Technische Hochschule
Brandenburg
University of
Applied Sciences
Fachbereich
Wirtschaft

Sicherheitskonzept für das Rechenzentrum des Wirtschafswissenschaftlichen Zentrums an der Technischen Hochschule Brandenburg

Semesterarbeit

Fachbereichs Wirtschaft der

Technische Hochschule Brandenburg

vorgelegt von:

Hendrik Müller

1. Semester

Dozent: Ralph Wölpert

Müller, Hendrik Master Security Management 1. Fachsemester	Zahnderstraße 10G 14770 Brandenburg an der Havel hendrik.mueller@th-brandenburg.de Matr.-Nr. 2020-2183 Abgabe: 29.07.2017

Brandenburg/H., den 29. Juli 2017

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

THB	Technische Hochschule Brandenburg
USV	Unterbrechungsfreie Stromversorgung
WWZ	Wirtschaftswissenschaftliches Zentrums

1 Einleitung

Zu Beginn des Sicherheitskonzeptes sollen zunächst alle Rahmenbedingungen beschrieben werden, die als Grundlage für die weitere Betrachtung dienen.

1.1 Betrachtungsgegenstand

Betrachtungsgegenstand des Sicherheitskonzepts ist das Rechenzentrum des Wirtschaftswissenschaftlichen Zentrums (*WWZ*) der Technischen Hochschule Brandenburg (*THB*). Dieses ist eines von mehreren Rechenzentren an der Hochschule. Die folgenden Ausführungen beziehen sich ausschließlich auf dieses Rechenzentrum und auf das Gebäude, in dem sich das Rechenzentrum befindet. Hierzu gehört zusätzlich zum eigentlichen Serverraum auch noch die Räumlichkeit, in der sich weitere, für das Rechenzentrum notwendige, technische Einrichtungen befinden. Diese Räumlichkeit, sowie andere Rechenzentren und Serverräume sind nicht Gegenstand der Betrachtung und werden im Folgenden nicht weiter erwähnt oder behandelt.

1.2 Vorgehensweise

Der Erstellung dieses Dokuments geht ein Seminar voraus, in dem fachspezifische Kenntnisse zur Evaluierung eines Rechenzentrums vermittelt wurden. Vor allem die DIN EN 50600[1] wurde als Grundlage herangezogen um den aktuellen Stand der Technik für die Errichtung und den Betrieb von Rechenzentren zu beurteilen und zu bewerten. Dabei spielt vor allem die Sicherheit, aber auch die Energieversorgung und –effizienz eine entscheidende Rolle. Der Schwerpunkt dieses Konzepts soll sich auf die Brandschutz- und Zutrittskonzeption fokussieren, wobei auch auf die anderen Punkte eingegangen wird. Die spätere Analyse des Ist-Zustands und die darauffolgende Bewertung sollen diesen Fokus wiederspiegeln.

[1] Die DIN EN 50600 steht für eine Normenreihe mit mehreren Normen. Hauptsächlich ist die DIN EN 50600-2 für diese Arbeit relevant. Der Einfachheit geschuldet soll im Folgenden jedoch die DIN EN 50600 als Referenz genügen.

Dem Seminar folgte eine vor Ort Begehung des unter *KAPITEL 1.1* beschriebenen Gegenstandes. Hierbei wurden die Begebenheiten vor Ort betrachtet und dokumentiert. Diese Begehung ist integraler Bestandteil für die folgende Analyse des Ist-Zustandes.

Der Aufbau des Sicherheitskonzepts soll sich an der Vorgehensweise orientieren und besteht im Grunde aus drei Teilen:

- Zunächst sollen die Begebenheiten vor Ort in einem Ist-Zustand erfasst und betrachtet werden (Risikoanalyse).
- Dieser Betrachtung folgt eine Bewertung der bei der Begehung festgestellten Verhältnisse (Risikobewertung).
- Anschließend soll eine Reihe von Maßnahmenempfehlungen als Ergebnis aus diesem Dokument hervorgehen. Diese Maßnahmen bieten eine Option zur Risikobewältigung an.

Da dem Autor keine Version der DIN EN 50600 bei der Erstellung dieses Dokuments vorlag und auch nicht zugänglich war, basieren die Anforderungen auf den an der DIN angelehnten Inhalten des Seminars. Auch hier wird sich der Schwerpunkt auf die bereits genannten Bereiche fokussieren, sodass nicht alle Inhalte der DIN EN 50600 in dieser Arbeit umfänglich betrachtet werden.

1.3 Terminologie

Aufgrund der teilweise sehr unterschiedlichen Auslegung der Begriffe *Risikoidentifikation*, *Risikoanalyse*, *Risikobewertung*, etc. erschien es als sinnvoll hier einen kurzen Verweis auf die in diesem Dokument benutzte Terminologie zu erbringen. Die Terminologie entstammt der österreichischen Norm *ONR 49000 - Risikomanagement für Organisationen und Systeme*[2]. Als solches wird der Prozess zur Risikobeurteilung in die Schritte Risikoidentifikation, Risikoanalyse und Risikobewertung unterteilt. Die Risikoanalyse erfasst dabei das Wesen des Risikos, was als Grundlage für die Risikobewertung dient. Die Risikobewertung ist dabei ein eigener Prozess um die Ergebnisse der Risikoanalyse mit den Anforderungen[3] zu vergleichen und eine Aussage über das Risiko treffen zu können.

---

[2] Mit Rückzug der DIN ISO 31000 wurde hier die ONR 49000 als deutschsprachige und offen zugängliche Interpretation der ISO 31000 referenziert.

[3] Als Anforderungen sind hierbei die in *KAPITEL 2.2* erwähnten Kriterien zu verstehen auf die Geprüft werden soll; speziell die DIN EN 50600.

2 Ist-Zustand

Wie einleitend bereits erwähnt findet zunächst eine Erfassung des Ist-Zustandes statt. Hierzu wird das betrachtete Objekt noch einmal genauer beschrieben und anschließend die Ergebnisse der Begehung erläutert.

2.1 Objektbeschreibung

Wie in *KAPITEL 1.1* kurz erwähnt handelt es sich bei dieser Betrachtung um das Rechenzentrum des *WWZ*. Das Rechenzentrum befindet sich im 1. OG des *WWZ*; einem Altbau im Backsteinhaus-Stil. Das Gebäude besteht größtenteils aus Holzdecken und –böden und ist geprägt von großen Deckenhöhen. Für den gesamten Komplex gelten besondere Vorschriften aufgrund des Denkmalschutzes unter dem das Gebäude steht. Insofern ist bereits vorab anzumerken, dass gewisse Anforderungen der DIN EN 50600 sehr wahrscheinlich nicht erfüllt sind und auch nicht umgesetzt werden können.

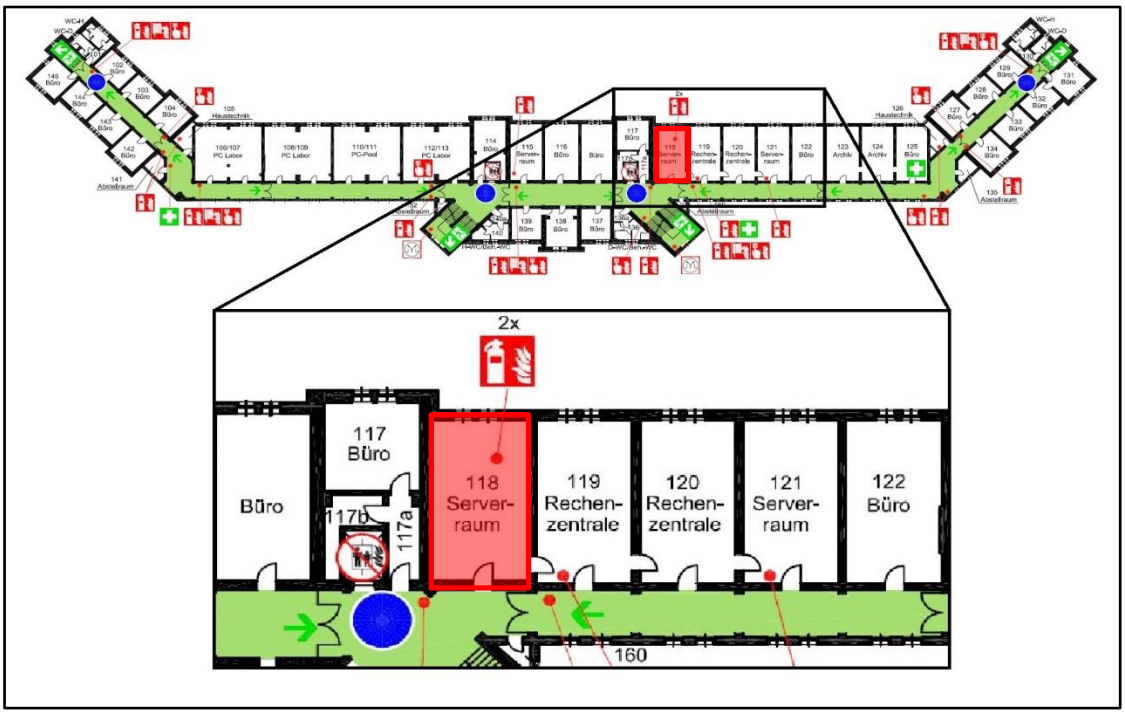

Abbildung 1: Lage des Rechenzentrums anhand eines Ausschnitts aus der BSO Teil A, ohne Legende.

ABBILDUNG 1 zeigt auf, wo genau sich das Rechenzentrum auf dem Stockwerk befindet. Es ist auch deutlich zu sehen, dass das Rechenzentrum relativ klein ist und nur aus einem Raum besteht (zzgl. einer ausgelagerten unterbrechungsfreien Stromversorgung [*USV*] weshalb die Terminologie als Rechenzentrum zutreffen dürfte). Die anliegenden, als Rechenzentrale ausgeschriebenen Räumlichkeiten sind dabei im Grunde ganz normale Büros. Der Lageplan zeigt noch einmal deutlich, dass das Rechenzentrum improvisierend in das bestehende Gebäude eingegliedert wurde und es sich um keine, eigens für die Verwendung als ein Rechenzentrum errichtete Räumlichkeit handelt.

2.2 Risikoanalyse

Die Risikoanalyse wurde unter zur Hilfenahme einer Checkliste erstellt. Diese wurde während der Objektbegehung systematisch durchgegangen und später bei einem Interview mit dem Verantwortlichen der Haustechnik ergänzt.

Die Checkliste gliedert sich dabei in insgesamt acht Teilbereiche, zuzüglich einem Allgemeinen Teil. Im Einzelnen sind diese:

- R0 – Allgemeines
- R1 – Gebäudestruktur und Gebäudeaufteilung
- R2 – Zutrittskonzept
- R3 – Brandschutzkonzept
- R4 – Kühlanlagen
- R5 – Stromversorgung
- R6 – Energieeffizienz
- R7 – Sonstiges
- R8 – Lage des Rechenzentrums

Die Teilbereiche sind thematisch gegliedert und umfassen jeweils mehrere Unterpunkte, auf die konkret geprüft wurde. Das komplette Dokument ist ungekürzt diesem Dokument als separate Excel-Datei beigefügt. Auch der einleitend geschilderte Fokus dieses Sicherheitskonzepts spiegelt sich in diesem Dokument wieder. So wurden besonders das Zutrittskonzept sowie das Brandschutzkonzept betrachtet. Entsprechend finden sich hier die meisten Unterpunkte auf die geprüft wurde.

In den folgenden Unterkapiteln sollen nun jeweils die wichtigsten Punkte der während der Begehung festgestellten Schwachstellen kurz erläutert

werden. Die doch relativ kurz gefassten Ergebnisse im Dokument selbst werden somit etwas genauer beleuchtet und teilweise durch Bildmaterial ergänzt.

2.2.1 R0 – Allgemeines

Der Verfügbarkeitsanspruch des Rechenzentrums bewegt sich im geringen bis mittleren Bereich bzw. der Verfügbarkeitsklasse 1-2 gemäß DIN EN 50600 (*SIEHE ABBILDUNG 2*). Dieser Verfügbarkeitsanspruch wird maßgebend für die weitere Betrachtung sein.

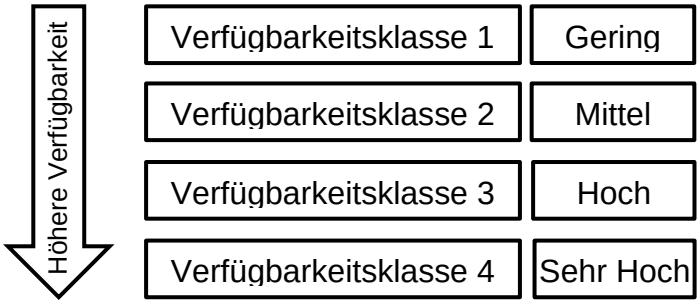

Abbildung 2: Verfügbarkeitsklassen nach DIN EN 50600 (eigene Darstellung, 2017).

Bereits in der Vergangenheit kam es zu vereinzelten Ausfällen des Rechenzentrums, was aber zu keinen größeren Störungen führte und der Hochschule keinen Schaden verursachte. Die im Rechenzentrum laufenden Prozesse und Systeme (Software) wurden als wenig kritisch eingestuft. Hinzukommt, dass Teile des Rechenzentrums bei Ausfall durch andere Rechenzentren von der *THB* kompensiert werden können. Somit besteht eine Redundanz, was wiederum dem Verfügbarkeitsanspruch gerecht wird.

Bei der Hardware gibt es keine Besonderheiten. Es kommen Server zum Einsatz für Computing- und Storage-Anwendungen, sowie Switches für die Netzwerkinfrastruktur. Auch eine *USV*-Einheit ist vorhanden.

2.2.2 R1 – Gebäudestruktur und Gebäudeaufteilung

Aufgrund der Größe des Rechenzentrums gibt es bezüglich der Gebäudestruktur nicht allzu viel zu sagen. Die wichtigen Funktionseinheiten – in diesem Fall der Rechnerraum und die *USV* – sind räumlich getrennt und separiert. Auch Arbeitsplätze sind getrennt vom eigentlichen Rechenzentrum, weshalb es in der Räumlichkeit keine festen Arbeitsplätze gibt. Die Arbeitsplätze der Mitarbeiter grenzen direkt an das Rechenzentrum an.

2.2.3 R2 – Zutrittskonzept

Ein Zutrittskonzept besteht nur im rudimentären Sinne. Ein einfaches Schließsystem beschränkt den Zugang zum Rechenzentrum für autorisiertes Personal. Die Schlüssel für den Zugang werden dabei intern vergeben und die Vergabe schriftlich festgehalten. Ob ein Schlüssel jedoch weitergegeben wird kann nicht festgestellt werden, bzw. wird erst bei der Rückgabe auffällig.

Unabhängig der Verfügbarkeitsklassen der DIN EN 50600, unterteilt die DIN ebenfalls vier verschiedene Schutzklassen (*SIEHE ABBILDUNG 3*). Diese Schutzklassen beziehen sich auf den physischen Schutz, inklusive dem Schutz vor unautorisiertem Zugang und dem Brandschutz. Das derzeitige Schutzniveau zum Schutz vor unautorisiertem Zugang kann mit der Schutzklasse 2 nach DIN EN 50600 verglichen werden. Die Empfehlung der DIN geht jedoch hin zur Schutzklasse 3, bzw. Schutzklasse 4 für den Rechnerraum und die Serverracks.

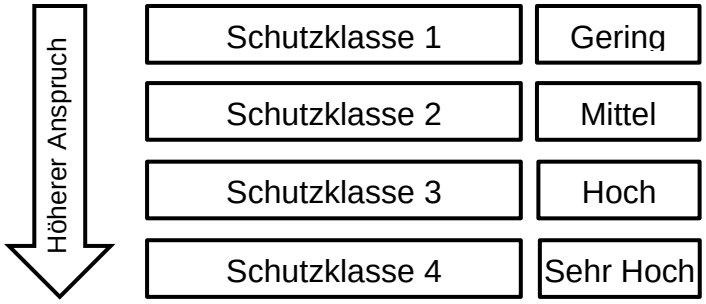

Abbildung 3: Schutzklassen nach DIN EN 50600 (eigene Darstellung, 2017).

Das Rechenzentrum hat insgesamt zwei Zugänge. Es kann direkt vom Gang, aber auch von dem anliegenden Büro aus betreten werden. Ein Zonenmodell oder vergleichbare organisatorische Maßnahmen gibt es keine. Wohingegen die Türe zum Gang hin immer geschlossen zu halten ist (hierauf wird auch im inneren des Rechenzentrums mit einem Zettel an der Türe beim Verlassen des Raums hingewiesen), ist die Türe zum anliegenden Büro unverschlossen. Dies wird damit begründet, dass in den anliegenden Büros ebenfalls nur autorisierte Mitarbeiter Zutritt haben und die Bürotüren entsprechend verschlossen werden.

Eine sonstige Sicherung bzw. Härtung der Türen (beispielsweise nach Widerstandsklassen) besteht genauso wenig wie eine Sicherung der zwei vorhandenen Fenster. Auch andere technische Sicherungsmaßnahmen wie

eine Videoüberwachung der Zugänge oder eine Einbruchmeldeanlage sind für das Rechenzentrum nicht vorgesehen.

Die Racks innerhalb des Rechenzentrums sind alle, bis auf den separat stehenden Rack verschlossen. Die Schlüssel für die Racks werden dabei im Schloss gelassen, sodass der Zugang zu den Servern ohne Probleme besteht. Dies soll vor allem die Arbeit an den Servern erleichtern, zumal nur autorisierte Personen Zugriff zum Rechenzentrum haben.

(a) *(b)*

Abbildung 4: (a) Rollcontainer neben den Racks; (b) Notizzettel auf dem Rollcontainer (eigene Darstellung, 2017).

Für die temporäre Arbeit an den Servern im Rechenzentrum steht ein Rollcontainer zur Verfügung, auf dem unter anderem ein Monitor und eine Tastatur bereit liegen (*SIEHE ABBILDUNG 4*). Daneben finden sich auch Notizzettel mit Netzwerkadressen und anderen Informationen. Der Rollcontainer selbst ist wie die Racks unverschlossen.

2.2.4 R3 – Brandschutzkonzept

Auch in Sachen Brandschutz empfiehlt der DIN die Orientierung an den Schutzklassen. Hierbei geben die einzelnen Schutzklassen Aufschluss darüber, welche übergeordneten Maßnahmen ergriffen werden sollten. Folgende Anforderungen werden seitens der DIN an die verschiedenen Schutzklassen gestellt:

Schutzklasse 1: Branderkennung

Schutzklasse 2: Branderkennung sowie Einsatz von Unterdrückungsanlagen zur Aufrechterhaltung der Funktionen innerhalb dieser Bereiche, sowie der Bereiche der Schutzklasse 1

Schutzklasse 3: Branderkennung sowie Einsatz von Unterdrückungsanlagen zur Aufrechterhaltung der Funktionen innerhalb dieser Bereiche, sowie Bereiche der Schutzklasse 1 und 2

Schutzklasse 4: Branderkennung sowie Einsatz von Unterdrückungsanlagen zur Aufrechterhaltung kritischer Funktionen innerhalb des Rechenzentrums

Die im Rechenzentrum vorhandenen Maßnahmen im technischen Brandschutz beschränken sich auf einen Rauchwarnmelder zur Branddetektion und der Bereitstellung von Löschmitteln in Form von zwei Handfeuerlöschern (je 6 kg CO_2 Löschmittel). Dies würde der Schutzklasse 1 nach DIN EN 50600 entsprechen. Der Einbau einer Lösch- bzw. Unterdrückungsanlage konnte aufgrund von speziellen Anforderungen an den Denkmalschutz im gesamten *WWZ* Gebäude nicht umgesetzt werden. Es sei an dieser Stelle kurz vermerkt, dass die Prüfung der vorhandenen Handfeuerlöscher zum Zeitpunkt der Begehung bereits überfällig war.

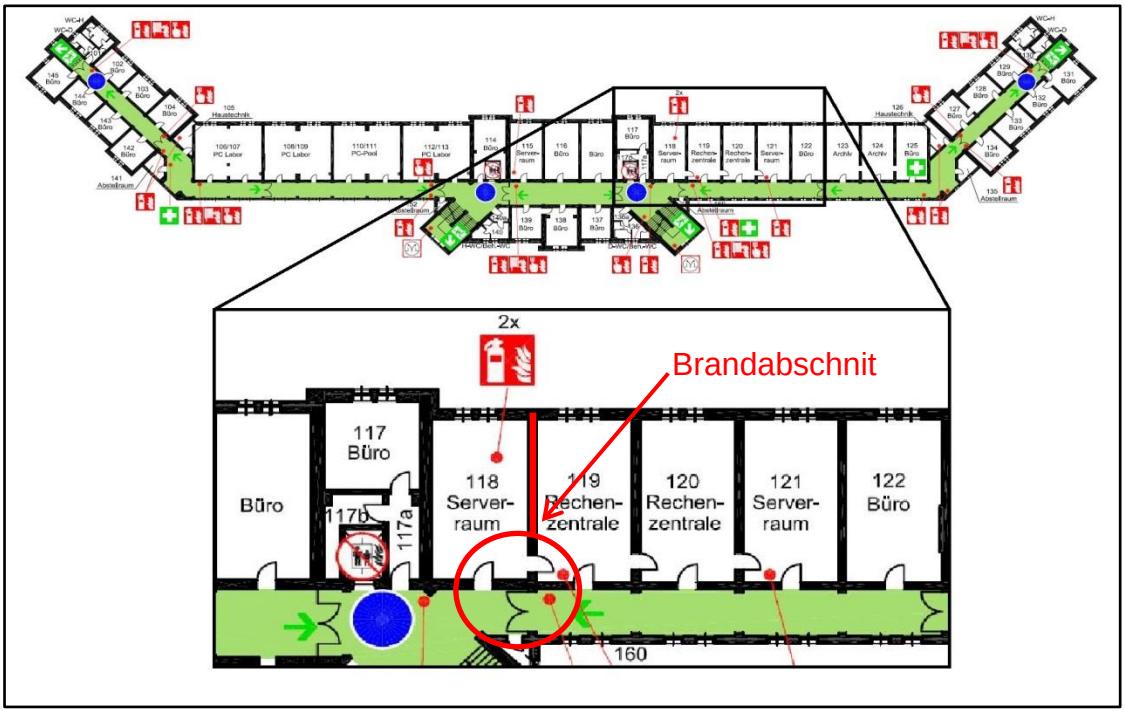

Abbildung 5: Brandabschnitt zwischen Rechenzentrum und Büroräume (BSO Teil A, 2017).

Auch Maßnahmen im Bereich baulicher Brandschutz sind aufgrund besonderen Bestimmungen nicht umgesetzt worden. So bestehen die Decke und Böden aus Holz. Zwar wurden in den Fluren Brandabschnitte gebildet, es ist aber anzunehmen, dass die Widerstandsfähigkeit der angrenzenden Wände diese Brandabschnitte nicht unterstützen. Dies ist vor allem mit Blick auf die *ABBILDUNG 6* von Bedeutung. Hier ist zu sehen, dass zwischen dem Rack in dem sich die Switches und Patchkabel befinden und der Wand nur wenige Zentimeter Platz sind (a). Auf der anderen Seite der Wand befindet sich ein Büro mit relativ hoher Brandlast (b). Es ist anzunehmen, dass obwohl es sich um eine Unterteilung zweier Brandabschnitte handelt (*SIEHE ABBILDUNG 5*), die Wand keine besonderen feuerhemmenden oder feuerbeständigen Eigenschaften besitzt. Selbst wenn eine Feuerwiderstandsfähigkeit gegeben wäre, so könnte die Hitze, die bei einem Brand im anliegenden Büro entstehen könnte, die Geräte nahe der Wand beschädigen. Auch die Türe zum Nebenraum ist im Gegensatz zur Türe die auf den Flur führt keine gekennzeichnete feuerbeständige, noch eine feuerhemmende Türe.

(a) *(b)*

Abbildung 6: (a) Rack mit nur wenig Platz zur Wand; (b) Brandlast auf der anderen Seite der Wand (eigene Darstellung, 2017).

Zwischen den zwei Brandabschnitten verläuft zusätzlich noch ein Kabelschacht (*SIEHE ABBILDUNG 7*). Hier verlaufen einige Rohre, die zur Klimaanlage gehören. Ein Blick auf den Durchbruch in der Wand lässt

vermuten, dass hier keine speziellen abdichtenden und feuerhemmenden Baustoffe eingebracht wurden.

Abbildung 7: Wanddurchbruch vom Rechenzentrum ins anliegende Büro (eigene Darstellung, 2017).

2.2.5 R4 – Kühlanlage

Für die Kälteversorgung greift die DIN nicht auf die in den beiden vorhergehenden Unterkapiteln beschriebenen Schutzklassen zurück, sondern es werden diesmal die Verfügbarkeitsklassen herangezogen. Für die bereits festgelegte Verfügbarkeitsklasse, die sich sehr wahrscheinlich zwischen Klasse 1 und 2 befindet, sieht die DIN EN 50600 keine, bzw. eine einfache Kälteversorgung ohne besondere Anforderungen oder Redundanzen vor.

Im Rechenzentrum befinden sich insgesamt drei Raumkühler. Diese werden von insgesamt sechs Kühlgeräten auf dem Dach mit Gas gespeist. Zusätzlich kommt im Winter ein Freikühler zum Einsatz. Die Raumkühler werden durch einen im Raum befindlichen Thermostat zentral gesteuert. Gemessen an der Leistung der Raumkühler wäre bereits einer der drei Geräte ausreichen, um den gesamten Raum angemessen kühl zu halten. Somit kann nicht nur von einer Redundanz von N+1 ausgegangen werden, sondern man könnte die vorhandene Kühlanlage als zusätzlich fehlertolerant während der Wartung beschreiben. Dies wäre gemäß DIN EN 50600 für ein Rechenzentrum der Verfügbarkeitsklasse 4 (bzw. erweiterte Klasse 4) erforderlich.

2.2.6 R5 – Stromversorgung

Wie die Anforderungen an die Kühlanlage orientieren sich die Anforderungen an die Stromversorgung ebenfalls an der Verfügbarkeitsklasse. Die Stromversorgung des gesamten Hochschulgeländes erfolgt über insgesamt drei Zuführungen. Diese werden von insgesamt zwei Mittelspannungs-transformatoren auf die Gebäude verteilt. Das Rechenzentrum per se wird dabei von nur einer Zuleitung gespeist. Dies ist für die gewünschte Verfügbarkeitsklasse auch gemäß DIN EN 50600 ausreichend.

Zusätzlich zum Stromnetz ist das Rechenzentrum auch an eine *USV* angeschlossen. Diese ist wie bereits erwähnt räumlich vom Rechenzentrum getrennt und erlaubt es die Funktion des Rechenzentrums über einen Zeitraum von ca. 45 – 80 min aufrecht zu erhalten. Eine Notstrom- oder Netzersatzanlage gibt es keine. Auch eine automatische Notabschaltung der Systeme ist nicht eingerichtet. Im Falle eines längeren Stromausfalls müsste eine manuelle Abschaltung innerhalb der durch die *USV* überbrückten Zeit stattfinden.

Aufgrund der baulichen Gegebenheiten verlaufen die Kabel im Rechenzentrum nicht im Boden, sondern werden durch eine Gitterstruktur über den Racks geführt. Somit wird verhindert, dass Kabeltrassen auf dem Boden verlegt werden, was eine Unfallgefahr für Mitarbeiter bedeuten würde.

2.2.7 R6 – Energieeffizienz

Zur Messung der Energieeffizienz unterscheidet die DIN drei verschiedene Granularitätsniveaus:

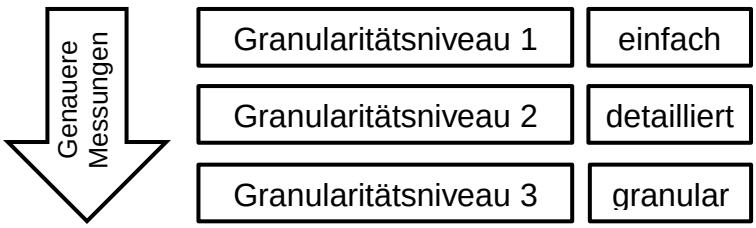

Abbildung 8: Niveaus zur Messung der Energieeffizienz gemäß DIN EN 50600 (eigene Darstellung, 2017).

Die Messung der Energieeffizienz hat keine Relation zu den Verfügbarkeits- oder Schutzklassen. Es geht dabei lediglich um die Wünsche des Rechenzentrumsbetreibers. Im Rechenzentrum des *WWZ* findet kein richtiges Monitoring von Verbrauch und Temperatur statt. Es werden lediglich

die Raumluft gemessen um die Steuerung der Kühlanlage zu regeln, sowie eine Software basierte Messung der Server Core-Temperaturen. Kommt es zu einer Überhitzung der Server müssen manuelle Maßnahmen eingeleitet werden. Das Monitoring ist an keinen anderen Prozess angebunden.

2.2.8 R7 – Sonstiges

Zur Südseite hin befinden sich zwei normale Fenster im Rechenzentrum (*SIEHE ABBILDUNG 9*). Diese sind unverschlossen und es gibt keine Möglichkeit, die Fenster abzudunkeln. Zwar befinden sich außerhalb des Fensters größere Bäume, die einiges an Sonnenstrahlung abfangen, dennoch ist davon auszugehen, dass hier Wärmestrahlung dazu bei trägt, dass sich der Raum stärker aufheizt.

Abbildung 9: Fenster im Rechenzentrum (eigene Darstellung, 2017).

Ein sich auf dem Fenstersims befindliches Telefon kann als mögliche Stolperstelle eine Gefahr für sich im Rechenzentrum befindliche Mitarbeiter bedeuten. Wie in *ABBILDUNG 10* zu sehen verläuft das relativ lange Kabel über dem Fußboden in der Ecke des Raumes. Dies mag eine kleine Gefahr darstellen, ist aber aus Sicht der Arbeitssicherheit durchaus zu beanstanden und durch relativ einfache und kostengünstige Maßnahmen reduzierbar.

Abbildung 10: Telefonkabel verläuft über den Boden des Rechenzentrums (eigene Darstellung, 2017).

2.2.9 R8 – Lage des Rechenzentrums

Zur Lage des Rechenzentrums gibt es nicht allzu viel zu sagen. Wie bereits in diesem Dokument erwähnt befindet sich das Rechenzentrum im 1. OG des *WWZ*. Eine Gefährdung durch Hochwasser ist trotz der Nähe zu Flüssen und Seen relativ gering. Auch in der Vergangenheit gab es hier keine nennenswerten Vorfälle.

Ein Blitzschutz am Gebäude ist vorhanden und entspricht den allgemeinen baulichen Bestimmungen. Eine besondere zusätzliche Absicherung für das Rechenzentrum ist nicht vorhanden.

3 Risikobewertung

In diesem Kapitel werden nun die in *KAPITEL 2.2* identifizierten Risiken bewertet und in einen Kontext gebracht. Dazu wird zunächst die Methodik erklärt und anschließend die Ergebnisse vorgestellt.

3.1 Methodik

Für die Bewertung wurde wieder die bei der Objektbegehung verwendete Checkliste herangezogen. Anstatt die dort abgebildeten Punkte auf generische Risiken abzuleiten bzw. zu transformieren und eine neue Liste zu erstellen, wurde die Bewertung stattdessen direkt anhand dieser Punkte durchgeführt. Dies bedeutet, dass bspw. kein generisches Risiko *Brandgefahr* betrachtet wurde, sondern stattdessen die Auswirkungen der vorhandenen oder nicht vorhandenen Maßnahmen der Punkte der Kategorie *R3* bewertet wurden. So wurde bspw. eine Einschätzung vorgenommen, wie kritisch oder unkritisch die bestehenden oder fehlenden Maßnahmen bezüglich einer Löschanlage zu bewerten sind. Anhand dieses Vorgehens kann das gesamte Konzept vereinheitlicht werden und alle Schritte orientieren sich direkt an den während der Begehung festgestellten Punkten. Diese Punkte basieren wiederum wie bereits zu Beginn des Konzeptes geschildert aus den Anforderungen der DIN EN 50600. Somit werden die in der DIN genannten Anforderungen hier als Grundlage genommen und bestehende Maßnahmen dahingehend betrachtet, inwieweit die Anforderungen der DIN EN 50600 umgesetzt wurden.

Bei der Bewertung der einzelnen Punkte wurde von der traditionellen Einschätzung der Wahrscheinlichkeit und Schadensausmaß abgewichen. Die hierfür benötigten Informationen, sofern überhaupt vorhanden, wären nur sehr schwer zu generieren und würde einige Aspekte vernachlässigen. Stattdessen wurde eine qualitative Bewertung gewählt, anhand derer Tendenzen zu erkennen sind. Je bewertetem Punkt bzw. Risiko werden Punkte zwischen -4 und +4 vergeben. Durch eine 4-stufige Unterteilung wird verhindert, dass es eine Mitte gibt die bei einer qualitativen Bewertung gerne herangezogen wird. Eine Skale von -4 bis +4 scheint zunächst sehr groß gefasst, Ziel ist es

allerdings anhand des Ergebnisses später eine Tendenz erkennen zu können. Wird die Skala verkleinert, so nähern sich die Ergebnisse einander an. Bei positiv bewerteten Risiken ist zunächst kein Handlungsbedarf vorhanden, bei negativ bewerteten Risiken jedoch schon. Eine Erläuterung der Bewertungsskala kann auch noch einmal in der diesem Dokument beigefügten Excel-Tabelle entnommen werden. Grundsätzlich sind die Ergebnisse wie folgt zu interpretieren:

Tabelle 1: Frei formulierte Interpretation der Risikobewertung (erstellt von dem Verfasser, 2017).

Skala	Interpretation
+4	Die vorhandenen Maßnahmen sind absolut ausreichend
+1 – +3	Grundsätzlich kein Handlungsbedarf, allerdings noch Raum für Verbesserungen
N/A	Keine Bewertung
-1 – -3	Handlungsbedarf vorhanden
-4	Handlungsbedarf vorhanden, Maßnahmen absolut nicht ausreichend

Zusätzlich dieser Einteilung wurden die jeweiligen Kategorien ebenfalls berücksichtigt. So wurden je Kategorie die Bewertungen zusammengefasst und ein Mittelwert gebildet. Der Mittelwert wurde aus der Summe der maximal, bzw. minimal zu erreichenden Punkte je Kategorie gebildet. Da jede Kategorie unterschiedlich viele Risiken aufweisen unterscheiden sich die maximale und minimale Punktzahl. Aufgrund der hier angewendeten Methodik kann jedoch pro Kategorie eine Tendenz abgelesen werden. Dominiert der positive Balken, so sind die Risiken der Kategorie recht gut behandelt und es wird nur vereinzelt Handlungsbedarf geben. Dominiert jedoch der negative Balken, so ist in der jeweiligen Kategorie noch großer Handlungsspielraum. Gleichen sich die beiden Balken an, so ist prinzipiell ebenfalls von einem Handlungsbedarf auszugehen. Grob gesagt kann man von einem Handlungsbedarf ausgehen, wenn sich der Mittelwert der 0 nähert. Ist der Mittelwert negativ hat man einen großen Handlungsbedarf in der jeweiligen Kategorie.

3.2 Ergebnisse

Die zuvor skizzierte Methodik wurde nun auf die hier identifizierten Risiken angewendet. Dadurch entstand die in der beigefügten Excel-Tabelle zu

findende Risikobewertung. Eine Zusammenfassung, sowie die wichtigsten Ergebnisse sollen in diesem Dokument noch einmal separat mit aufgenommen werden.

TABELLE 2 zeigt eine Zusammenfassung der Bewertungen je Kategorie. Die farblich markierten Balken geben Aufschluss über die in Zahlen verfassten Ergebnisse. Kategorie R2 – Zutrittskonzept und R3 – Brandschutzkonzept weisen dabei Handlungsbedarf auf. Zusätzlich könnte auch Kategorie R7 – Sonstiges als kritisch angesehen werden. Die anderen Kategorien sind bereits sehr gut aufgestellt, was bedeutet, dass bereits bestehende Maßnahmen wirksam sind.

Tabelle 2: Zusammenfassung der Risikobewertung nach Kategorie [Auszug aus der beigefügten Excel-Tabelle] (erstellt von dem Verfasser, 2017).

Lfd.-Nr.	Kategorie	-	Bewertung	+	Min/Max Punkte
R0	Allgemeines	0.8	9	1 2 2.6	-20/+20
R1	Gebäudestruktur und Gebäudeaufteilung	0.6	6	1 2 2.6	-12/+12
R2	Zutrittskonzept	3 2 1	-16	0.3	-24/+24
R3	Brandschutzkonzept	1.2 1	1	1 1.4	-20/+20
R4	Kühlanlagen	0	12	1 2 3 4	-12/+12
R5	Stromversorgung	0.5	5	1 1.8	-16/+16
R6	Energieeffizienz	0	4	1 2 3 4	-4/+4
R7	Sonstiges	1	1	1 1.3	-12/+12
R8	Lage des Rechenzentrums	0	8	1 2 3 4	-8/+8

Dennoch sollten an dieser Stelle alle Risiken noch einmal betrachtet werden. So geben die einzelnen Kategorien zwar preis, welche Tendenz zu erwarten ist, dennoch kann es sein, dass einzelne als kritisch bewerteten Risiken in der Zusammenfassung untergehen und nicht beachtet werden. Deshalb soll *TABELLE 3* zusätzlich noch eine Übersicht über alle Risiken und deren Bewertung geben.

Tabelle 3: Zusammenfassung der Risikobewertung [Auszug aus der beigefügten Excel-Tabelle] (erstellt von dem Verfasser, 2017).

+	Bewertung	-	Zuordnung
4 3 2 1	-4		R2.01; R2.04; R2.05; R2.06; R3.01;
3 2 1	-3		
2 1	-2		R1.03; R2.03; R3.07; R7.03;
1	-1		R5.03; R5.04; R7.02;
	N/A		R0.01; R0.05; R0.06; R3.02; R3.05;
	1	1	R3.06;
	2	1 2	R0.03; R2.02;
	3	1 2 3	R0.08; R3.03; R3.04; R5.01;
	5	1 2 3 4	R0.02; R0.04; R1.01; R1.02; R4.01; R4.02; R4.03; R5.02; R6.01; R7.01; R8.01; R8.02;

Die Risiken werden hier den einzelnen Bewertungen zugeordnet. Interessant sind vor allem die mit -4, -3 und -2 bewerteten Risiken. Hier finden sich lediglich Risiken der Kategorien R1, R2, R3 und R7. Bis auf das Risiko R1.03 passt dies zu den in der Zusammenfassung der Kategorien identifizierten Risiken mit Handlungsbedarf. Diese Risiken decken sich größtenteils mit dem zu Beginn festgelegten Schwerpunkt dieses Konzeptes, der sich auf die Zutrittskonzepte und den Brandschutz fokussiert. Im Folgenden Kapitel sollen für die hier identifizierten Risiken nun entsprechende Maßnahmen-empfehlungen getroffen werden, womit die Risiken behandelt werden könnten.

Es sollte jedoch ebenfalls angemerkt werden, dass der Großteil der identifizierten Risiken bereits behandelt wurde und es keinen Handlungsbedarf gibt. Insofern werden diese Risiken im Folgenden nicht weiter beachtet und keine Maßnahmenempfehlungen ausgesprochen. Es empfiehlt sich jedoch ggf. je nach vorhandenen Ressourcen auch diese Risiken zu betrachten um zu einem späteren Zeitpunkt ggf. Maßnahmen umzusetzen um das Risiko noch weiter zu minimieren. Potential hierfür ist jedenfalls gegeben.

4 Maßnahmen

Ausgehend der vorausgegangenen Risikoanalyse werden nun Maßnahmenempfehlungen ausgesprochen, um das Risiko der Risiken zu senken, bei denen ein Handlungsbedarf festgestellt wurde. Dabei werden die jeweiligen Risiken noch einmal beschrieben und anschließend eine oder mehrere Maßnahmen benannt die zur Senkung des Risikos beitragen können. Alle Maßnahmen können im Maßnahmenkatalog nachgeschlagen werden. Dieser befindet sich in der dem Dokument beigefügten Excel-Tabelle.

4.1 R1 – Gebäudestruktur und Gebäudeaufteilung

Im Bereich der Gebäudestruktur und –aufteilung gibt es nur bzgl. des Risikos *R1.03* Handlungsbedarf (*SIEHE TABELLE 4*).

Tabelle 4: Zu behandelnde Risiken der Kategorie R1 (erstellt von dem Verfasser, 2017).

Lfd.-Nr.	Kategorie	-		Bewertung		+		Anmerkungen
R1.03	Angrenzende Räumlichkeiten		2	1	-2			Es grenzt zur Westseite hin ein Büroraum an in dem sich IT-Administratoren befinden. Der Raum weist einige Brandlasten aus und ist nur bedingt vom Rechenzentrum baulich abgeschirmt.

Da es sich um ein Bestandsgebäude handelt und die Unterbringung des Rechenzentrums in den derzeitigen Räumlichkeiten nicht optimal ist, aber auch nicht geändert werden kann, ist eine Maßnahmenempfehlung bzgl. dieses Risikos schwierig. Eine Maßnahme wäre es die Räumlichkeiten anderweitig zu nutzen oder das gesamte Rechenzentrum zu verlegen (*M1.01*). Dies wird allerdings keine befriedigende Lösung darstellen, weshalb an dieser Stelle eine Risikoakzeptanz unumgänglich erscheint. Da das festgestellte Risiko mit einer -2 nach der vorliegenden Methodik bewertet wurde erscheint dies ein durchaus realistischer und annehmbarer Kompromiss zu sein.

4.2 R2 – Zutrittskonzept

Im Bereich der Zutrittskonzeption wurde der größte Handlungsbedarf bei der Bewertung festgestellt. In diesem Bereich fielen insgesamt fünf Risiken auf, die

durch weitere Maßnahmen ergänzt werden sollten. Eine Liste mit diesen fünf Risiken ist in *TABELLE 5* zu finden.

Tabelle 5: Zu behandelnde Risiken der Kategorie R2 (erstellt von dem Verfasser, 2017).

Lfd.-Nr.	Kategorie	-				Bewertung	+				Anmerkungen
R2.01	Zutrittskontrollsystem	4	3	2	1	-4					-
R2.03	Berechtigungs-verwaltung			2	1	-2					Eine organisatorisch geregelte Berechtigungsverwaltung für den physischen Zutritt zum RZ besteht nicht (siehe Schließsystem).
R2.04	Zonenmodell	4	3	2	1	-4					Es existiert kein Zonenmodell zur Einteilung der Räumlichkeiten in sicherheitsrelevante Bereiche.
R2.05	Videoüberwachung	4	3	2	1	-4					Es existiert keine Videoüberwachung, weder eine Volumenüberwachung, noch eine Zutrittsüberwachung.
R2.06	Einbruchmeldeanlage	4	3	2	1	-4					Es existiert keine EMA, weder für das RZ noch für das gesamte WWZ Gebäude.

Die Implementierung eines einheitlichen elektronischen Zutrittskontrollsystems (*M2.01*) wäre wünschenswert, im Rahmen der Möglichkeiten und finanziellen Mitteln der Hochschule jedoch nur bedingt umsetzbar. Da allerdings an einheitlichen, elektronischen Zugangssystemen bereits gearbeitet wird, bzw. dies in anderen Gebäuden der *THB* bereits umgesetzt werden, könnte die Implementierung auch auf das *WWZ* ausgeweitet werden.

Unabhängig eines Zutrittskontrollsystems sollte eine Berechtigungsverwaltung eingeführt werden (*M2.02*). Die bisher recht legere Handhabung der Schlüsselvergabe (besonders innerhalb der IT-Verwaltung) sollte strukturierter und geregelter werden. Es sollten Rollen vergeben werden und Regeln definiert, die den Zutritt zum Rechenzentrum und den Servern regeln.

In Verbindung mit, oder unabhängig der Zutrittskontrollsysteme und Berechtigungsvergabe sollte über die Entwicklung eines Zonenmodells (*M2.03*) nachgedacht werden. Dies scheint aufgrund der Größe des Rechenzentrums für dieses alleine nicht nötig zu sein, könnte aber im Rahmen einer hochschulweiten Implementierung auch das Rechenzentrum berücksichtigen.

Die zusätzliche Implementierung einer Videoüberwachung (*M2.04*) und Einbruchmeldeanlage (*M2.05*) sind im Hinblick auf das Rechenzentrum alleine evtl. etwas hochgegriffen, könnten aber in einem hochschulweiten System integriert werden. Eine Videoüberwachung an Hochschulen ist heut zu Tage genau so realistisch und vorstellbar wie eine Einbruchmeldeanlage.

4.3 R3 – Brandschutzkonzept

In Sachen Brandschutz gab es zwei Risiken, die einen Handlungsbedarf aufweisen. Zum einen gibt es keine Löschanlage, und zum anderen die teilweise ungeeignete Lokation der Server bzw. Racks (*SIEHE TABELLE 6*).

Tabelle 6: Zu behandelnde Risiken der Kategorie R3 (erstellt von dem Verfasser, 2017).

Lfd.-Nr.	Kategorie	-				Bewertung	+				Anmerkungen
R3.01	Löschanlage	4	3	2	1	-4					Es gibt keine Löschanlage, weder für das RZ noch für das WWZ.
R3.07	Lokation der Server			2	1	-2					Der Rack mit den Switches liegt nur wenige Zentimeter entfernt zur westlichen Wand. Das dahinterliegende Büro würde im Fall eines Brandes auch mit bestehender F90 Wand eine enorme Hitzestrahlung auf den Rack abgeben.

Ähnlich des Risikos *R1.03* können in diesen Fällen wieder nur bedingt Maßnahmenempfehlungen ausgesprochen werden. Die Implementierung einer Löschanlage ist aufgrund bautechnischer Begebenheiten nicht möglich. Evtl. existierende Lösungsansätze wären aus wirtschaftlicher Sicht nicht Tragbar für die Hochschule. Insofern scheint auch hier die einzige Möglichkeit das Risiko zu akzeptieren. Ggf. wäre dies eine Argumentation um das Rechenzentrum anderweitig unterzubringen.

Auch die Lokation der Server bzw. Racks innerhalb des Rechenzentrums wird nur mit relativ hohem Aufwand möglich sein. So wäre abzuschätzen, ob der Rack mit den Switches ggf. ebenfalls in das Rauminnere platziert werden kann, weg von der anliegenden Wand. Hierfür müssten ggf. bauliche Eingriffe stattfinden. Die Maßnahmen sind im beigefügten Maßnahmenkatalog unter *M3.01* und *M3.02* zu finden.

4.4 R7 – Sonstiges

Das letzte festgestellte Risiko, *R7.03* (*SIEHE TABELLE 7*), beschränkt sich auf einen nicht vorhandenen Lichtschutz des Rechenzentrums.

Tabelle 7: Zu behandelnde Risiken der Kategorie R7 (erstellt von dem Verfasser, 2017).

Lfd.-Nr.	Kategorie	-				Bewertung	+				Anmerkungen
R7.03	Lichtschutz			2	1	-2					Das RZ hat zwei relativ große Fensterflächen die jedoch weder innen noch außen einen Lichtschutz aufweisen. Da sich die Fenster an der Nordwand befinden relativiert sich dieser Mangel ein wenig.

Eine Maßnahme zur Reduzierung des Risikos stellt die Installation eines Sicht- bzw. Lichtschutzes dar (*M7.01*). Durch eine einfache Jalousie könnte die Wärmeeinstrahlung bereits reduziert werden. Zwar wäre die Anbringung einer äußeren Jalousie wünschenswert, dies wäre jedoch aufwendiger und evtl. auch kostenintensiver als eine Anbringung im Inneren des Rechenzentrums.

5 Ausblick

Bei der Begehung wurde festgestellt, dass bereits einige Maßnahmen im Rechenzentrum umgesetzt wurden und somit viele der Anforderungen bereits erfüllt wurden. Dies spiegelte sich auch in der Risikobewertung wieder. Mit dem spezifischen Schwerpunkt, der hier auf die Zutrittskontrolle und den Brandschutz gelegt wurde, ergaben sich letztendlich dennoch insgesamt neun Maßnahmen, die das Sicherheitsniveau des Rechenzentrums erhöhen würden. Es ist jedoch festzuhalten, dass nicht alle Maßnahmen auch wirtschaftlich sind und aufgrund baulicher Gegebenheiten nicht umgesetzt werden können. Im Hinblick auf eine langfristig geplante Re-Lokalisierung des Rechenzentrums wird es ggf. realistischer sein einige Restrisiken zu akzeptieren. Dennoch gibt es ein paar Maßnahmenempfehlungen die auch mit relativ wenig Aufwand und finanziellen Mitteln umgesetzt werden könnten.

Bei der Bearbeitung hat sich die Vorgehensweise mit einer Checkliste als gut erwiesen. Die im Vorfeld präparierte Liste hat es erlaubt die Begehung strukturiert anzugehen und die Ergebnisse einheitlich festzuhalten. Bei der späteren Bearbeitung der Risiken konnte man sich weiterhin an der Checkliste orientieren, sodass sich ein einheitliches und übersichtliches System ergeben hat. Dennoch wurden bereits bei der Begehung einige Punkte gesehen, die noch nicht in der Liste erfasst waren, weshalb die Liste zu Beginn öfters angepasst werden musste. Der modulare Aufbau des Sicherheitskonzeptes erlaubt die relativ einfache Anpassung der Risikobewertung und des Maßnahmenkatalogs. Dadurch können die Ergebnisse auch später noch angepasst werden oder neue Maßnahmen ergänzt werden. Auch die Beurteilung anderer Rechenzentren könnte anhand dieses Vorgehens relativ einfach durchgeführt werden.

Literaturverzeichnis

DIN EN 50600. (2017). Informationstechnik - Einrichtungen und Infrastrukturen von Rechenzentren. Teil 1: DIN EN 50600-1:2013 Allgemeine Konzepte; Teil 2-1: DIN EN 50600-2-1:2014 Gebäudekonstruktion; Teil 2-2: DIN EN 50600-2-2:2014 Stromversorgung; Teil 2-3: DIN EN 50600-2-3:2015 Regelung der Umgebungsbedingungen; Teil 2-4: DIN EN 50600-2-4:2015 Infrastruktur der Telekommunikationsverkabelung; Teil 2-5: DIN EN 50600-2-5:2016 Sicherungssysteme; Teil 3-1: DIN EN 50600-3-1:2016 Informationen für das Management und den Betrieb; Teil 4-1: DIN EN 50600-4-1:2017 Überblick über und allgemeine Anforderungen an Leistungskennzahlen; Teil 4-2: DIN EN 50600-4-2:2017 Kennzahl zur eingesetzten Energie; Teil 4-3: DIN EN 50600-4-3:2017 Anteil erneuerbarer Energien. Berlin: Deutsches Institut für Normung e.V.

ONR 49000. (2014). Risikomanagement für Organisationen und Systeme – Begriffe und Grundlagen. Wien: Austrian Standards.

Anhang

Siehe beiliegendes Excel-Dokument.

Ehrenwörtliche Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen oder Hilfsmittel benutzt habe und dass die Arbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt wurde.

Bisingen, den 29.07.2017

Ort, Datum

Unterschrift

(Hendrik Müller)