlende Prozedur und Mittel zur Überprüfung der Herkunft der Software (Codesignatur, Binärsignatur usw.)	
Entitätstypen	PER_DEV: Entwickler
Fehlende Protokollierung der Personenzugänge	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Prozeduren zur Kontrolle der Ermächtigungen beim Zugang des Personals zum Standort oder zu den Räumlichkeiten	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Prozeduren zur Identitätskontrolle beim Zugang von Personen zu den Räumlichkeiten oder Zonen	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Herkunftskontrolle der Anwendungsprogramme vor der Installation	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Die Zugangseinrichtung ermöglicht die Speicherung von Softwareprogrammen	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System

Die Zugangseinrichtung ermöglicht das Herunterladen von Softwareprogrammen

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System

DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 35 - BENUTZUNG GEFÄLSCHTER ODER KOPIERTER SOFTWAREPROGRAMME

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.36 DATENMANIPULATION

Fehlende Kontrolle der Integrität von Produkten

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Ermächtigungsprozedur und -einrichtung zur Datenänderung

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Die Hotline zur Telewartung ist permanent aktiviert

Entitätstypen	SYS_MES: Nachrichtenübermittlung RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Fehlende Beschränkung der Software-Eingangspunkte

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Fehlende Überprüfung der Anwendungsprogramme vor der Installation

Entitätstypen	SYS_MES: Nachrichtenübermittlung LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Fehlender Einsatz von Basis-Sicherheitsregeln, die bezüglich des Betriebssystems und der Softwareprogramme anzuwenden sind

Entitätstypen	SYS_MES: Nachrichtenübermittlung LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Über die Software besteht Zugriff auf die Daten (Inhalt der Festplatte, Datenbank usw.)

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Möglichkeit zur Fern-Systemadministration von jeder beliebigen Arbeitsstation aus	
Entitätstypen	SYS_MES: Nachrichtenübermittlung RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_OS: Betriebssystem
Möglichkeit zur Systemadministration aus der Entfernung mit nicht verschlüsselten Administrationstools	
Entitätstypen	SYS_MES: Nachrichtenübermittlung RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_OS: Betriebssystem
Über das Betriebssystem besteht Zugriff auf die Daten (Datenbank u. ä.)	
Entitätstypen	LOG_OS: Betriebssystem
Unzureichende Komplexität der Zugangspasswörter	
Entitätstypen	SYS_MES: Nachrichtenübermittlung LOG_OS: Betriebssystem
Fehlende Überprüfung des Betriebssystems vor der Installation	
Entitätstypen	LOG_OS: Betriebssystem
Durch die gemeinsame Nutzung der Ressourcen wird der Systemzugriff durch Unbefugte vereinfacht	
Entitätstypen	LOG_OS: Betriebssystem
Möglichkeit zur Systemadministration aus der Entfernung	
Entitätstypen	SYS_MES: Nachrichtenübermittlung RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_OS: Betriebssystem
Die SNMP-Schicht ist aktiviert	
Entitätstypen	SYS_MES: Nachrichtenübermittlung RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_OS: Betriebssystem
Fehlende Datenschutzvorschriften	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Die Hardware kann von jedermann von einem beliebigen Peripheriegerät aus gebootet werden (z. B. Diskette, CD-ROM)	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Veraltete Betriebsmittel	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Redundanz oder Speicherprozedur	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware
Abnutzung der Datenträger	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT.3: Verarbeitungsperipheriegerät
Fehlende Mittel zum Schutz und zur Kontrolle der Integrität der Daten	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT.3: Verarbeitungsperipheriegerät

Fehlende Vorschriften und fehlende Prozedur zur Ermächtigung des Personals	
Entitätstypen	ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Fehlen der an den Standorten der Institution vorgeschriebenen Politik zur Verwaltung und Kontrolle der Zugangsermächtigungen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende, an den Standorten der Institution vorgeschriebene Datenschutzpolitik	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Politik bezüglich der Ermächtigungen zum Informationszugriff	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Absicherung der Zugänge zum IS (Gateways, Intrusionsdetektion, Überwachung der Sicherheitsereignisse usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Vertragsklauseln über den Schutz des IT-Materials	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Kontrolle bezüglich der Anwendung der Sicherheitspolitik	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Anweisungen hinsichtlich der Benutzung von IT-Material	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Vorbeugung und Detektion von Viren und sonstigen Softwareprogrammen mit böser Absicht	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Informationszugriffskontrolle	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlender Ausbildungsplan im Hinblick auf Sicherheitsprobleme	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Prozedur zur Kontrolle externer Disketten	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Informatik-Charta, in der die Benutzungsanforderungen definiert werden	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Nicht-Einhalten der Informatik-Charta, in der die Benutzungsanforderungen definiert werden	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlender Schutz und fehlende Klassifizierung der Informationen	
Entitätstypen	PER_UTI: Benutzer

	PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Sensibilisierung des Personals über die Risiken von Sanktionen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Manipulierbares Personal	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Konfliktgeladenes Klima zwischen den einzelnen Personen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Prozeduren zur Identitätskontrolle beim Zugang von Personen zu den Räumlichkeiten oder Zonen	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Prozeduren zur Kontrolle der Ermächtigungen beim Zugang des Personals zum Standort oder zu den Räumlichkeiten	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Protokollierung der Personenzugänge	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Sicherung der Kommunikationsleitungen und -ausstattung	
Entitätstypen	PHY_SRV.1: Kommunikation
Fehlender physischer und logischer Schutz (z. B durch Abtrennung)	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
Möglichkeit zur Einwirkung auf die über ein Kommunikationsmedium übertragenen Date	
Entitätstypen	RES_INF: Medien und Informationsträger

Das Netzwerk lässt es zu, Systemressourcen zu ändern oder auf sie einzuwirken	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Das Netzwerk vereinfacht die Nutzung von Ressourcen durch Unbefugte	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Fehlende robuste Einrichtung zur Zugangskontrolle	
Entitätstypen	RES_REL: Passives oder aktives Relais
Fehlende Speicherprozedur	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_ANU: Unternehmensverzeichnis
Die Einrichtung ermöglicht das Löschen, Ändern oder Installieren von Programmen aus der Entfernung	
Entitätstypen	SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang
Über die Einrichtung können feindselige Programme wie z. B. Trojanische Pferde, Viren, Würmer oder logische Bomben eingeschleust werden	
Entitätstypen	SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang
Die Einrichtung ermöglicht eine Ausnutzung des Asynchronbetriebs bestimmter Bereiche oder Befehle des Betriebssystems (z. B. Javascript-Komponenten zur Erkundung des Inhalts der Festplatte)	
Entitätstypen	SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang
Fehlende Abtrennung der Kommunikationsnetze	
Entitätstypen	SYS_ITR: Intranet
Die Mailfunktion ermöglicht eine Ausnutzung des Asynchronbetriebs bestimmter Bereiche oder Befehle des Betriebssystems (z. B. automatischer Start von Anhängen)	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Fehlende Auditierung bzw. Überwachung der Zugänge	
Entitätstypen	SYS_WEB: Externes Portal
Fehlende Zugangsvorschriften	
Entitätstypen	SYS_WEB: Externes Portal
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 36 - DATENMANIPULATION	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung

	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.37 UNZULÄSSIGE VERARBEITUNG VON DATEN

Jedermann zugängliche Software (z. B. zur Fernadministration einer Station ist kein Passwort erforderlich)
Entitätstypen: LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Fehlende Verschlüsselungseinrichtung
Entitätstypen: LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Möglichkeit zur Benutzung einer Backdoor oder eines Trojanischen Pferdes im Betriebssystem
Entitätstypen: LOG_STD: Programmpaket oder Standard-Software LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Möglichkeit, mehrere Betriebssysteme auf dem gleichen Rechner zu betreiben (z. B. Zugang zu NTFS-Partitionen via Linux)
Entitätstypen: LOG_OS: Betriebssystem
Möglichkeit zur Benutzung einer Backdoor oder eines Trojanischen Pferdes im Betriebssystem
Entitätstypen: LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
Fehlender physischer Schutz
Entitätstypen: MAT_ACT.3: Verarbeitungsperipheriegerät
Fehlendes Mittel zur Identifizierung der Sensibilität der auf den Datenträgern enthaltenen Informationen
Entitätstypen: MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Datenträger allgemein zugänglich
Entitätstypen: MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Attraktive Datenträger (Marktwert und technologische und strategische Werte)
Entitätstypen: MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Mobile oder leicht zu transportierende Datenträger (z. B. Disketten, ZIP, externe Festplatten)
Entitätstypen: MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Fehlendes Mittel zur Verschlüsselung
Entitätstypen: MAT_PAS.1: Elektronischer Datenträger
Fehlende Prozedur und fehlendes Mittel zur Vernichtung
Entitätstypen: MAT_PAS.1: Elektronischer Datenträger
Fehlende Informationen über die für die Informationsverarbeitung spezifischen Gesetze und Vorschriften

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende, an den Standorten der Institution vorgeschriebene Datenschutzpolitik	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklausel über die Vertraulichkeit	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Verschlüsselungseinrichtung	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Anweisungen zum Verhalten bei Zwischenfällen (Detektion, Aktion usw.)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Informationszugriffskontrolle	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Sensibilisierung bezüglich der individuellen Verantwortungen	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlender Verantwortlicher für den Individuen-spezifischen Daten- und Informationsschutz	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Nicht-Anwendung der Sicherheitspolitik, insbesondere was die Bearbeitung nominativer Daten anbelangt	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Sensibilisierung des Personals	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Fehlender Schutz und fehlendes Audit bezüglich des Zugriffs auf sensitive Informationen	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Fehlende Sensibilisierung des Personals über die Risiken von Sanktionen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Schulung über die Bedingungen einer zulässigen Nutzung von Informationen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlender Schutz und fehlende Klassifizierung der Informationen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal

Fehlende Kenntnis der Sicherheitsmaßnahmen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Existenz eines unzulässigen Abhörpunkts	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger
Fehlende Identifizierung der Schutzniveaus der Systeme	
Entitätstypen	SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis
Fehlende Kontrolle des Inhalts	
Entitätstypen	SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis
Fehlende Auditierung bzw. Überwachung der Zugänge	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis
Fehlende Verwaltung der Zugangsermächtigungen	
Entitätstypen	SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis
Die Einrichtung vereinfacht die Verbreitung von Informationen nach außen	
Entitätstypen	SYS_MES: Nachrichtenübermittlung SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis
Anschluss der Einrichtung an externe Netzwerke	
Entitätstypen	SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 37 - UNZULÄSSIGE VERARBEITUNG VON DATEN	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte

	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.38 BENUTZUNGSFEHLER

Fehlende klare Dokumentation über die Anwendungssysteme

Entitätstypen	LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Mangelnde Kompetenz des Benutzers

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_INT: Kommunikationsschnittstelle MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Fehlende Test- und Abnahmeprozedur gemäß den Spezifikationen

Entitätstypen	LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Fehlende Validierung der Eingangsdaten (Erfassungsdaten)

Entitätstypen	LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Fehlende Verantwortung

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Komplexe Benutzungsanwendung

Entitätstypen	LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Informationsmedien sind dem Benutzer nicht zugänglich

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang

	SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Keine intuitive Benutzung der Software	
Entitätstypen	LOG_OS: Betriebssystem
Fehlende Kompetenz	
Entitätstypen	LOG_OS: Betriebssystem
Informationsmedien nicht zugänglich	
Entitätstypen	LOG_OS: Betriebssystem
Fehlende Schulung bezüglich der Nutzung oder Wartung neuer Softwareprogramme	
Entitätstypen	LOG_OS: Betriebssystem
Komplex anzuwendende Software	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
Komplex anzuwendende und wenig ergonomische Hardware	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware
Schlechte Nutzungsbedingungen	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware
Möglichkeit, dass bestimmte Betriebsmittel schädliche Einwirkungen auf das benutzende Personal haben (Arbeiten am Bildschirm, Wellen usw.)	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Labelisierung der Datenträger	

Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Komplex anzuwendende und wenig ergonomische Datenträger	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Fehlende Kontrolle kritischer Prozesse durch die Mutterorganisation	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende doppelte Kontrolle kritischer Prozesse	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Schulung bezüglich der zum Einsatz kommenden Hardware- und Softwarekomponenten	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Schlechte Kenntnis der Verantwortungen	
Entitätstypen	PER_DEC: Entscheidungsträger
Fehlende Formalisierung der allgemein bekannten Verantwortungen	
Entitätstypen	PER_DEC: Entscheidungsträger
Ungünstige Arbeitsbedingungen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Fehlender Professionalismus	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Nicht-Einhalten der Anweisungen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Benutzendes Personal nur wenig oder schlecht ausgebildet	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Vorhandensein von hochsensitiven Operationen, die von einer einzelnen Person ausgeführt werden können	
Entitätstypen	PER_DEC: Entscheidungsträger
Fehlende Benutzungsunterlagen über die vorhandenen Anwendungsprogramme	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Fehlende Motivation für Arbeiten, die mit der Datenerfassung zu tun haben	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Mit der Datenerfassung wenig vertrautes Personal	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung

	PER_DEV: Entwickler
Ungünstige Arbeitsumgebung (zu kleine Räume, kein Platz zum Wegräumen usw.)	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlende Etikettierung von Kabeln oder fehlender Kabelplan	
Entitätstypen	PHY_SRV.1: Kommunikation
Platzmangel in den technischen Räumlichkeiten	
Entitätstypen	PHY_SRV.1: Kommunikation
Fehlende Betriebsprozedur	
Entitätstypen	PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie
Fehlende Etikettierung und fehlendes Architekturschema auf neuestem Stand	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger
Fehlender Verkabelungsplan	
Entitätstypen	RES_INF: Medien und Informationsträger
Schnittstelle enthält landesspezifische technische Merkmale (z. B. verschiedene Telefonsteckertypen zwischen Frankreich und Großbritannien)	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Medien und Informationsträger enthalten technische Merkmale, die sie lokalisierbar machen (z. B. verschiedene ADSl-Konfigurationsparameter zwischen Frankreich und Großbritannien)	
Entitätstypen	RES_REL: Passives oder aktives Relais
Fehlende Schutzmaßnahmen (nur Lesemodus z. B.)	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Fehlendes Überwachungstool	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 38 - BENUTZUNGSFEHLER	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten

	PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.39 RECHTSMISSBRAUCH

Fehlende Audit-Politik

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Fehlende Speicherung der Ereignisjournale

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Fehlende Ereignisprotokollierung

Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun

Komplexe bzw. wenig ergonomische Dateien

Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_OS: Betriebssystem

Unzureichende Komplexität der Zugangspasswörter

Entitätstypen	LOG_OS: Betriebssystem

Möglichkeit zur Systemadministration aus der Entfernung mit nicht verschlüsselten Administrationstools

Entitätstypen	LOG_OS: Betriebssystem

Die Passwörter-Datenbank des Betriebssystems ist entschlüsselbar

Entitätstypen	LOG_OS: Betriebssystem

Die SNMP-Schicht ist aktiviert

Entitätstypen	LOG_OS: Betriebssystem

Möglicherweise wird das Betriebssystem mit unkorrekten Anfragen bzw. Daten konfrontiert (z. B. Buffer overflow)

Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_OS: Betriebssystem

Die Hotline zur Telewartung ist permanent aktiviert

Entitätstypen	LOG_OS: Betriebssystem

Möglichkeit zur Systemadministration aus der Entfernung

Entitätstypen	LOG_OS: Betriebssystem
Die Logs und Journale des Betriebssystem können von jedermann geändert werden	
Entitätstypen	LOG_OS: Betriebssystem
Durch die gemeinsame Nutzung der Ressourcen wird der Systemzugriff durch Unbefugte vereinfacht	
Entitätstypen	LOG_OS: Betriebssystem
Das Betriebssystem ist allgemein zugänglich und von jedermann benutzbar (z. B. über das Konto "Gast")	
Entitätstypen	LOG_OS: Betriebssystem
Das Betriebssystem protokolliert keine Logs oder Systemereignisse	
Entitätstypen	LOG_OS: Betriebssystem
Das Betriebssystem ermöglicht die Herstellung anonymer Verbindungen	
Entitätstypen	LOG_OS: Betriebssystem
Das Betriebssystem ermöglicht das Öffnen einer Session ohne Passwort	
Entitätstypen	LOG_OS: Betriebssystem
Möglichkeit zur Fern-Systemadministration von jeder beliebigen Arbeitsstation aus	
Entitätstypen	LOG_OS: Betriebssystem
Verwendung einer veralteten Version des Betriebssystems oder der Anwendungsprogramme	
Entitätstypen	LOG_OS: Betriebssystem
Die Passwörter zum Zugang zum Betriebssystem sind entschlüsselbar	
Entitätstypen	LOG_OS: Betriebssystem
Möglichkeit, mehrere Betriebssysteme auf dem gleichen Rechner zu betreiben (z. B. Zugang zu NTFS-Partitionen via Linux)	
Entitätstypen	LOG_OS: Betriebssystem
Jedermann zugängliche Software (z. B. zur Fernadministration einer Station ist kein Passwort erforderlich)	
Entitätstypen	LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
Fehlender physischer Schutz	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende robuste Einrichtung zur Zugangskontrolle	
Entitätstypen	MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlendes Audit über die Prozeduren bezüglich der physischen Zugriffskontrolle	
Entitätstypen	MAT_PAS.2: Sonstige Datenträger
Fehlen der an den Standorten der Institution vorgeschriebenen Politik zur Verwaltung und Kontrolle der Ermächtigungen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklauseln zur Begrenzung der Verantwortungen beider Parteien	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Definition des Begriffs "Informationsanspruch"	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems

	ORG_GEN: Organisation der Institution
Fehlende Einrichtung zur Kontrolle und Verhängung von Sanktionen	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Verordnung, mit Definition der Rechte	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Die Zuweisungen von Benutzerrechten sind nicht klar definiert	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Kontrolle hinsichtlich der Zuweisung von Benutzerrechten	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Vorrangstellung von Personalkategorien	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Vorhandensein von hochsensitiven Operationen, die von einer einzelnen Person ausgeführt werden können	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Verschaffung eines Vorteils	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Definition des Begriffs "Recht" für das Personal	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Prozeduren zur Kontrolle der Ermächtigungen beim Zugang des Personals zum Standort oder zu den Räumlichkeiten	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlender physischer und logischer Schutz	
Entitätstypen	RES_INF: Medien und Informationsträger
Der Least-Privileg-Grundsatz wird nicht angewendet	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis

	SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Möglichkeit zur Benutzung von Betriebsmitteln ohne Hinterlassen von Spuren	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Die Einrichtung ist allgemein zugänglich	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 39 - RECHTSMISSBRAUCH	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.40 RECHTSANMASSUNG

Fehlende Audit-Politik	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Fehlende Speicherung der Ereignisjournale	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Fehlende Ereignisprotokollierung	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Die Logs und Journale des Betriebssystem können von jedermann geändert werden	
Entitätstypen	LOG_OS: Betriebssystem
Das Betriebssystem ermöglicht das Öffnen einer Session ohne Passwort	
Entitätstypen	LOG_OS: Betriebssystem
Das Betriebssystem ermöglicht die Herstellung anonymer Verbindungen	
Entitätstypen	LOG_OS: Betriebssystem
Das Betriebssystem protokolliert keine Logs oder Systemereignisse	
Entitätstypen	LOG_OS: Betriebssystem
Das Betriebssystem ist allgemein zugänglich und von jedermann benutzbar (z. B. über das Konto "Gast")	
Entitätstypen	LOG_OS: Betriebssystem
Durch die gemeinsame Nutzung der Ressourcen wird der Systemzugriff durch Unbefugte vereinfacht	
Entitätstypen	LOG_OS: Betriebssystem
Die Passwörter-Datenbank des Betriebssystems ist entschlüsselbar	
Entitätstypen	LOG_OS: Betriebssystem
Die SNMP-Schicht ist aktiviert	
Entitätstypen	SYS_MES: Nachrichtenübermittlung LOG_OS: Betriebssystem
Komplexe bzw. wenig ergonomische Dateien	
Entitätstypen	RES_REL: Passives oder aktives Relais

	RES_INT: Kommunikationsschnittstelle LOG_OS: Betriebssystem
Möglichkeit zur Systemadministration aus der Entfernung mit nicht verschlüsselten Administrationstools	
Entitätstypen	SYS_MES: Nachrichtenübermittlung LOG_OS: Betriebssystem
Möglichkeit zur Systemadministration aus der Entfernung	
Entitätstypen	SYS_MES: Nachrichtenübermittlung RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_OS: Betriebssystem
Die Hotline zur Telewartung ist permanent aktiviert	
Entitätstypen	SYS_MES: Nachrichtenübermittlung RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle LOG_OS: Betriebssystem
Die Passwörter zum Zugang zum Betriebssystem sind entschlüsselbar	
Entitätstypen	LOG_OS: Betriebssystem
Unzureichende Komplexität der Zugangspasswörter	
Entitätstypen	SYS_MES: Nachrichtenübermittlung LOG_OS: Betriebssystem
Verwendung einer veralteten Version des Betriebssystems oder der Anwendungsprogramme	
Entitätstypen	SYS_MES: Nachrichtenübermittlung LOG_OS: Betriebssystem
Möglicherweise wird das Betriebssystem mit unkorrekten Anfragen bzw. Daten konfrontiert (z. B. Buffer overflow)	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_OS: Betriebssystem
Möglichkeit, mehrere Betriebssysteme auf dem gleichen Rechner zu betreiben (z. B. Zugang zu NTFS-Partitionen via Linux)	
Entitätstypen	LOG_OS: Betriebssystem
Möglichkeit zur Fern-Systemadministration von jeder beliebigen Arbeitsstation aus	
Entitätstypen	SYS_MES: Nachrichtenübermittlung LOG_OS: Betriebssystem
Jedermann zugängliche Software (z. B. zur Fernadministration einer Station ist kein Passwort erforderlich)	
Entitätstypen	LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
Anschluss des Betriebsmittels an externe Netzwerke	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende robuste Einrichtung zur Zugangskontrolle	
Entitätstypen	RES_REL: Passives oder aktives Relais MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Fehlende Abtrennung der Systemausstattung	
Entitätstypen	MAT_ACT.3: Verarbeitungsperipheriegerät
Fehlender Schutz der Datenträger	
Entitätstypen	MAT_PAS.1: Elektronischer Datenträger
Fehlendes Audit über die Prozeduren bezüglich der physischen Zugriffskontrolle	
Entitätstypen	MAT_PAS.2: Sonstige Datenträger

Die Verantwortlichen haben keinen Kontakt zu den technologischen Prüf- und Überwachungsdiensten	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vorschriften und fehlende Prozedur zur Ermächtigung des Personals	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Sensibilisierung über die Risiken von Sanktionen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Überwachungsprozedur	
Entitätstypen	ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Möglichkeit zur freien Benutzung der Ressourcen der Institution (Selbstbedienung)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlender Schutz der Bereiche, die dem Austausch bzw. der gemeinsamen Nutzung von Informationen vorbehalten sind	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Prozedur zur Ermächtigung des Personals	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Kein Klima des Vertrauens untereinander	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Die Sicherheitsverantwortungen bezüglich der Ermächtigungsverwaltung sind nicht formalisiert	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Kommunikation und Unterrichtung des Personals bezüglich der Ermächtigungsprozeduren	
Entitätstypen	ORG_GEN: Organisation der Institution
Fehlende Prozedur hinsichtlich der Informationsweitergabe im Falle von Detektionen	
Entitätstypen	ORG_GEN: Organisation der Institution
Die Sicherheitspolitik wird nicht angewendet	
Entitätstypen	ORG_GEN: Organisation der Institution
Unangepasste Organisation	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Die zugestandenen Rechte gehen über den gerechtfertigten Bedarf hinaus	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Konfliktgeladenes Klima zwischen den einzelnen Personen	
Entitätstypen	PER_UTI: Benutzer

	PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende moralische oder ethische Vorschriften	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Verschaffung eines Vorteils	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Vorhandensein von hochsensitiven Operationen, die von einer einzelnen Person ausgeführt werden können	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Für das Personal unangemessene Missionen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Fehlende Prozeduren zur Kontrolle der Ermächtigungen beim Zugang des Personals zum Standort oder zu den Räumlichkeiten	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Fehlender physischer und logischer Schutz (z. B durch Abtrennung)	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk
Fehlende Netzabtrennung	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger
Die Schnittstellen sind an externe Netzwerke angeschlossen	
Entitätstypen	RES_INF: Medien und Informationsträger
Die Informationsträger und Kommunikationsmedien sind an externe Netzwerke angeschlossen	
Entitätstypen	RES_INF: Medien und Informationsträger
Technische Merkmale können geändert werden (z. B. MAC-Adresse einer Ethernet-Karte)	
Entitätstypen	RES_INF: Medien und Informationsträger

Fehlender physischer Schutz	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger
Das Netzwerk lässt es zu, Systemressourcen zu ändern oder auf sie einzuwirken	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Verwendung eines Protokolls ohne Authentifizierungsfunktion	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Die Schnittstellen sind allgemein zugänglich	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Das Netzwerk ermöglicht eine problemlose Nutzung der Ressourcen durch Unbefugte	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Die Relais identifizieren weder die Quellen noch die Ziele (mögliche Auswirkungen: Anfälligkeit des Systems für Spoofing-Angriffe)	
Entitätstypen	RES_REL: Passives oder aktives Relais
Die Einrichtung ist allgemein zugänglich	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis
Möglicherweise wird die Einrichtung mit unkorrekten Anfragen bzw. Daten konfrontiert (z. B. Buffer overflow)	
Entitätstypen	SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis
Fehlende Überprüfung der Anwendungsprogramme vor der Installation	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Die Einrichtung zur Nachrichtenübermittlung ist über Internet zugänglich	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
Verwendung einer veralteten Version des Mailboxservers	
Entitätstypen	SYS_MES: Nachrichtenübermittlung
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 40 - RECHTSANMASSUNG	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten

PHY_LIE.1: Äußere Umgebung
PER_UTI: Benutzer
PER_EXP: Betreiber / Wartung
PER_DEV: Entwickler
PER_DEC: Entscheidungsträger
PER: Personal
ORG_PRO: Organisation eines Projekts oder eines Systems
ORG_GEN: Organisation der Institution
ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
ORG_DEP: Organisation, von der die Institution abhängt
ORG: Organisation
MAT_PAS: Datenträger (passiv)
MAT_PAS.2: Sonstige Datenträger
MAT_PAS.1: Elektronischer Datenträger
MAT_ACT: Datenverarbeitungsmittel (aktiv)
MAT_ACT.3: Verarbeitungsperipheriegerät
MAT_ACT.2: Ortsfeste Hardware
MAT_ACT.1: Tragbare Hardware
MAT: Hardware
LOG_STD: Programmpaket oder Standard-Software
LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
LOG_OS: Betriebssystem
LOG_APP: Tätigkeitsgebundene Anwendung
LOG_APP.2: Tätigkeitsgebundene Sonderanwendung
LOG_APP.1: Tätigkeitsgebundene Standardanwendun
LOG: Software

4.41 VERLEUGNUNG VON AKTIONEN

Fehlende Audit-Politik	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software
Fehlende Speicherung der Ereignisjournale	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Fehlende Ereignisprotokollierung	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun
Das Betriebssystem protokolliert keine Logs oder Systemereignisse	
Entitätstypen	LOG_OS: Betriebssystem
Die SNMP-Schicht ist aktiviert	
Entitätstypen	LOG_OS: Betriebssystem
Möglichkeit zur Systemadministration aus der Entfernung mit nicht verschlüsselten Administrationstools	
Entitätstypen	LOG_OS: Betriebssystem
Komplexe bzw. wenig ergonomische Dateien	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger LOG_OS: Betriebssystem
Unzureichende Komplexität der Zugangspasswörter	
Entitätstypen	LOG_OS: Betriebssystem
Die Passwörter zum Zugang zum Betriebssystem sind entschlüsselbar	
Entitätstypen	LOG_OS: Betriebssystem
Die Passwörter-Datenbank des Betriebssystems ist entschlüsselbar	
Entitätstypen	LOG_OS: Betriebssystem
Das Betriebssystem ermöglicht die Herstellung anonymer Verbindungen	
Entitätstypen	LOG_OS: Betriebssystem

Möglicherweise wird das Betriebssystem mit unkorrekten Anfragen bzw. Daten konfrontiert (z. B. Buffer overflow)	
Entitätstypen	LOG_STD: Programmpaket oder Standard-Software LOG_OS: Betriebssystem
Möglichkeit zur Fern-Systemadministration von jeder beliebigen Arbeitsstation aus	
Entitätstypen	LOG_OS: Betriebssystem
Verwendung einer veralteten Version des Betriebssystems oder der Anwendungsprogramme	
Entitätstypen	LOG_OS: Betriebssystem
Das Betriebssystem ist allgemein zugänglich und von jedermann benutzbar (z. B. über das Konto "Gast")	
Entitätstypen	LOG_OS: Betriebssystem
Möglichkeit zur Systemadministration aus der Entfernung	
Entitätstypen	LOG_OS: Betriebssystem
Die Logs und Journale des Betriebssystem können von jedermann geändert werden	
Entitätstypen	LOG_OS: Betriebssystem
Möglichkeit, mehrere Betriebssysteme auf dem gleichen Rechner zu betreiben (z. B. Zugang zu NTFS-Partitionen via Linux)	
Entitätstypen	LOG_OS: Betriebssystem
Das Betriebssystem ermöglicht das Öffnen einer Session ohne Passwort	
Entitätstypen	LOG_OS: Betriebssystem
Die Hotline zur Telewartung ist permanent aktiviert	
Entitätstypen	LOG_OS: Betriebssystem
Durch die gemeinsame Nutzung der Ressourcen wird der Systemzugriff durch Unbefugte vereinfacht	
Entitätstypen	LOG_OS: Betriebssystem
Jedermann zugängliche Software (z. B. zur Fernadministration einer Station ist kein Passwort erforderlich)	
Entitätstypen	LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme
Fehlende Einrichtung für Protokolldaten und Audits	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Die Hardware ist allgemein zugänglich und von jedermann benutzbar	
Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware
Datenträger allgemein zugänglich	
Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger
Fehlende Prozedur über den Zugriff auf klassifizierte Informationen	
Entitätstypen	MAT_PAS.2: Sonstige Datenträger
Änderung der Organisationspolitik oder -strategie	
Entitätstypen	PER_UTI: Benutzer PER_DEC: Entscheidungsträger ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Definition der Verantwortungen	

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
In der Betriebsordnung werden mit keinem Thema die Sicherheitsverantwortungen im Hinblick auf die Informationssysteme angesprochen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Disziplinarverfahren	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt
Tiefgreifende politisch-wirtschaftliche Konsequenzen absehbar	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Globalpolitik zur Verwaltung und Archivierung von Protokolldaten und sonstigen Beweiselementen	
Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt
Fehlende Vertragsklausel über die Definition von Prozeduren für Kommunikation und Datenaustausch	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende gegenseitige Code-Kontrolle	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Übertriebene oder nicht dem Kontext angepasste Straf- oder Sanktionsklausel	
Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle
Fehlende Mechanismen zur Weiterverfolgung von Aktionen und Ereignis- oder Alarmjournalen	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Möglichkeit zur freien Benutzung der Ressourcen der Institution (Selbstbedienung)	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution
Fehlende Hierarchisierung der Organisation und fehlende Reporting-Prozedur	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Keine Unterscheidung zwischen Auditfunktionen und Funktionen zur Nachkontrolle	
Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Die Anwendung der Sicherheitspolitik wird durch die Direktion nicht gefördert	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal
Verschaffung eines Vorteils	
Entitätstypen	PER_UTI: Benutzer PER_DEC: Entscheidungsträger
Fehlendes Vertrauen in die Organisation	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Verantwortung jedes einzelnen unbekannt	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger

Konfliktgeladenes Klima zwischen den einzelnen Personen	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger
Fehlende Protokollierung der ein- und ausgehenden Personen	
Entitätstypen	PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten
Die Relais sind allgemein zugänglich	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger
Das Kommunikationsmedium ermöglicht eine Benutzung des Systems von außen	
Entitätstypen	RES_INF: Medien und Informationsträger
Die Informationsträger und Kommunikationsmedien sind allgemein zugänglich und standardmäßig aktiv (z. B. alle angeschlossenen RJ45-Stecker)	
Entitätstypen	RES_INF: Medien und Informationsträger
Das Netzwerk vereinfacht die Nutzung von Ressourcen durch Unbefugte	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Das Protokoll erlaubt keine eindeutige Identifizierung des Absenders	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Das Netzwerk lässt es zu, Systemressourcen zu ändern oder auf sie einzuwirken	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle
Das Protokoll ermöglicht nicht den Versand einer Empfangsbestätigung	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Möglichkeit zur Benutzung von Betriebsmitteln ohne Hinterlassen von Spuren	
Entitätstypen	RES_INT: Kommunikationsschnittstelle
Die Zugangseinrichtung protokolliert keine betriebsspezifischen Protokolldaten	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Der Zugriff zur Protokolliereinrichtung ist nicht geschützt	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Die Einrichtung ist allgemein zugänglich (z. B. keine Authentifizierung der Client-Stationen oder der Benutzer durch die Einrichtung)	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
Anschluss der Einrichtung an externe Netzwerke	
Entitätstypen	SYS_WEB: Externes Portal

	SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 41 - VERLEUGNUNG VON AKTIONEN	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

4.42 BEEINTRÄCHTIGUNG DER PERSONALVERFÜGBARKEIT

Möglichkeit, dass bestimmte Betriebsmittel schädliche Einwirkungen auf das benutzende Personal haben (Arbeiten am Bildschirm, Wellen usw.)

Entitätstypen	MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware

Fehlende Prozedur zur Archivierung

Entitätstypen	MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger

Ungünstiges soziales Klima

Entitätstypen	ORG_DEP: Organisation, von der die Institution abhängt

Politisch-wirtschaftlicher Konflikt zwischen dem Mutterland der Organisation und dem gastgebenden Land der Institution

Entitätstypen	ORG_GEN: Organisation der Institution ORG_DEP: Organisation, von der die Institution abhängt

Fehlende Klausel oder Vorschriften zum Thema Wissenstransfer

Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle

Fehlende finanzielle oder technologische Beständigkeit der Institution

Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle

Fehlende Klausel über die Kontinuität bei der Erbringung von Dienstleistungen

Entitätstypen	ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle

Fehlende Einheit zum Schutz des Personals

Entitätstypen	ORG_GEN: Organisation der Institution

Ausbruch einer lokalen Virusepidemie

Entitätstypen	ORG_GEN: Organisation der Institution

Fehlende Prozeduren im Hinblick auf den Wissenstransfer

Entitätstypen	PER_UTI: Benutzer ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution

Soziales Klima innerhalb der Organisation nicht förderlich für die Aktivität

Entitätstypen	ORG_GEN: Organisation der Institution

Fehlender Plan zur Sensibilisierung und Schulung in Prozessen zur Kontinuität der beruflichen Aktivität

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution

Fehlende Verwaltungsprozesse zur Kontinuität der beruflichen Aktivität innerhalb der Institution

Entitätstypen	ORG_GEN: Organisation der Institution

Unterdimensionierung der Organisation

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems

Keine Redundanz des strategischen Personals

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems

Fehlende redundante Organisation der sensitiven Funktionen

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems

Fehlende Verwaltungsprozesse zur Kontinuität der beruflichen Aktivität innerhalb der Projektgruppe

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems

Fehlende Unterlagendatenbank über Vorschriften und Prozeduren

Entitätstypen	ORG_PRO: Organisation eines Projekts oder eines Systems
Nichtverfügbarkeit infolge konkurrenzieller Belange	
Entitätstypen	PER_DEC: Entscheidungsträger
Nichtverfügbarkeit auf Grund von Krankheit	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Nichtverfügbarkeit durch Fernbleiben von der Arbeit	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Provozierte Nichtverfügbarkeit (Überfall, Geiselnahme usw.)	
Entitätstypen	PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Soziale Probleme	
Entitätstypen	PER_EXP: Betreiber / Wartung PER_DEV: Entwickler
Konfliktgeladenes soziales Klima	
Entitätstypen	PER_UTI: Benutzer
Schwieriges soziales Klima mit möglichen Streiks in den Transportbetrieben	
Entitätstypen	PHY_LIE.1: Äußere Umgebung
Unterbringung des Fachpersonals in großer Entfernung	
Entitätstypen	PHY_LIE.2: Räumlichkeiten
Wohnsitze der Mitarbeiter in großer Entfernung	
Entitätstypen	PHY_LIE.2: Räumlichkeiten
Mögliche schädliche Einwirkung auf das benutzende Personal (Übertragung per Funk, Wellen usw.)	
Entitätstypen	RES_REL: Passives oder aktives Relais RES_INF: Medien und Informationsträger
DURCH DIE ANGRIFFSMETHODE BEDINGTE SCHWACHSTELLEN 42 - BEEINTRÄCHTIGUNG DER PERSONALVERFÜGBARKEIT	
Entitätstypen	SYS_WEB: Externes Portal SYS_MES: Nachrichtenübermittlung SYS_ITR: Intranet SYS_INT: Einrichtung für Internetzugang SYS_ANU: Unternehmensverzeichnis SYS: System RES_REL: Passives oder aktives Relais RES_INT: Kommunikationsschnittstelle RES_INF: Medien und Informationsträger RES: Netzwerk PHY_SRV: Wesentlicher Dienst PHY_SRV.3: Abkühlung / Verschmutzung PHY_SRV.2: Energie PHY_SRV.1: Kommunikation PHY_LIE: Orte PHY_LIE.3: Zone PHY_LIE.2: Räumlichkeiten PHY_LIE.1: Äußere Umgebung PER_UTI: Benutzer PER_EXP: Betreiber / Wartung PER_DEV: Entwickler PER_DEC: Entscheidungsträger PER: Personal

	ORG_PRO: Organisation eines Projekts oder eines Systems ORG_GEN: Organisation der Institution ORG_EXT: Unterauftragnehmer / Lieferanten / Industrielle ORG_DEP: Organisation, von der die Institution abhängt ORG: Organisation MAT_PAS: Datenträger (passiv) MAT_PAS.2: Sonstige Datenträger MAT_PAS.1: Elektronischer Datenträger MAT_ACT: Datenverarbeitungsmittel (aktiv) MAT_ACT.3: Verarbeitungsperipheriegerät MAT_ACT.2: Ortsfeste Hardware MAT_ACT.1: Tragbare Hardware MAT: Hardware LOG_STD: Programmpaket oder Standard-Software LOG_SRV: Dienst-, Wartungs- oder Administrationsprogramme LOG_OS: Betriebssystem LOG_APP: Tätigkeitsgebundene Anwendung LOG_APP.2: Tätigkeitsgebundene Sonderanwendung LOG_APP.1: Tätigkeitsgebundene Standardanwendun LOG: Software

Formular zur Meinungsäußerung

Dieses Formular kann an folgende Adresse gesendet werden:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identifizierung der Beitrags
Name und Institution (fakultativ): .....
Elektronische Adresse: .....
Datum: .....

Allgemeine Bemerkungen zu diesem Dokument
Entspricht das Dokument Ihren Bedarfe? Ja ☐ Nein ☐

Wenn ja:

Glauben Sie, dass es vom Inhalt her verbessert werden könnte? Ja ☐ Nein ☐

Wenn ja:

Was haben Sie vermisst?
.....
.....

Welche Teile des Dokuments erscheinen Ihnen überflüssig oder unangemessen?
.....
.....

Glauben Sie, dass es von der Form her verbessert werden könnte? Ja ☐ Nein ☐

Wenn ja:

In welchem Bereich ist es verbesserungsfähig?
- Leserlichkeit, Verständnis ☐
- Aufmachung ☐
- Sonstiges ☐

Formulieren Sie Ihre Wünsche bezüglich der Form:
.....
.....

Wenn nein:

Geben Sie den Bereich an, der Ihnen nicht gefällt und umschreiben Sie, was Ihnen gefallen hätte:
.....
.....

Welche weiteren Themen hätten Sie gerne vorgefunden?
.....
.....

Spezielle Bemerkungen zu diesem Dokument

In nachstehender Tabelle können Sie detailliert Stellung nehmen.

Unter Nr. ist die Laufnummer einzutragen.

In die Spalte "Typ" sind zwei Buchstaben einzutragen:

Mit dem ersten Buchstaben wird die Kategorie der Bemerkung umschrieben:

- R Rechtschreib- oder Grammatikfehler
- E Mangelnde Erläuterung oder Klärung des behandelten Punktes
- U Text unvollständig oder nicht vorhanden
- F Fehler

Der zweite Buchstabe beschreibt den Bedeutungsgrad:

- g geringfügig
- G Gravierend

Unter "Referenz" ist die genaue Lokalisierung im Text anzugeben (Kapitelnummer, Zeile...).

Unter "Wortlaut der Bemerkung" kann ein Kommentar abgegeben werden.

Unter "vorgeschlagene Lösung" können Mittel zur Lösung des aufgeworfenen Problems angegeben werden.

Nr.	Typ	Referenz	Wortlaut der Bemerkung	Vorgeschlagene Lösung
1				
2				
3				
4				
5				

Vielen Dank für Ihre Teilnahme