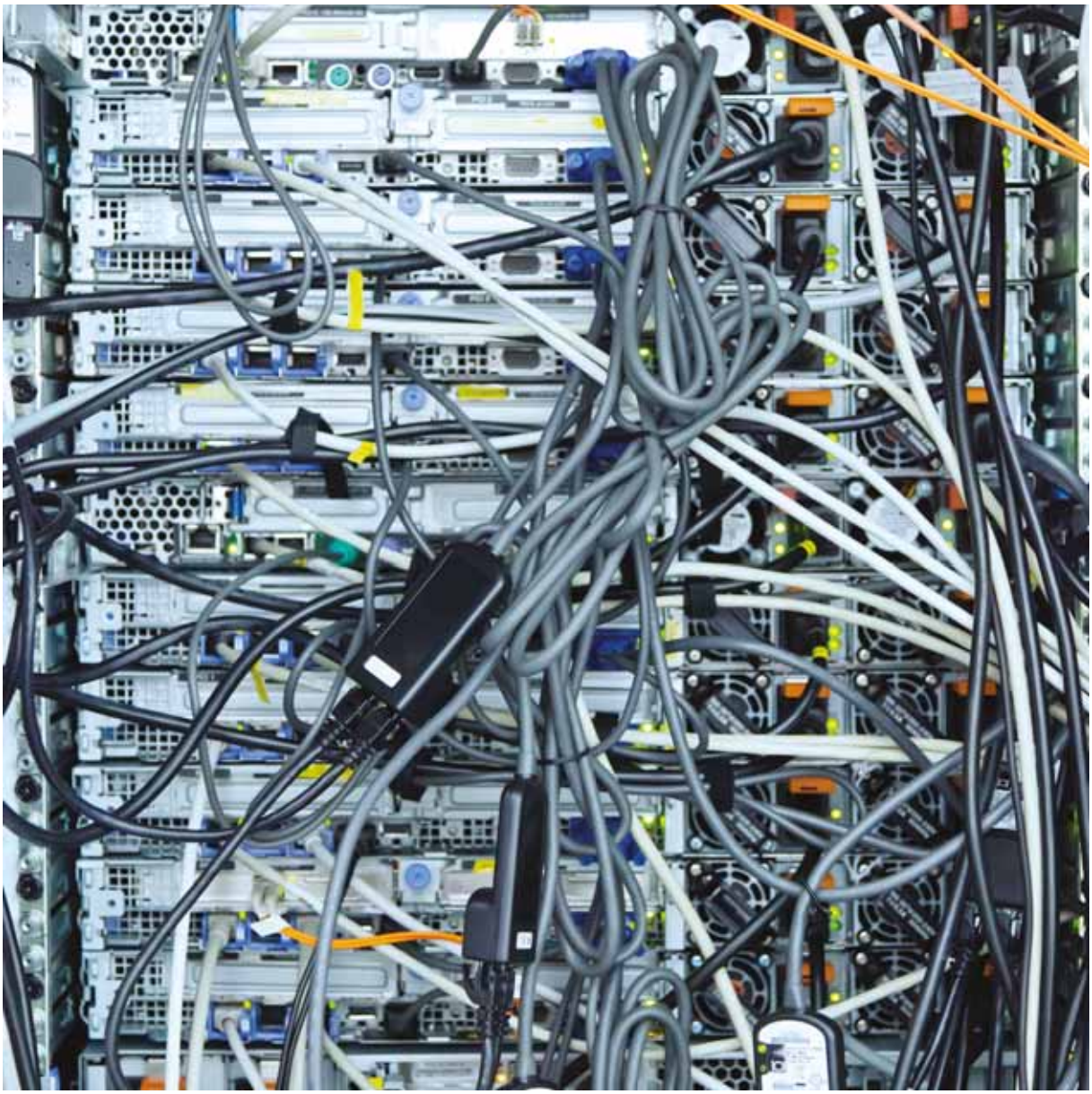
Publikation der deutschen Versicherer
(GDV e.V.) zur Schadenverhütung

Informationstechnologie (IT-Anlagen) – Gefahren und Schutzmaßnahmen



VdS 2007 : 2016-03 (04)

Zusammenfassung

IT-Anlagen gehören mit zu den wichtigsten Einrichtungen eines Unternehmens – unabhängig von der Größe, angefangen vom Gewerbebetrieb bis hin zum Industrieunternehmen. IT-Anlagen besitzen auch, speziell unter Betriebsunterbrechungsaspekten, eine erhebliche versicherungstechnische Relevanz.

In dieser Publikation werden Gefahren sowie Schutzmaßnahmen für einen sicheren Betrieb der IT-Anlagen aus Sicht der Sachversicherung aufgezeigt.

Die Publikation enthält Hinweise zur Schadenverhütung, um insbesondere Sach- und Betriebsunterbrechungs-Schäden zu vermeiden oder in ihren Auswirkungen möglichst zu begrenzen. Dazu werden mögliche bauliche, anlagentechnische sowie organisatorische Schutzmaßnahmen beschrieben. Was wie zur Erreichung der Schutzziele angewendet und umgesetzt wird, ist immer objektspezifisch im Rahmen einer Risikobetrachtung zu ermitteln. Die Publikation gibt dazu eine Hilfestellung.

Gefahren können aus dem Standort und seiner Umgebung entstehen, wie z. B. Erdbeben, Hochwasser/Starkregen. Weitere Gefahrenpunkte bilden Brand, Rauch, Explosion, nicht risikogerechte Organisation sowie auch Folgen einer unsicheren Technik, beispielsweise mangelhafte Energie-/Medienversorgung. Die Schutzmaßnahmen sind entsprechend der Bedeutung der IT-Anlage und der Größe des Betriebes genannt und schutzzielorientiert erläutert.

Der ungestörte Betrieb der IT-Anlage muss, unabhängig vom Versicherungsumfang, ein grundlegendes Ziel des Unternehmens sein und ist damit ein unabdingbarer Baustein eines unternehmerischen Gesamtschutzkonzeptes. Dies beinhaltet somit auch Anforderungen an die IT-Verfügbarkeit sowie deren kritische und physikalische Infrastrukturen.

Es werden weitere Informationsquellen und mögliche Dienstleistungen rund um den Schutz von IT angeführt. Diese Publikation versteht sich als ein Leitfaden.

Dieser Leitfaden ist komplett überarbeitet und ersetzt die Ausgabe 2004-08.

Informationstechnologie (IT-Anlagen) – Gefahren und Schutzmaßnahmen

Inhalt

1 Risiken, Zielsetzung, Anwendungsbereich, Schutzklassifikation

1.1 Risiken

Die Erfahrung der Versicherer zeigt, dass notwendige Konzepte zur Anlagensicherheit der Informationstechnologie häufig nicht dem Risiko eines Betriebes oder der möglichen Gefährdung angemessen entsprechen.

Steigende Automatisierung von Arbeitsabläufen, komplexer werdende Prozesse mit hohen technischen Anforderungen, zunehmender elektronischer Informationsaustausch und rascher technologischer Wandel mit entsprechendem Fortbildungsbedarf treffen auf ältere Infrastruktur, knapp bemessene Investitions- und Zeitpläne, wechselnde Umfeldbedingungen, z. B. höhere Umgebungstemperaturen oder Staubbelastungen, und vermeintlich überzogene Sicherheitsanforderungen.

Ein Restrisiko ist grundsätzlich nicht auszuschließen. Viele Schadenfälle belegen aber, dass mit einer konzeptionellen Risikovorsorge und teils einfachen Maßnahmen diese hätten verhindert werden können.

Aufgrund eines Leitungswasserschadens ist beispielsweise die komplette IT-Anlage eines mittelständigen Unternehmens ausgefallen. Dies verursachte einen mehrwöchigen Betriebsunterbrechungsschaden.

Eine Entscheidung vom OLG Hamm (Urt. v. 01.12.2003 – 13 U 133/03) ist von Interesse. Ein Unternehmen wollte von einem Dienstleister wegen eines größeren Datenverlustes Schadenersatz geleistet bekommen. Dieser Anspruch wurde abgelehnt. Begründung: Das Unternehmen hätte nicht für eine zuverlässige Sicherheitsroutine gesorgt. Es hätte sie grob vernachlässigt. Daten wären arbeitstäglich zu sichern gewesen und eine Vollsicherung hätte mind. wöchentlich erfolgen sollen. Der zurückbleibende Datenstand war mehrere Monate alt.

Die folgenden Aussagen sind entnommen der Publikation „IT-Sicherheitsniveau in kleinen und mittleren Unternehmen-Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie“ (Stand 09-2012):

- Die **Hauptursachen möglicher IT-Probleme und Schadensfälle** sind nach Bewertung von Unternehmen vor allem im Ausfall der vorhandenen Technik (81 Prozent) und im Fehlverhalten der eigenen Mitarbeiter (64 Prozent) zu erwarten. Die absichtliche Manipulation von IT oder Daten durch Außentäter wird von weniger als der Hälfte der Unternehmen als mögliche Ursache angeführt (44 Prozent), die Spionage von Nachrichtendiensten oder konkurrierenden Unternehmen nur von jedem neunten (11 Prozent) – siehe Bild 01.

Bild 01: Hauptursachen möglicher IT-Probleme und Schadenfälle

- **Konkrete Erfahrungen mit IT-Sicherheitsproblemen** hat fast jedes Unternehmen gemacht (93 Prozent). Am häufigsten genannt wurden der Ausfall der IT-Systeme (79 Prozent) sowie Probleme durch Viren (51 Prozent) und Spam (47 Prozent). In fast der Hälfte der betroffenen Unternehmen führte das zuletzt aufgetretene IT-Sicherheitsproblem zu keinen bzw. nur geringfügigen Beeinträchtigungen (45 Prozent), bei etwa jedem fünften Unternehmen waren die Geschäftsprozesse einen Tag und länger gestört (19 Prozent) – siehe Bild 02.

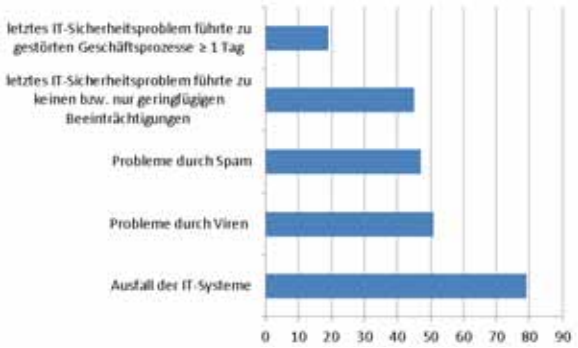


Bild 02: Konkrete Erfahrungen mit IT-Sicherheitsproblemen

1.2 Zielsetzung

Ziel des Leitfadens ist die Sensibilisierung durch Aufzeigen potentieller Gefahren und möglicher risikoadäquater Schutzmaßnahmen. Letzteres erfolgt anhand von Schutzklassifikationen (SK).

Im Rahmen dieses Leitfadens wird die Datensicherheit nur in Hinblick auf den technischen Datenverlust berücksichtigt.

Themenkomplexe wie z. B. haftungsrechtliche und versicherungsvertragliche Aspekte, Cybersicherheit sowie Softwareanforderungen werden nicht betrachtet.

Das Thema Cybersicherheit wird in der VdS-Richtlinie "Informationssicherheit in kleinen und mittleren Unternehmen (KMU)", VdS 3473, dargestellt. Diese befasst sich mit der Nutzung moderner IT zur Bewältigung von betriebswirtschaftlichen, logistischen und technischen Geschäftsprozessen sowie dem Anschluss an das Internet.

Hinsichtlich weiterführender Informationen wird auf gesetzliche, behördliche Vorschriften sowie auf Richtlinien, Merkblätter und Literatur weiterer Institutionen verwiesen (siehe Kapitel 4).

1.3 Anwendungsbereich

Dieser Leitfaden kann unabhängig von der Betriebsart eines Unternehmens auf alle IT-Anlagen angewendet werden.

IT-Anlagen werden anhand ihrer Größe und Verfügbarkeitsanforderungen in Schutzklassen von I bis IV eingeteilt – siehe Tabelle 01.

Die Schutzklasse IV wird in diesem Leitfaden nicht betrachtet. Diese Klasse erfordert weiterführende Anforderungen, die hier nicht abschließend dargestellt werden können.

Diese Publikation richtet sich an Versicherungsnehmer als Betreiber von IT-Anlagen sowie Mitarbeiter von Versicherungsunternehmen, wie Underwriter und Berater. Aufgrund dieses Anspruches sind die Informationen dieser Publikation auch von Interesse für Planer (z. B. Architekten), Fachplaner, ausführende Unternehmen und Fachkräfte. Ebenso bietet sich der Leitfaden bei der Überprüfung eines ganzheitlichen IT-Schutzkonzeptes durch externe Dienstleister an.

1.4 Schutzklassifikation

Die IT-Größe und deren Verfügbarkeit stellen die beiden Parameter zur Bildung von Schutzklassen.

Die IT-Größe korreliert erfahrungsgemäß mit dem Stellenwert der IT in einem Unternehmen, kann aber in Abhängigkeit der Verfügbarkeit in der daraus abzuleitenden Schutzklasse variieren (siehe Tabelle 01). Eine business impact analyse wird im Regelfall im kleingewerblichen Bereich nicht angewendet.

Die Einteilung der Verfügbarkeit folgt hier der Annahme:

- „normal" versteht sich als die Mindestanforderung für ein Unternehmen bzw. Bereich und bedeutet eine tolerierbare Einschränkung des Betriebsablaufes;
- „erhöht" bedeutet einen bedingt tolerierbaren Ausfall, der durch Mehraufwendungen kompensiert werden kann;
- „hoch" bedeutet einen nicht tolerierbaren Ausfall, der nicht kompensiert werden kann;
- „sehr hoch" bedeutet einen nicht tolerierbaren Ausfall, da selbst kurzzeitige Ausfälle ruinöse Auswirkungen erwarten lassen.

Die Verfügbarkeitsanforderungen müssen frühzeitig festgelegt und bei der Auswahl der Schutzmaßnahmen berücksichtigt werden! Der Aufwand steigt mit einer höheren Verfügbarkeitsanforderung und der IT-Größe, bspw. angefangen bei einem einzelnen Server, über eine Ansammlung von Servern in einem abgeschlossenen Raum bis hin zu einer Vielzahl von Servern in einem Rechenzentrum.

Schutzklassifikation				
IT-Größe	**Verfügbarkeit**			
	normal	erhöht	hoch	sehr hoch
Hochverfügbares Rechenzentrum (RZ)	--	--	IV	IV
Rechenzentrum (RZ)	II	III	III	IV
Serverraum	I	II	III	III
Einzel-Server	I	I	II	III

Tabelle 01: Zuordnungsmöglichkeit der Schutzklassifikation

2 Definitionen und Glossar

Bei **genannten Personengruppen**, wird von folgender Zuordnung ausgegangen:

- Interne Personen = Mitarbeiter des eigenen Betrieb/Firma
- DV-Personal = Mitarbeiter der EDV (interne oder externe Personen)
- Externe Personen = Fremde; Mitarbeiter von Fremdfirmen; externe Gäste

Weiße Wanne
Wasserundurchlässiges Bauwerk – in der Regel sind die äußeren Begrenzungsflächen aus wasserundurchlässigem Beton hergestellt – Außenwände, Bodenplatte, ggf. auch Decken.

Außenluft
Von außen angesaugte, der Luftaufbereitungsanlage zugeführte Luft.

Zuluft
Ggf. aufbereitete Luft, die dem Versorgungsbereich (z. B. einem Raum) zugeführt wird.

Abluft
Luft, die aus dem Versorgungsbereich, z. B. einem Raum, abgeführt wird.

Umluft
Luft, die aus der Abluft der Luftaufbereitungsanlage wieder zugeführt wird.

Fortluft
Luft, die ins Freie abgeführt wird.

Raid-System
Raid-System steht für eine redundante Anordnung unabhängiger physischer Festplatten zu einem logischen Laufwerk. Durch das System wird eine bessere Datenverfügbarkeit und größerer Datendurchsatz gegenüber den singulären Laufwerken erzielt.

3 Gefahren, Schutzmaßnahmen und Schutzziele für IT-Anlagen

Ein wirkungsvoller Schutz wird erfahrungsgemäß durch ein ganzheitliches Schutzkonzept erreicht, welches auf einer objekt- und nutzungsspezifischen Gefährdungsanalyse beruht und somit auf die betreffende IT-Anlage abgestimmt ist. Dieses Konzept basiert primär auf Schutzzielen zur Gewährleistung des Geschäftsbetriebes.

In der Tabelle 02 werden den potentiellen Risiken/Gefahren mögliche Schutzmaßnahmen analog der folgenden Struktur gegenübergestellt (siehe Bild 03):

Hinweise zur unten angeführten Tabelle 02:

- Schutzmaßnahmen können sich ggf. im Einzelfall ausschließen.
- Tabelle 02 dient der Orientierung und ist nicht als abschließend zu verstehen.
- Schutzmaßnahmen können fakultativ hinzugewählt werden.
- **Maßnahmen kleinerer Schutzklassen sind auch bei den größeren Schutzklassen zu berücksichtigen – beispielsweise Maßnahmen der Schutzklasse I auch in II.**
- Bei redundanter Ausführung der IT-Anlage kann eine Reduzierung der technischen Verfügbarkeitsanforderung angenommen werden.
- Zusätzlich sollten vorgelagerte oder nachgeschaltete Dienstleister hinsichtlich ihrer Verfügbarkeit betrachtet werden.

Nachbarschaft, Lage: Standortauswahl (3.1)
Einbruch-Diebstahl/Sabotage, Vandalismus (3.2)
Elementargefahren (Erdbeben, Sturm, Hochwasser/Starkregen, Schneedruck) (3.3)
Technische Gebäudeausstattung (TGA: Heizung, Klima/Lüftung, Wasser) (3.4)
Elektrische Anlagen (3.5)
Brand, Rauch, Explosion (3.6)
Organisation (3.7)
Instandhaltung (3.8)
Datenverlust (3.9)

Schutzklassifikation				
IT-Größe	**Verfügbarkeit**			
	normal	erhöht	hoch	sehr hoch
Hochverfügbares Rechenzentrum (RZ)	--	--	IV	IV
Rechenzentrum (RZ)	II	III	III	IV
Serverraum	I	II	III	III
Einzel-Server	I	I	II	III

Tabelle 01: Zuordnungsmöglichkeit der Schutzklassifikation

Bild 03: Gefährdungen – IT-Größe – Verfügbarkeit – Schutzklassifikation – Schutzklasse

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
3.1 Risiken durch die Nachbarschaft, Lage ■ Standortauswahl				
3.1.1 Sabotage, Anschläge, Brandstiftung aus dem Umfeld/der Nachbarschaft	+ von außen nicht erkennbare Lage des DV-Bereiches auf dem Grundstück bzw. im Gebäude		+ Auswahl eines Grundstückes in einem „gesicherten" Umfeld	Vermeiden/Vermindern der Erkennbarkeit von Dritten zur Verhinderung ■ einer Sabotage-, Anschlagsgefährdung, ■ eines ED-Risikos, ■ einer Brandstiftungsgefährdung.
3.1.2 Beeinträchtigung, Gefährdung der IT-/DV-Technik durch äußere Einwirkungen	+ sichere Lage innerhalb eines Gebäudes	+ sichere Lage auf dem Grundstück	+ Auswahl eines Grundstückes mit geringem Störrisiko	Vermeiden von Erschütterungen (Folge: z. B. Headcrash) durch ■ betriebliche Einrichtungen, ■ von Kraftfahrzeugverkehr in der Nachbarschaft. Vermeiden der Gefährdung durch ■ Fahrzeuganprall, ■ vagabundierende Streuströme durch Oberleitungen des Schienenverkehrs, ■ etc.
3.1.3 Elementargefahren		+ Auswahl eines Grundstückes ohne erhöhte Elementargefahren, wie z. B. keine Tal-/Flusslage (siehe Tabelle 02, Abschnitt 3.3)		Ausschluss/Berücksichtigen potentieller Elementargefahren bereits in der Planungsphase.
3.1.4 Staub, Rauch, Gase, Dämpfe			+ Standortwahl unter Berücksichtigung emittierender Nachbarschaft, z. B. Sandflächen, wie Sportplätze, Küstengewässer, Industriebetriebe	Vermeiden der Gefährdung der DV-Technik durch kritische Immissionen.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
3.1.5 Nagetiere	+ Leitungen mit Nagetierschutz + keine geschlossenen Kabelkanäle + in Räumen sind Maßnahmen durch einen Kammerjäger zu treffen			Vermeiden von Leitungsunterbrechungen und -störungen.
3.2 Risiken durch Einbruch-Diebstahl/Sabotage, Vandalismus				
IT-Anlagen können wegen der gespeicherten Informationen sowie der materiellen Werte der installierten technischen Einrichtungen und Geräte immer wieder Ziel von Einbrüchen und Diebstählen sein. Dabei ist zu bedenken, dass Angriffe sowohl von außerhalb des Unternehmens als auch von innerhalb geführt werden können. Unter Zuhilfenahme der VdS-Richtlinien und Empfehlungen lassen sich für alle individuellen Risiken und Gewerkkonstellationen angemessene und praxisgerechte Sicherungslösungen erarbeiten. Umfangreiche Informationen zu den VdS-Richtlinien finden Sie unter www.vds.de/richtliniennavigator				
	+ Verschluss der Betriebsräume + selbstschließende Tür, nur mit Schlüssel, Chip oder Zahlencode zu öffnen + Besucherregelung	+ Zutrittskontrollsysteme + Begleiteter Zugang + mechanische Sicherungen nach Sicherungsklasse SG "X" und Einbruchmeldeanlage nach VdS Klasse C-SG "Y" – siehe Erläuterung	+ Aufnahme und ggf. Prüfung der Personalien interner und externer Personen + Werkschutz + Räumliche Trennung und separate Zugänge von Besucherbereichen und neuralgischen Zonen + Videoüberwachung + mechanische Sicherungen nach Sicherungsklasse SG "X" und Einbruchmeldeanlage nach VdS Klasse C-SG "Y" – siehe Erläuterung	Um eine adäquate Einbruchhemmung zu erreichen, orientieren sich alle beschriebenen Sicherungsmaßnahmen an der Einstufung des Versicherungsrisikos in die jeweilige Sicherungsklasse Gewerbe nach Betriebsartenverzeichnis, VdS 2559. Detaillierte Maßnahmen für die mechanische Absicherung der Risiken sind in den Sicherungsrichtlinien für Geschäfte und Betriebe, VdS 2333 veröffentlicht. Hier werden grundsätzliche Einbruchdiebstahlrisiken und wirksame Gegenmaßnahmen beschrieben. Aber nicht in allen Fällen ist es sinnvoll oder möglich, eine spezielle Sicherungsempfehlung als alleinige Anforderung zu formulieren. Deswegen sollte sich mit dem Versicherer abgestimmt werden.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
3.3 Risiken durch Elementargefahren ■ Erdbeben, Sturm, Hochwasser/Starkregen, Schneedruck				
3.3.1 Erdbeben: vollständige Zerstörung der Technik durch Erschütterungen, Abreißen von Leitungen			+ Berücksichtigen der Erdbebenzonen: „erdbebensichere Bauweise“ + Vermeiden von Hanglagen (Erdrutsch) + Backup-RZ außerhalb der Erdbebenzone	Erhöhen der Verfügbarkeit eines Rechenzentrums.
3.3.2 Überschwemmung	Maßnahmen analog Hochwasser (3.3.3)	Maßnahmen analog Hochwasser (3.3.3)	Maßnahmen analog Hochwasser (3.3.3)	Beurteilen mit ZÜRS (Zonierungssystem für Überschwemmung, Rückstau und Starkregen).
3.3.3 Hochwasser, Grundwasser: Auftrieb, Eindringen von Wasser, Durchfeuchten von Bauteilen	+ Auswahl eines geeigneten Raum	+ Wassermelder	+ Auswahl eines geeigneten Standortes + Ausführung von in Erdreich liegenden Gebäudeteilen in wasserdichter Bauweise (z. B. „Weiße Wanne“; wasserdruck-dichte Leitungseinführungen in das Gebäude/Serverraum) + Anordnen von Öffnungen in Außenbauteilen oberhalb der Hochwasser-Schwelle	Vermeiden ■ des Eindringens von Wasser, ■ von wasserbedingten Schäden. *Hinweis: Die Publikation „Schutz vor Überschwemmungen“, VdS 3521, stellt umfänglich Schutzkonzepte und Schutzmaßnahmen vor.* *Es wird empfohlen, sich zur Hochwassergefahr zu informieren, z. B. ZÜRS-Abfrage.*
3.3.4 Schlag-/Starkregen	Maßnahmen analog Hochwasser (3.3.3) + Beachten der Regenfallrohre (z. B. innenliegend)	Maßnahmen analog Hochwasser (3.3.3) + von Gebäude abfallendes Gelände oder Gebäude-Standort erhöhen	Maßnahmen analog Hochwasser (3.3.3) + Vermeidung von Flachdächern	Vermeiden ■ von Wasseransammlungen (auch Statik), ■ des Eindringens von Wasser, ■ von wasserbedingten Schäden.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
3.3.5 Sturm	+ Begrenzung bzw. keine öffenbaren Außenwandflächen im Rechner-/Serverraum		+ Berücksichtigen der Windbeeinflussung durch die Nachbarschaft (verstärkte Winddruckkräfte) + Begrenzung offener/ungeschützter Technikaufbauten	Vermeiden ■ der Gefährdung durch äußere Beanspruchungen, wie Staub, Winddruck/Windsog, ■ der Gefährdung von technischen Anlagen (Antennen, Richtfunk-/Laser-Sende-/Empfangseinrichtungen). *Hinweis: Die Publikation „Sturm", VdS 2389, enthält Planungs- und Ausführungshinweise.*
3.3.6 Schnee/Eis		+ Prüfen und Anpassen der Gebäudestatik + rechtzeitiges Schneeräumen	+ Gestalten der Gebäudegeometrie und -ausführung zum Vermeiden von Schnee-/Eisansammlungen (Schneesackbildung, Dach-/Wandanhäufungen/Wasserabfluss)	Vermeiden von Überlast und Ansammlung von Tauwasser.
3.4 Risiken durch die Technische Gebäudeausstattung (TGA) ■ Heizung, Klima/Lüftung, Wasser; Elektrische Anlagen (siehe 3.5)				
3.4.1 Grundanforderungen	+ Integration der wesentlichen Technikbereiche/-anlagen in die ggf. vorhandene BMA-Überwachung/Löschanlagenschutz	+ Feuerbeständige Abtrennung des Serverraum zu angrenzenden Räumen (siehe 3.6.1)	+ für wichtige Einrichtungen (Klima, Kühlung): redundante Auslegung mit feuerwiderstandsfähiger Abtrennung zueinander	Erhalten der Redundanz bzw. des Weiterbetriebs bei Ausfall einer betriebsnotwendigen Versorgungstechnik. Entkoppeln der Energietechnik vom primären DV-Betrieb. Sicherstellung eines einheitlichen Schutzniveaus.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
3.4.2 Wasser (Leitungs- oder Abwasser)	+ Aufständerung der IT-Technik ca. 12 cm über Boden [analog Inventarversicherungsbedingungen] + Vermeiden von elektrischen Steckverbindungen im Feuchtigkeitsgefährdungsbereich analog vorangestellter Schutzmaßnahme	+ Verlegen von Frisch- oder Abwasser-/Kondenswasserleitungen außerhalb des Serverraumes + keine Öffnungen zu Abwasserleitung oder Einbau von Rückstau-/Absperrklappen + Überwachen des EDV-Bodens auf Leckage	+ Herstellen des Serverraum-/Doppelbodens mit Gefälle und Auffangraum/Pumpensumpf für Flüssigkeiten + keine wasserführenden Leitungen oberhalb der Serverraumdecke oder Herstellen/Einbringen einer Wassersperrschicht in oder unterhalb der Serverraumdecke - Verlegen nicht vermeidbarer Flüssigkeitsleitungen in Doppelrohren	Verhindern der Ansammlung oder des Eintritts von Wasser in den Serverraum bei Leckagen oder durch Rückstau. Abführen und Erkennen von eingetretenen Flüssigkeiten.
3.4.3 Lüftung	+ Ansteuern der Brandschutzklappen durch Kenngröße Rauch	+ Überwachen der Außen- und Umluft mittels geeigneter Brandfrüherkennung und ggf. Abschalten der Lüftungsanlage	+ Außenluftansaugung darf durch eine Fortluft nicht beeinträchtigt werden + Verwenden nicht brennbarer Dämmstoffe, speziell auch bei Außenluftleitungen + Außenluftansaugung über Dach auf der windabgewandten Seite und unter Berücksichtigung der Nachbarschaft + Bei Inertisierung: Integration der Lüftungstechnik (inkl. Raumlufttechnische Zentrale) in die Inertisierung	Vermindern des Ansaugen belasteter Luft. Vermeiden ■ einer Kurzschlusslüftung und Ansaugen verunreinigter Außenluft, ■ der Verbreitung von Rauch.

Gefahren/Risiken		Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
		I	II	III	
3.4.4	Übertemperatur	+ Überwachen der Serverumgebungstemperatur mindestens mit Störmeldung + Installation von stationären Kühl-/Lüftungseinrichtungen – keine Provisorien + geordnetes Herunterfahren der EDV		+ Redundante Überwachung der Umgebungstemperatur mit Störmeldung	Verringern einer die DV-Technik gefährdenden erhöhten Temperaturbeanspruchung – z. B. Umgebungstemperatur $T_{max.}$ 50° C.
3.4.5	kritische Betriebszustände der TGA	+ Not-Aus-Schaltung der TGA			Vermeiden von Schäden an der TGA. Bei Not-Aus-Schaltung müssen Folgen für die IT-Technik berücksichtigt werden.
3.4.6	Fehlerhafte Auslegung von Doppelböden			+ ausreichende Dimensionierung unter der Berücksichtigung der Nutz- und Punktlasten + elektrische Ableitfähigkeit und Integration in den Potentialausgleich nach VDE 0800-2-310	Anwendungsrichtlinie zu Doppelböden (DIN EN 12825) und DIN 1055 beachten.
3.5	**Risiken durch elektrische Anlagen**				
3.5.1	Blitzschlag		+ äußere Blitzschutzanlage mit Blitzschutzpotentialausgleich (auch Blitzstromableiter für Energie- und Datenleitung, Typ 1) (VDE 0185-305)		Blitzströme werden für das Gebäude gefahrlos ins Erdreich geleitet. Blitzströme sind aufgeprägte Ströme, die trotz Ableitung Überspannungen im Gebäude erzeugen können – siehe „Risikoorientierter Blitz- und Überspannungsschutz“, VdS 2010, und „Blitz- und Überspannungsschutz in elektrischen Anlagen“, VdS 2031.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
3.5.2 Ausfall einer Mittelspannungseinspeisung			+ zweite unabhängige MS-Einspeisung	Getrennte und redundante Energieversorgung des Versorgungsnetzbetreibers.
3.5.3 Ausfall einer Niederspannungseinspeisung			+ zweite unabhängige NS-Einspeisung; (VDE0100-100)	Getrennte und redundante Energieversorgung des Betreibers.
3.5.4 Störlichtbögen (Hauptverteilung)			+ Lichtbogenerkenn-ung/ -abschaltung in Anlagen	Frühzeitiges Abschalten der Hauptverteilung um die Auswirkungen eines Kurzschlusses zu minimieren.
3.5.5 Ausfall der Netzeinspeisung		+ Ersatzstromanlage (Generator); (VDE 0100-551)		Zweite unabhängige Energieversorgung; Notstromaggregate – Richtlinie für Planung, Errichtung und Betrieb von Anlagen mit Notstromaggregaten; 5. Auflage 2004 (VDN, Verband der Netzbetreiber beim VDEW/ BDEW).
3.5.6 Ausfall der Zuleitung durch Brand		+ Stromversorgung mit Funktionserhalt	+ zweiter unabhängiger Leitungsweg der Stromversorgung	Zweiter Leitungsweg durch andere Brandabschnitte gewährleistet die Stromversorgung bei einem Teilbrand. Leitungsverlegung mit Funktionserhalt gewährleistet die Funktion über eine gewisse Zeit trotz Brand.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
3.5.7 Ausfall der Netzeinspeisung hinsichtlich ■ Unterbrechung der Einspeisung ■ Gleichtaktstörungen ■ Rauschen ■ Spannungsspitzen und Impulse ■ Spannungsregelung ■ Oberschwingungen	+ USV für Einzelgeräte; (VDE 0558-510)	+ zentrale USV-Anlage		Unterbrechungsfreie Energieversorgung (Norm in Anhang) unter Beachtung der Versorgungszeit und technischen Anforderungen resultierend aus der Beherrschung der Gefahren (statische oder dynamische USV). USV-Anlagen können zusammen mit Notstromanlagen genutzt werden, um die Unterbrechung zu vermeiden und den längeren Betrieb zu gewährleisten.
3.5.8 Beeinflussung durch Einflüsse aus dem Versorgungsnetz		+ Überwachung der Netzparameter und ggf. Nachbesserung mittels eigener Maßnahmen;(DIN EN 50160; VDE 0100-444; VDE 0487)		Lokalisieren einer Störquelle und Eleminieren der Auswirkungen vom Versorgungsnetz zur ungestörten Energieversorgung. Überwachung kann auch vor der IT-Versorgung innerhalb eines großen Betriebes geschaltet werden.
3.5.9 Beeinflussung durch eigene Installationen	+ eigene Unterverteilung direkt vom Hauptverteiler			Keine Störungen durch die eigene Hausinstallation/elektromagnetische Verträglichkeit (EMV).
3.5.10 Störungen aus dem eigenen Netz (Strom auf dem Schutzleiter)	+ Netzform TN-S oder TT (5-Leiter-System); (VDE 0100-444; VDE 0487)		+ zentraler Erdungspunkt	Keine Ausgleichsströme auf Datenleitungsschirmen; wenn Zentraler Erdungspunkt bei mehreren Einspeisungen realisiert wird, sind weitere Maßnahmen erforderlich.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
3.5.11 Spannungsunterschiede des Erdpotentials	+ Potentialausgleich; (VDE 0100-444/-540)		+ Systembezugspotentialebene SRPP	Keine Störungen durch Spannungsdifferenzen. Vermeiden von Spannungsdifferenzen und weiteren Störungen in komplexen IT-Systemen.
3.5.12 Blitz- oder ähnliche Überspannungen (z. B. Schaltüberspannungen oder Auslösen einer Sicherung)	+ Überspannungs-ableiter; (VDE 0100-443, VdS 2031, VdS 2010, VDE 0185-305)			Schutz vor kurzen hohen Spannungsimpulsen.
3.5.13 Spannungsspitzen		+ Netzfilter; (VDE 0100-444)		Schutz vor netzbedingten Spannungsspitzen oder Oberschwingungen.
3.5.14 Überspannungen durch elektrische Felder	+ Schirmung; (VDE 0100-444, VDE 0185-305)			Schutz vor elektromagnetischen Feldern.
3.5.15 Provisorische Mehrfachanschlüsse (Tischsteckdosen)	+ Festinstallierte Steckdosen in ausreichender Anzahl			Bei Tischsteckdosen kann die Kontaktsicherheit unzureichend sein.
3.5.16 Ausschalten von RCD (Fehlerstrom-Schutzschalter)		+ selbsttätige wiedereinschaltende RCD + RCM		Fehlerstrom-Schutzschalter können durch kurzzeitige Netzanomalien auslösen, ohne dass ein konkreter Isolationsfehler vorliegt. RCM sind Überwachungsgeräte, ohne dass ein sofortiges Ausschalten erfolgt. Es wird zunächst nur gemeldet. Die Versorgungssicherheit steht im Vordergrund, wie z. B. in Operationsräumen.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
3.5.17 Lichtbogenfehler (Endstromkreis)		+ AFFD (Fehlerlichtbogen-Schutzeinrichtungen)		Das Auslösen dieser Schutzeinrichtung muss gemeldet werden, damit je nach USV-Konstellation Maßnahmen ergriffen werden können.
3.5.18 Beeinflussung der Datenleitung	+ getrennte Verlegung von Daten- und elektrischen Energieleitungen; (VDE 0100-520) + Netzwerkkabel mind. Cat 7 + Koordinierung zwischen Energietechnik und Datentechnik, um optimalen Schutz zu erreichen			Vermeiden von Beeinflussungen. Die richtige Auswahl der Maßnahmen kann nur in Abstimmung erreicht werden.
3.5.19 Absicherung von Steckdosen C 14/ Steckern C13	+ Steckdosen C14/Stecker C13 (VDE 0625-1) haben einen Bemessungsstrom von max. 10 A und sind entsprechend abzusichern			

Bild 04: Kaltgerätebuchse C14

Gefahren/Risiken		Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
		I	II	III	
3.5.20	Risikopotential PV-Anlage	+ Nachweis/Dokumentation von normenkonform errichteter Anlage	+ Prüfung alle 2 Jahre	+ keine PV-Anlage an oder auf dem Gebäude	Ein Verbot ist begründet in dem erhöhten Brandrisiko.
3.6	**Risiken durch Brand, Rauch, Explosion**				
3.6.1	Bauliches Layout	+ Anordnen des Server/-raumes in brandlastarmen Nutzungsbereichen	+ Erstellen eines geeigneten Raumkonzeptes mit der Definition von Schutzzonen: Gliederung mit brandschutztechnisch getrennten Räumen für Server, Operator, Drucker mit Papierlager, Energie-/Haustechnik, Notstrom		Vermeiden einer wechselseitigen negativen Beeinflussung der Nutzungen sowie Erhalt wichtiger Bausteine zur Minimierung der Ausfallzeit bei Zerstörung eines DV-Bausteines.
3.6.2	Brandentwicklung, -begrenzung		+ Ausführung von Bauteilen, Bekleidungen, Dämmstoffen etc. (Wandbekleidungen, Doppelbodenplatten) aus nicht brennbaren Baustoffen (Minimieren baulicher Brandlasten)		Verringern/Begrenzen der Brandbelastung.
3.6.3	Brandausbreitung		+ Abtrennung des Serverraumes (und gleichwertiger Peripherietechnik) zu angrenzenden Räumen durch raumabschließende Bauteile, die eine max. Raumlufttemperatur von 50 bis 60 °C nach 90 min. Brandbeanspruchung gewährleisten		Verringern ■ der Brandbeanspruchung und Brandausbreitung, ■ einer erhöhten Temperaturbeanspruchung der DV-Technologie.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
3.6.4 Rauchgasbeanspruchung	+ Rauchdichte Abtrennung der Zentraltechnik von angrenzenden Räumen, speziell Türen/Klappen, Kabel-/Leitungsdurchführungen	+ Anordnung unkritischer (brandlastarmer) Räume unmittelbar angrenzend an den Serverraum + Verwendung „raucharmer" Kabel, Minimierung von PVC-Kabeln (z. B. Stromschienensystem) oder Schutz dieser (Anstrich, Umhüllung)		Verhindern des Eintrags von Rauch und gefährdender Gase/Dämpfe: Rauchgaskontamination – siehe auch 3.4.3; Vermeiden der Entstehung kritischer Rauchgase. Wirksame Entrauchung des Serverraumes. Verhindern des Eindringens von Rauch aus der Peripherie.
3.6.5 fehlende Branderkennung und –bekämpfung	+ Ausstattung mit geeigneten Feuerlöschern (CO_2 für elektrische Anlagen, Schaum-/Wasser für Bürobereiche)	+ automatische Brandfrüh-(-frühst-)erkennung inkl. Doppelböden, Unterdecken und Technik-/(horizontalen und vertikalen) Peripherieräume mit Erstellung einer Brandfallsteuermatrix, unter Berücksichtigung von Störfaktoren, wie Lüftung + Automatisch auslösende Objektschutzlöschanlage	+ automatisch auslösende Raumschutzlöschanlage + Brandunterdrückungs-/(Permanent-) Inertisierungsanlage	Frühzeitiges Erkennen einer Brandentstehung mit gesicherter und abgestimmter Reaktion wie Alarmierung, Durchführung einer Sicherung, Herunterfahren der DV, Abschaltung der Lüftung, Schließen von Klappen, Auslösen von Löschanlagen z. B. Brandfallsteuermatrix. Unterdrücken einer Brandentwicklung. Frühzeitiges Löschen eines Entstehungsbrandes, ggf. als Raum- oder Objektschutz. Vermeiden von Löschmittelfolgeschäden. Auslegen der Löschanlagen entsprechend VdS-Richtlinien oder gleichwertig.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
3.7 Organisation: Risiken durch unzureichende organisatorische Maßnahmen				
3.7.1 Brandentstehung				
a) feuergefährliche Arbeiten	+ Einführung des Schweißerlaubnisscheins mit Unterweisung der mit Heißarbeiten beauftragten Personen, z. B. nach VdS 2036M + Verbot von Elektroschweißen + Einweisung von Fremdfirmen			Vermeiden der Brandentstehung durch ■ alternatives Reparaturverfahren, ■ Trennung von Brandlast und Zündinitial. Bekämpfen von Entstehungsbränden.
b) elektrische Installation	+ regelmäßige optische Kontrollen auf sichtbare Beschädigungen			Vermeiden elektrisch bedingter Schadenursachen.
c) elektrische Geräte	+ Verbot der Nutzung von betriebsfremden Elektrogeräten, wie Kaffeemaschinen und Kühlschränke + Einbeziehen in die betrieblichen Wiederholungsprüfungen			Vermeiden elektrisch bedingter Schadenursachen.
d) unzureichende Ausbildung/ menschliches Fehlverhalten	+ Unterweisung und Training der Mitarbeiter gem. VdS 2213 + Brandschutzkontrollgänge + Erstellung einer Brandschutzordnung + Betriebsanweisungen/Verhalten bei betrieblichen Störungen + Unterweisung von externen Personen	+ Bestellung von Brandschutz-Beauftragten gem. VdS 3111 + Begleitung externer Personen		Vermeiden ■ der Brandgefahren, ■ der (Brand)-Schäden.
e) Rauchen	+ Rauchverbot			Vermeiden fahrlässigen Umgangs mit Zündquellen.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
f) durch Abfall	+ grundsätzlich selbstverlöschende Abfallbehälter im EDV-Bereich verwenden	+ keine Lagerung von Materialien, die nicht dem unmittelbaren Betrieb der IT dienen		Vermeiden von Brandlasten, z. B. Ersatzteile, Altgeräte, Verbrauchsmittel.
3.7.2 Brandentwicklung/Brandausbreitung				
a) durch vorhandene Brandlasten	+ in Technikbereichen keine Lagerung brennbarer Materialien + unnötige Brandlasten, wie Altanlagen und nicht mehr benötigte Leitungen sind zu entfernen + Einhaltung der allgemeinen Ordnung und Sauberkeit			Vermeiden Brandentstehung/-ausbreitung durch fehlende/geringe Brandlasten.
b) bauliche Mängel	+ Kontrollen der brandschutztechnischen Trennwände und Türen/Tore/Klappen			Vermeiden der Brand- und Rauchausbreitung.
3.7.3 Wirksame Löscharbeiten				
a) unkoordiniertes Abschalten der Anlage		+ Erstellen von Notfallplänen/Abschaltplänen		Vermeiden einer Betriebsunterbrechung durch Regelung der Zuständigkeiten, Ansprechpartner und Abschaltkriterien/-möglichkeiten.
b) fehlende betriebsspezifische Information für die Feuerwehr	+ Benennen eines Feuerwehransprechpartners	+ Erstellen/Vorhalten eines Feuerwehrplanes und Feuerwehrlaufkarten + Einrichten eines EDV-Bereitschaftsdienstes		Ermöglichen eines schnellen und zielführenden Eingreifens durch die Feuerwehr.
c) fehlende/verstellte Angriffswege für die Feuerwehr	+ Kennzeichnung und Freihalten möglicher Aufstellflächen und Angriffswege	+ Vorhalten von Generalschlüsseln		Ermöglichen eines schnellen und zielführenden Eingreifens durch die Feuerwehr.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
d) fehlende Löschmittel	+ Bereitstellung von risikoadäquaten Löschmitteln in ausreichender Menge; keine Pulverlöscher, sondern Gaslöscher im EDV-Bereich (ASR A2.2) + Kennzeichnung (ASR A1.3)			Ermöglichen eines schnellen und zielführenden Erstangriffs.
3.7.4 Unerprobte Tests und Prozeduren, fehlende Konzepte				
a) Wiederanfahrbetrieb – fehlende Betriebswiederaufnahme-Vorbereitung	+ Erstellen von Wiederanlaufplänen (Business Continuity und Contingency Planning)			Nach Brandfall so schnell wie möglich einen provisorischen Betrieb aufnehmen und anschließend in den Regelbetrieb übergehen. Vorkehrung treffen, um durch Brand verlorengegangene Einrichtungen zu ersetzen.
b) Nachrüstungen	+ Einbindung von neuen Anlagen, Betriebsmitteln oder Systemen in das vorhandene Schutzkonzept			Berücksichtigen von z. B. PV-Anlage, Klimaanlage oder geänderter Raumnutzung.
3.8 Instandhaltung (Prüfung/Wartung/Instandsetzung)				
Fehlende Organisation		+ Einführung eines IT-Sicherheitsbeauftragten zur regelmäßigen Überprüfung des festgelegten Schutzkonzeptes und Überwachung der Instandhaltung für alle IT-Technik relevanten Einrichtungen inkl. Kontrolle der Herstellervorgaben		Übergeordnete Kontrollfunktion zur Einhaltung der Instandhaltungsmaßnahmen. Hinweise für den Sicherheitsbeauftragen siehe BSI IT – Grundschutzhandbuch.

Gefahren/Risiken	Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
	I	II	III	
Unzureichende Instandhaltung (Prüfung und Instandsetzung)	+ regelmäßige Instandhaltung der Betriebseinrichtungen (Geräte) und gemäß Herstellervorgaben + regelmäßige Wiederholungsprüfung der elektrischen Anlage nach SK 3602, z. B. durch VdS-anerkannte Sachverständige + regelmäßige Prüfungen elektrischer Anlagen und Betriebsmittel (DGUV Vorschrift 3) + Instandsetzung	+ Thermographie-Prüfung VdS 2858		Verhindern technischer und elektrischer Defekte.
Betrieblich auftretende Mängel	+ regelmäßige Kontrollgänge mit Dokumentation Veranlassung der Mängelbehebung			Wiederholungsprüfungen
3.9 Risiken Datenverlust				
Die Schutzmaßnahmen für Datenverlust beschränken sich auf die technische Datensicherheit zur Sicherstellung des Systembetriebs und dem Datenzugriff. Maßnahmen zum Persönlichkeitsschutz und Missbrauch der Daten bleiben unberührt.				
3.9.1 Datenträgerausfall	+ Datensicherung mit räumlich/baulich getrennter Aufbewahrung	+ Raid-System (ab RAID 1, z. B. als Datenspiegelung) + Aufstellung eines redundanten Raid-Systems räumlich/baulich getrennt		Speicherung auf mehreren Datenträgern. Raid-System zur Erhöhung der Datensicherheit.
3.9.2 Hardwaredefekt		+ Externe (Backup-) Rechner	+ Spiegel-RZ mit brandschutztechnischer Trennung (als eigener Brandabschnitt) und eigenständiger Versorgungstechnik	Backup der eigentlichen Servertechnik unter der Voraussetzung einer Datensicherung/-spiegelung

Gefahren/Risiken		Schutzmaßnahmen entsprechend Schutzklassen I bis III			Erläuterung (Schutzziele)
		I	II	III	
3.9.3	Fehlfunktion Backup	+ Überprüfen der Backups + Test und Üben der Rücksicherung + Datensicherungsplan A/B Datensicherung			Überprüfen, ob die zu sichernden Daten wirklich gesichert wurden. Üben der Rücksicherung ist notwendig, um im Bedarfsfall das System zeitnah wieder herzustellen. Durch Datensicherungsplan die zu sichernden Daten und Sicherungsarten regelmäßig und vollständig erfassen. Regelmäßiges Backup mit wechselnden Datenträgern
3.9.4	Ausfall IT-Verantwortlicher	+ Dokumentation der Systemdaten und des Schutzkonzeptes + Hinterlegen von Passwörtern + Vertretungsregelung	+ Notfallplan		Beschreibung von Systemstruktur und Daten für andere beauftragte Personen.
3.9.5	Aufbewahrung von Datenträger	+ Auswahl von Sicherungsschränken Feuer – Güteklasse S60 D bzw. DIS;	+ Auswahl von Sicherungsschränken Feuer – Güteklasse S90 D bzw. DIS	+ Auswahl von Sicherungsschränken Feuer – Güteklasse S120 D bzw. DIS	

Tabelle 02: Matrix Gefahren – Schutzmaßnahmen – Schutzklassifikation

4 Literaturangaben

4.1 Gesetze und Verordnungen, behördliche Richtlinien und Empfehlungen

IT Grundschutzhandbuch des BSI

Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
Internet: www.bsi.de

Technische Regeln für Arbeitsstätten
- ASR A1.3 Sicherheits- und Gesundheitsschutzkennzeichnung
- ASR A2.2 Ausrüstung von Arbeitsstätten mit Feuerlöschern

Betriebsicherheitsverordnung (BetrSichV);
ab dem 1. Juni 2015 in einer neuen Fassung!

Bundesanstalt für Arbeitsschutz und
Arbeitsmedizin (BAuA)
Friedrich-Henkel-Weg 1-25
D-44149 Dortmund
Internet: www.baua.de

4.2 Normen

DIN VDE 0100 Bestimmungen für das Errichten von Starkstromanlagen mit Netzspannungen bis 1000 V
- Teil 420 Schutz gegen thermische Gefahren
- Teil 444 Schutz gegen elektromagnetische Störungen (EMI) in Anlagen von Gebäuden
- Teil 551 Niederspannungsstromerzeugungseinrichtungen

DIN V VDE V 0800-2 (VDE V 0800-2) Informationstechnik – Teil 2: Potentialausgleich und Erdung (Zusatzfestlegungen)

DIN EN 50173-5 (VDE 0800-173-5) Informationstechnik – Anwendungsneutrale Kommunikationskabelanlagen – Teil 5: Rechenzentren

DIN EN 50174 (VDE 0800-174)-Reihe Informationstechnik – Installation von Kommunikationsverkabelung

DIN EN 50301 (VDE 0800-2-310) Anwendung von Maßnahmen für Erdung und Potentialausgleich in Gebäuden mit Einrichtungen der Informationstechnik

DIN EN 50600 (VDE 0801-600)-Reihe Informationstechnik – Rechenzentren mit
- VDE 0801-600-1Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 1: Allgemeine Konzepte
- VDE 0801-600-2-1 Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2-1: Gebäudekonstruktion;
- VDE 0801-600-2-2 Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2-2: Stromversorgung;
- VDE 0801-600-2-3 Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2-3: Überwachung der Umgebung
- VDE 0801-600-2-4 Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2-4: Infrastruktur der Telekommunikationsverkabelung
- E VDE 0801-600-2-5 Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2-5: Sicherungssysteme
- E VDE-0801-600-2-6 Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2-6: Informationen für das Management und den Betrieb

DIN EN 62305 (VDE 0185-305)-Reihe Blitzschutz baulicher Anlagen,

VDE-Verlag GmbH Berlin – Offenbach
Bismarkstr. 33, 10625 Berlin
Internet: www.vde-verlag.de

oder

Beuth Verlag GmbH
Burggrafenstraße 6
10787 Berlin
Internet: www.beuth.de

VDI 2054 Raumlufttechnische Anlagen für Datenverarbeitung

VDMA 24 991 Prüfbedingungen für das Brandverhalten von Stahlschränken und sonstigen Behältern

Beuth Verlag GmbH
Burggrafenstraße 6
10787 Berlin
Internet: www.beuth.de

4.3 VdS-Publikationen

VdS 2000 Brandschutz im Betrieb, Leitfaden für den Brandschutz

VdS 2005 Leuchten, Richtlinien zur Schadenverhütung

VdS 2009 Brandschutzmanagement, Leitfaden für die Verantwortlichen im Betrieb und Unternehmen

VdS 2010 Risikoorientierter Blitz- und Überspannungsschutz, Richtlinien zur Schadenverhütung

VdS 2025 Kabel- und Leitungsanlagen, Richtlinien zur Schadenverhütung

VdS 2031 Blitz- und Überspannungsschutz in elektrischen Anlagen, Richtlinien zur Schadenverhütung

VdS 2093 CO_2-Feuerlöschanlagen, Planung und Einbau

VdS 2095 Brandmeldeanlagen, Richtlinien für Planung und Einbau

VdS 2163 Richtlinien für mechanische Sicherungstechnik, Einbruchhemmende Verglasung, Anforderungen und Prüfmethoden

VdS 2234 Brand- und Komplextrennwände, Merkblatt für die Anordnung und Ausführung

VdS 2298 Brandschutz in Lüftungsanlagen, Merkblatt für den Brandschutz

VdS 2311 Einbruchmeldeanlagen, Richtlinien für Planung und Einbau

VdS 2333 Sicherungsrichtlinien für Geschäfte und Betriebe

VdS 2358 Richtlinien für Zutrittskontrollanlagen, Planung und Einbau

VdS 2380 Planung und Einbau von Löschanlagen mit nicht-verflüssigten Inertgasen

VdS 2381 Planung und Einbau von Löschanlagen mit halogenierten Kohlenwasserstoffen

VdS 2496 Richtlinien für die Ansteuerung von Feuerlöschanlagen

VdS 2534 Richtlinien für mechanische Sicherungseinrichtungen, Einbruchhemmende Fassadenelemente, Anforderungen und Prüfmethoden

VdS 3473 Informationssicherheit in kleinen und mittleren Unternehmen (KMU)

VdS 2556 Sicherung von verfahrenstechnischen Anlagen mit Mitteln der Prozessleittechnik

VdS 3527 Richtlinien für Inertisierungs- und Sauerstoffreduzierungsanlagen

VdS CEA 4001 Planung und Einbau von Sprinkleranlagen

VdS Schadenverhütung Verlag
Amsterdamer Str. 174,
50735 Köln
Internet: www.vds.de

4.4 Weiterführende Literatur

Bundesverband der Deutschen Industrie e. V. (BDI)
Breite Straße 29
10178 Berlin
Internet: www.bdi.eu

BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM
Albrechtstraße 10
10117 Berlin-Mitte
Internet: www.bitkom.org

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.
Reinhardtstr. 32
10117 Berlin
Internet: www.bdew.de

VIRZ - Verband Innovatives Rechenzentrum e.V.
Heckenweg 11
82285 Hattenhofen
Internet: www.virz.de

Bilder mit freundlicher Genehmigung von:

Titelbild:
fotolia.de

Herausgeber: Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV)

Verlag: VdS Schadenverhütung GmbH • Amsterdamer Str. 174 • D-50735 Köln
Telefon: (0221) 77 66 - 0 • Fax: (0221) 77 66 - 341