Hochschule
Augsburg University of
Applied Sciences

Fakultät für Informatik

Bachelorarbeit

Studienrichtung

Wirtschaftsinformatik

Farruh Djumayev
Vorgehensweise bei der Einführung eines IT-Risikomanagements an Hochschulen

Prüfer: Prof. Dr. Clemens Espe

Zweitprüfer: Christian S. Fötinger

Abgabe der Arbeit am: 19.10.2018

Hochschule für angewandte
Wissenschaften Augsburg
University of Applied Sciences

An der Hochschule 1
D-86161 Augsburg

Telefon +49 821 55 86-0
Fax +49 821 55 86-3222
www.hs-augsburg.de
info@hs-augsburg.de

Fakultät für Informatik
Telefon: +49 821 5586-3450
Fax: +49 821 5586-3499

Verfasser der Bachelorarbeit:
Farruh Djumayev
Moosacherstr. 81,
80809 München
Telefon: +4917620565261
djumayev@gmx.de

Erklärung zur Bachelorarbeit

Hiermit versichere ich, die eingereichte Abschlussarbeit selbstständig verfasst und keine anderen als die von mir angegebenen Quellen und Hilfsmittel benutzt zu haben. Wörtlich oder inhaltlich verwendete Quellen wurden entsprechend den anerkannten Regeln wissenschaftlichen Arbeitens zitiert. Ich erkläre weiterhin, dass die vorliegende Arbeit noch nicht anderweitig als Abschlussarbeit eingereicht wurde.

Das Merkblatt zum Täuschungsverbot im Prüfungsverfahren der Hochschule Augsburg habe ich gelesen und zur Kenntnis genommen. Ich versichere, dass die von mir abgegebene Arbeit keinerlei Plagiate, Texte oder Bilder umfasst, die durch von mir beauftragte Dritte erstellt wurden.

_____ _____

Ort, Datum Unterschrift des/der Studierenden

Abstract

Diese Bachelorarbeit unterstützt Hochschulen wie andere Organisationen bei der Einführung eines IT-Risikomanagements nach der ISO/IEC 27005. Nicht nur theoretische, sondern auch praxisorientierte Beispiele vermitteln der Leserinnen und Lesern ein Verständnis über den Risikomanagementprozess. Die einzelnen Risikomanagementprozessschritte sowie die Festlegung des Kontextes, die Risikobewertung, Risikobehandlung und Risikoakzeptanz werden untersucht, dokumentiert und in den vorbereiteten Formularen dargestellt.

Außerdem wird eine kurze Anleitung für Vorfall-, Change- und Projektmanagement zur Verfügung gestellt, damit eine schnelle Risikoanalyse durchgeführt werden kann.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
BayHSchG	Bayerisches Hochschulgesetz
Bed.	Bedrohung
BIOS	Basic Input /Output System
CCTV	Closed C-circuit Television (Überwachungskamerasysteme)
DDoS	Distributed Denial of Service
HIS	Hochschul-Informations-System
IEC	International Electrotechnical Commission
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnik
ITIL	Information Technology Infrastructure Library
IT-SecBe	Informationssicherheitsbeauftragter
OLE	Object Linking and Embedding
PDCA	Plan – Do – Check – Act
UEFI	Unified Extensible Firmware Interface

Begrifflichkeiten

Maßnahme	Maßnahmen zur Veränderung der Risiken
Anforderung	Erfordernis oder Erwartung, das oder die festgelegt, üblicherweise vorausgesetzt oder verpflichtend ist
Angriff	Versuch einen Wert zu zerstören, aufzudecken und zu verändern, außer Funktion zu nehmen, zu stehlen, zu diesem unbefugten Zugang zu erhalten oder diesen unbefugt zu verwenden
Bedrohung	Mögliche Ursache eines unerwünschten Vorfalls, der zum Schaden eines Systems oder einer Organisation führen kann
Firmware	Eine Software, welche in eine Hardware integriert wurde
Informationssicherheit	Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
Integrität	Eigenschaft der Richtigkeit und Vollständigkeit
Konformität	Erfüllung einer Anforderung
Managementsystem	Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer Organisation, um Politiken, Ziele und Prozesse zum Erreichen dieser Ziele festzulegen
Prozess	Satz zusammenhängender, sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt
Schwachstelle	Von einer oder mehreren Bedrohungen ausnutzbare Schwäche eines Wertes oder einer Maßnahme
Verfügbarkeit	Eigenschaft zugänglich und nutzbar zu sein, wenn eine befugte Entität Bedarf hat
Vertraulichkeit	Eigenschaft, dass Informationen unbefugten Personen, Entitäten oder Prozessen nicht verfügbar gemacht oder offengelegt werden

1. Einleitung

1.1 Problemstellung

Risikomanagement ist bereits in vielen Bereichen jegliches Unternehmens integriert. Es ist ein wichtiger Prozess innerhalb von Projektmanagement, Finanzen, Bankwesen und Gesundheit. Ein erfolgreich durchgeführtes Risikomanagement stellt die Sicherheit der Assets, eine dauerhafte Existenz eines Unternehmens und verbesserte Geschäftsprozesse sicher.

Im Gegensatz zu einem Unternehmen haben die Bildungseinrichtungen bzw. Hochschulen andere Strukturen, Prozesse und Bereiche. Aus diesem Grunde weichen die Erwartungen einer Hochschule an Risikomanagement ein wenig von jenen eines Unternehmen ab.

Da eine Hochschule einen starken Fokus auf Forschung und Entwicklung legt, ist es allerdings hier sehr wichtig, dass die Geräte, Systeme und Informationen sicher sind. Darüber hinaus sind die Hochschulnetze besonders stark zu schützen. Da die Hochschulen zu öffentlichen Einrichtungen gehören, könnte auf die Hochschulnetze von einem potenziellen Angreifer in einer unkomplizierten Art und Weise zugegriffen und diese ausgenutzt werden. Als Folge ist es möglich, dass die Verfügbarkeit und Integrität nicht mehr gewährleistet sind.

Den bei den Hochschulen dafür verantwortlichen Stellen begegnen viele Hürden bei der Durchführung eines Risikomanagements. Der Hauptgrund dafür ist, dass einer Hochschule weniger Budget als einem Unternehmen zur Verfügung steht. Eine weitere Schwierigkeit liegt darin, eine passende Vorgehensweise und Methodik für das Risikomanagement zu finden.

Obwohl die bestehenden Standards und Normen dafür eine Lösung anbieten, sind diese Vorgehensweisen nicht für eine Hochschule geeignet. Oft sind sie sehr detailliert oder entsprechen nicht den Hochschulzielen. Eine richtige Vorgehensweise dient als ein Schlüssel für den Erfolg des Risikomanagements sowie den einer Hochschule.

1.2 Motivation

Die Bekämpfung der Phishing-, Ransomware- sowie Distributed-Denial-of-Service-Angriffe (DDoS) ist eine wichtige Aufgabe von Unternehmen und Organisationen geworden, weil die Cyberkriminalität von Jahr zu Jahr kontinuierlich wächst. Laut Statista

hat sich die Anzahl der polizeilich erfassten Fälle von Cyberkriminalität zwischen 2002 und 2018 fast verdoppelt und Millionen Euro Schaden verursacht. (Blog Avira, 2018) Der Schutz der Vermögenswerte der Hochschulen und Universitäten ist sehr wichtig. Da die Hochschulen zum öffentlichen Dienst gehören, ist es schwierig, das Risikomanagement einzuführen. Andererseits, wenn jemand die Daten über die Studenten, Prüfungs- und Forschungsergebnisse manipulieren würde, verlören die Hochschulen ihr Image, Vertrauen und Wirtschaftsgüter. Aus diesem Grund ist es notwendig, dass Hochschulen das Informationssicherheitsmanagement einführen und kontinuierlich den Risikomanagementprozess durchführen. In den meisten Unternehmen ist schon das Informationssicherheitsmanagementsystem (ISMS) eingeführt, aber im öffentlichen Sektor noch nicht vollständig. Diese Themen und Problemfelder werden in dieser wissenschaftlichen Arbeit untersucht und für deren Lösung und Realisierung Vorschläge gegeben.

1.3 Zielsetzung und Forschungsfrage

Über die Bewertung der Informationssicherheit und des Risikomanagements gibt es in den Standards und im deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) viele Informationen. Da viele Organisationen sowie die Hochschulen keinen IT-Grundschutz umgesetzt haben, ist es schwierig, sofort mit dem Risikomanagement anzufangen. Das Ziel der vorliegenden wissenschaftlichen Arbeit ist es, eine praxisorientierte Dokumentation für die Einführung des Risikomanagements an den Hochschulen vorzubereiten, damit diese ohne große Schwierigkeiten eine Risikoanalyse durchführen können. Die Vorgehensweise bei der Einführung des Risikomanagements wird Schritt für Schritt in der Arbeit mit dem Fallbeispiel erklärt und die Formulare zur Sammlung der Informationen über die Organisationswerte und zur Durchführung des Risikomanagements als Prototypen erstellt.

Da die Hochschulen zu dem öffentlichen Sektor gehören, muss man zuerst fragen, wie der Informationssicherheitsrisikomanagementprozess an den Hochschulen praxisorientiert eingesetzt werden kann? Welche Standards und Normen passen am besten für bei der Einführung des Risikomanagements an den Hochschulen und welche Schritte müssen dabei ausführlich betrachtet werden? Welche Formulare werden bei der Einführung des Risikomanagements gebraucht, um die Risiken zu identifizieren und die Risikoanalyse durchzuführen?

Das sind die in dieser Arbeit zu diskutierenden und zu beantwortenden Forschungsfragen.

1.4 Aufbau der Arbeit

Nachdem die Problemstellung, Zielsetzung und Forschungsfrage der Arbeit erläutert wurden, gliedert sich die Arbeit in drei thematische Bereiche.

Im zweiten Kapitel werden die vorhandenen Standards, Normen und Methodik für das Informationssicherheitsrisikomanagement vorgestellt.

In Kapitel drei wird der gesamte Risikomanagementprozess von ISO/IEC 27005 mit einfachen Beispielen Schritt für Schritt erklärt und die für den Risikomanagementprozess benötigten Formulare zur Verfügung gestellt.

Die vorgestellten Beispiele gelten als Musterlösungen bei der Einführung eines Risikomanagements an Hochschulen. Dabei werden die Beispieldaten verwendet.

Kapitel vier umfasst die weiteren Einsatzbereiche des Risikomanagementprozesses an den Hochschulen. Informationssicherheitsvorfallmanagement, Changemanagement und Projektmanagement dienen dabei als wichtige Informationsquellen für die Risikobewertung.

Ein Fazit bildet den Schluss der Arbeit.

2. Einführung in das IT-Risikomanagement

Bereits in der Antike begegneten den Menschen diversen Risiken in ihrem alltäglichen Leben. Unwetter, Hungersnöte und Kriege waren die häufigsten Risiken jener Zeit, die den Alltag der damaligen Menschen beeinträchtigten. Zur Verhinderung oder Bewältigung möglicher Risiken versuchten sie, Gegenmaßnahmen zu treffen. Zum Beispiel wendeten sich die alten Griechen an ihre Götter, um die Zukunft vorhersagen zu können. Diese Art und Weise des Risikomanagements in antiker Zeit war eng mit den Göttern und Alltagserfahrungen der Menschen verbunden.

Im heutigen digitalen Zeitalter werden die Götter quasi durch die modernen Technologien und Methoden ersetzt, um genauere Prognosen der Zukunftsereignisse in Echtzeit zu ermöglichen. Die großen Unternehmen heutiger Zeit wie Amazon und Google sammeln eine große Menge an Daten. Anhand von Korrelationen und moderner Methoden der Datenanalyse stellen die Datensammler den anderen Unternehmen eine exakte Berechnung der zukünftigen Prognosen bereit.

Die weltweite Verwendung des Internets und von Computern sowie mobilen Geräten ermöglicht eine globale Vernetzung und einen blitzschnellen Informationsaustausch. Darüber hinaus zählen sie als Basisfaktoren für das Produzieren der Informationen.

Die Einführung neuer Technologien hat das Leben der Menschen auf einer Seite zwar sehr erleichtert, auf der anderen Seite entstehen aber auch neue Risiken.

Es werden immer mehr Daten in den Unternehmen produziert. Für die Gewährleistung eines reibungslosen Betriebs sollen die Unternehmensdaten geschützt werden. Allein Datenschutz ist heutzutage nicht ausreichend, ein erfolgreiches und konkurrenzfähiges Geschäft führen zu können. Die Unternehmen sollen ständig ihre Prozesse verändern und verbessern. Jede Änderung beinhaltet ihre Chancen und Risiken. Um die Risiken frühzeitig zu erkennen und diese beseitigen zu können, müssen sich die Unternehmen mit dem Risikomanagement beschäftigen. (Romeike, 2018)

An dieser Stelle ist es sinnvoll, die grundlegenden Begrifflichkeiten des Risikomanagements zu betrachten.

Obwohl die Wurzeln des Wortes „Risiko“ aus der arabischen und griechischen Sprache stammen, erklärt der deutsche Duden die Herkunft des Wortes als vulgärlateinisch (risicare). Das vulgärlateinische „risicare“ bedeutet „Gefahr laufen, wagen“.

Nach deutschem Sprachgebrauch steht das Wort Risiko für „mit einem Vorhaben verbundenes Wagnis, möglicher negativer Ausgang bei einer Unternehmung, Möglichkeit des Verlustes“ (vergl. Duden online).

Abbildung 1 veranschaulicht den Zusammenhang und Unterschied zwischen den Risiken und Chancen.

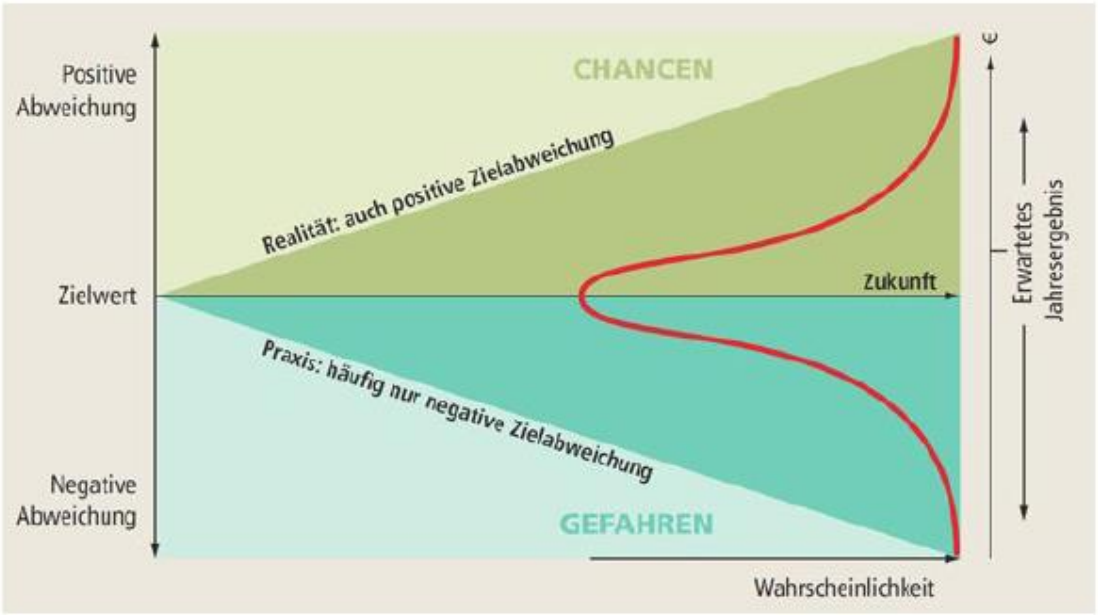

Abbildung 1: Begriff des Risikos (Quelle: Risikomanagement, Frank Romeike, S. 8-13)

Die Grundlage beider Ausdrücke bilden die Zielwerte, die vom Unternehmen während der Planung als zukünftig erwartendes Ergebnis festgelegt wurde. Unter dem Begriff Risiko wird meistens die ungewisse Folge einer Handlung oder die negative Abweichung geplanter Zielwerte verstanden. Liegen die erzielten Ergebnisse unter den Erwartungen, so spricht man von Risiken. Im Gegensatz werden die Chancen als übertroffene Zielwerte bezeichnet.

Die Hauptaufgabe des Risikomanagements besteht darin, die Chancen zu nutzen und die möglichen Risiken zu verhindern. Dabei ist es wichtig, Risikomanagement als einen kontinuierlichen Unternehmensprozess zu definieren. Zum Erreichen des beabsichtigten Zieles sollen die Quellen, Konsequenzen und Gegenmaßnahmen der potenziellen Risiken vollständig erfasst werden.

Vielen Unternehmen gelingt es nicht, ein Risikomanagement erfolgreich einzuführen. In den meisten Fällen liegt es daran, dass den Unternehmen das erforderliche Wissen über

Methoden und Vorgehensweise des Risikomanagements beziehungsweise über dessen Anwendung fehle. Das moderne Risikomanagement verlangt nämlich eine präzise Planung, eine übersichtliche Struktur und eine kontinuierliche Prozessverbesserung.

2.1 Normen und Standards für das Unterstützen des Informationssicherheitsrisikomanagements

Zur systematischen und effektiven Einführung des Risikomanagements wurden weltweit eine Reihe von Standards und Normen entwickelt. Die Standardisierung verfolgt das Ziel, jedem Lesenden ein vereinheitlichtes Verständnis zum Thema Risikomanagement zu vermitteln.

In den folgenden Kapiteln sind jene bekannten Standards aufgelistet, welche von Unternehmen oder Organisationen oft genutzt werden.

2.1.1 Prozessschritte von ISO/IEC 27005

Die ISO/IEC 27005 gehört zur ISO/IEC 27000 Familie, die sich hauptsächlich dem Aufbau eines Informationssicherheitsmanagementsystems (ISMS) widmet. Das Risikomanagement wird hier als Bestandteil der Unternehmensprozesse betrachtet. Die ISO/IEC 27000 Reihe weist darauf hin, dass Risikomanagement möglichst früh, und zwar, bereits bei der Planung eines ISMS miteinzubeziehen.

Die genauen Anforderungen für die Informationssicherheit hinsichtlich Risikobeurteilung und Risikobehandlung stehen in der ISO/IEC 27001. Mit der Vorgehensweise und Erklärung der einzelnen Schritte des Risikomanagementprozesses beschäftigt sich hingegen die ISO/IEC 27005.

In dieser Norm sind die erfolgreichen Risikomanagementmethoden und -vorgehensweisen besonders hinsichtlich des Informationssicherheitsmanagements beschrieben. Das Risikomanagement nach ISO/IEC 27005 analysiert die möglichen Ereignisse, stellt die Prioritäten fest und trifft Entscheidungen darüber, welche Gegenmaßnahmen wann angewendet werden sollen.

2.1.2 Risikomanagement im BSI-Standard 200-3

Dieser Standard betrachtet alle Risiken, die bei der Einführung des IT-Grundschutzes vorkommen können. Der IT-Grundschutz wurde vom Bundesamt für Sicherheit in der Informationstechnik veröffentlicht und beinhaltet die erforderlichen Vorgehensweisen, um die Sicherheitsmaßnahmen zu definieren und zu verwenden. Der BSI-Standard 200-3 bietet

den Organisationen ein Vorgehen zur Steuerung deren Risiken im Bereich Informationssicherheit an.

In diesem Standard wird der Risikomanagementprozess als Risikoanalyse bezeichnet. Dennoch werden hier ähnliche Schritte wie in den ISO/IEC Normen 27005 und 31000 (siehe folgende Abschnitt) durchgeführt.

2.1.3 Weitere Standards und Normen im Bereich Risikomanagement

Die Norm ISO/IEC 31000 (Risikomanagementprinzipien und -richtlinien) dient aufgrund ihrer allgemein-gültigen Richtlinien als ein Masterstandard für das Risikomanagement. In allen Bereichen wie zum Beispiel Finanzen, Maschinenbau und Sicherheit unterstützt ISO/IEC 31000 die Organisationen, um ihre eigenen Pläne hinsichtlich der Risiken zu verbessern sowie die jeweils richtigen Entscheidungen zu treffen.

Eine Reihe der in diesem Standard beschriebenen Richtlinien stellen außerdem die Effektivität eines Risikomanagements sicher.

Die Information Technology Infrastructure Library (ITIL) bietet eine Reihe von Prozessen, Rollen und Funktionen an, welche in kleinen, mittelständischen und großen Unternehmen zum Einsatz kommen können. ITIL gehört nicht zu einem Standard, sondern ist eine Sammlung von Best-Practise-Methoden aus den Management- und Servicebereichen. Deshalb kann ein Unternehmen die ITIL-Prozesse für sich anpassen und diese implementieren.

ITIL kann man als eine langjährige Dokumentation bezeichnen, die aus gewonnenen Erfahrungen die besten Lösungen herausfiltert und diese bereitstellt. Dabei stammen Erfahrungen nicht nur von einem, sondern von mehreren Unternehmen.

Dank der ITIL hat ein Unternehmen die Möglichkeit, einen Überblick über die Umsetzung der vordefinierten Prozesse zu bekommen. Jedoch wird die Zielerreichung durch die Komplexität der Inhalte von ITIL oft erschwert.

Das Unternehmen, welches ITIL-Lösungen umsetzen möchte, hat mit viel Kosten und Zeitbedarf zu rechnen. Da man für die Umsetzung der ITIL-Lösungen speziell ausgebildete Consultants braucht und dafür ITIL-Software gekauft werden muss, muss ein Unternehmen dafür viel Geld zur Verfügung stellen. Außerdem nimmt die Implementierung der Prozesse viel Zeit in Anspruch.

Die Hochschulen zählen zu den öffentlichen Organisationen. An den meisten deutschen Hochschulen, insbesondere in Bayern, wurden die Studiengebühren seit dem Jahr 2013

abgeschafft oder reduziert. Dies führte mit dazu, dass die Hochschulen nur über ein niedriges Budget für ihre IT-Infrastruktur und -Prozesse verfügen. Die teuren und zeitaufwendigen ITIL-Lösungen können daher keine Lösung für den Risikomanagementprozess an einer Hochschule sein.

2.2 Allgemeine Anforderungen und Richtlinien für den öffentlichen Sektor

Das enorme Wachstum der Cyberkriminalität in den letzten Jahren stellt große Herausforderungen für die Organisationen dar. Heutzutage investieren die Unternehmen immer mehr Geld in die Informationssicherheit, damit ihre IT-Assets und ihre sensiblen Daten geschützt sind. Obwohl sich die Ziele und Struktur einer Hochschule von denen eines Unternehmens unterscheiden, ist die Informationssicherheit für die Hochschulen ein wichtiges Thema.

Es gibt in Deutschland insgesamt 428 Hochschulen. Davon sind 217 Fachhochschulen, 106 Universitäten und 105 gehören zu weiteren Hochschularten. Jedes Bundesland hat ein eigenes Hochschulgesetz; in Bayern gilt das Bayerische Hochschulgesetz (BayHSchG) vom 23. Mai 2006.

Die Hochschulen fördern die Wissenschaft und Kunst durch Forschungs-, Studiums- und, Weiterbildungsprogramme und durch die Programme für Lehre. Die meisten Hochschulen werden vom Staat finanziert.

Der Schutz der Mitarbeiter- und Studentendaten sowie, der Forschungs- und Prüfungsergebnisse ist für die Sicherstellung ihrer Prozesse eine Grundvoraussetzung für die Hochschulen. Aus diesem Grund müssen sich die Hochschulen mit der Informationssicherheit auseinandersetzen und dafür Finanzmittel bereitstellen, um die möglichen Gefahren bezüglich der Informationssicherheit frühzeitig zu erkennen und diese zu beseitigen.

Es ist eine Herausforderung für die Hochschulen, ein Informationssicherheits-managementsystem richtig einzusetzen. Jede Hochschule hat je nach Struktur und Größe die jeweils richtige Vorgehensweise, Methoden und die passenden Richtlinien für die Informationssicherheit festzulegen. Darüber hinaus sollen die Zusammenarbeit mit externen Experten im Bereich Informationssicherheit organisiert und Compliance- sowie, Security-Awareness Maßnahmen durchgeführt werden.

2.3 Bisherige Arbeiten an der Fachhochschule Augsburg

Im Kontext der Informationssicherheit beziehungsweise des Risikomanagements an der Fachhochschule Augsburg wurden bisher verschiedene wissenschaftliche Arbeiten verfasst. Im Folgenden werden diese Arbeiten und deren Inhalte erläutert. Darüber hinaus werden die weiteren Schritte benannt, welche auf den bereits vorhandenen Arbeiten basieren.

Die Masterarbeit von Fr. Schnitzler (2017) widmet sich dem Thema „A universal guideline for the implementation of a specific ISMS for all Bavarian universities and universities of applied sciences using the example of the University of Applied Sciences Augsburg“. Die universelle Leitlinie für die Umsetzung eines spezifischen ISMS für alle bayerischen Hochschulen und Universitäten ist in der Arbeit ausführlich beschrieben. Die Masterarbeit liefert zusätzlich die Informationen über passende Standards und Normen für die Hochschulen. Dementsprechend ist in der Masterarbeit ISO/IEC 27005 als ein geeigneter Standard zur Durchführung des Risikomanagements an den Hochschulen genannt.

In der vorliegenden Arbeit werden auf Basis der Masterarbeit von Schnitzler passende, kompakte und handhabbare Vorgehensweisen und Formulare für das Risikomanagement vorbereitet und in den späteren Kapiteln dargestellt.

Über das Thema „Analyse und Ausarbeitung der in den ISO-Standards 27001-27005 geforderten Prozesse zum Betrieb eines ISMS“ hat Fr. Muhamadova (2018) ihre Bachelorarbeit geschrieben. In der Arbeit geht es darum, die für den Aufbau eines ISMS erforderlichen Prozess mithilfe der Prozessmodellierung zur Verfügung zu stellen und die Prozesse ausführlich zu beschreiben.

Der von Muhamadova vorgestellte Risikomanagementprozess wird in der vorliegenden Arbeit ins Leben gerufen. Zusätzlich werden Formulare für die einzelnen Vorgänge des Risikomanagements vorbereitet und zur Verfügung gestellt.

3. Prozesse innerhalb des IT-Risikomanagements

3.1 Festlegung des Kontextes

Bei der Festlegung des Risikomanagementkontextes ist es wichtig, die Anwendungsbereiche und Grenzen, die Rollen und Verantwortlichkeiten sowie die Basiskriterien des Risikomanagements zu definieren.

3.1.1 Anwendungsbereich und Grenzen

Bevor das Informationssicherheitsrisikomanagement von einer Organisation angewendet wird, soll festgelegt werden, wo der Einsatz des Informationssicherheitsrisikomanagements sinnvoll ist und wo dieser Prozess aufhört.

Zu den üblichen Anwendungsbereichen des Informationssicherheitsrisikomanagements zählen IT-Applikationen, IT-Infrastruktur und Geschäftsprozesse einer Organisation.

Eine Hochschule unterscheidet sich mit ihren Zielen und ihrer IT-Landschaft von anderen Organisationen, und dies beides spielt bei der Festlegung der Anwendungsbereiche von Informationssicherheitsrisikomanagement eine wichtige Rolle.

Die Tabelle 1 liefert einen Überblick über die wichtigsten Aspekte, die für die Bestimmung der Anwendungsbereiche von Informationssicherheitsrisikomanagement an einer Hochschule relevant sind.

Tabelle 1: Anwendungsbereiche von ISMS (Quelle: F. Djumayev).

Aspekte	Beispiele
Hochschulziele	Exzellente Lehre, exzellente Forschung
Hochschulprozesse (Beispiele)	Prüfungsbetriebsmanagement, Durchführung der Forschungsprojekte, Haushaltsverwaltung, Studienmanagement und Infocentermanagement, Hochschulverwaltung, Personalmanagement, Studentenverwaltung, Verwaltung des Hochschulrechenzentrums
Strategien	Praxisorientierte Lehre, gute Vernetzung mit Unternehmen bei der Forschungsarbeiten
Aufbau/Organisation der Hochschule	Hochschulleitung, Senat, Hochschulrat, Studiendekan, Fakultätsrat, Kanzler/-in, Präsident/-in
Risikomanagementziele, Servicekatalog	Gewährleistung des sicheren Ablaufs von Hochschulprozessen, Verbesserung der Prozesse

Informationssicherheitsleitlinie	Leitlinie zur Informationssicherheit an der Hochschule

Aus den gewonnenen Informationen wird klar, dass die exzellente Lehre und Forschung oberste Ziele der Hochschule sind.

Da ein ordnungsgemäßer und störungsfreier Ablauf der Prozesse von großer Bedeutung ist, sollen Hochschulprozesse vor möglichen negativen Ereignissen geschützt werden. Mithilfe des Informationssicherheitsrisikomanagements werden die potenziellen Risiken festgelegt, welche den sicheren Ablauf der Hochschulprozesse gefährden können.

Bei der Durchführung des Risikomanagements lehnt sich die Hochschule an den festgelegten Leitlinien für die Informationssicherheit an.

Unter Berücksichtigung der Informationen von Tabelle 1 werden schließlich die Anwendungsbereiche des Risikomanagements definiert. Die zentrale Fragestellung ist:

Welche Prozesse sind wichtig, damit die Hochschule ihre Ziele erreichen kann?

Die Kernprozesse und die unterstützenden Prozesse stehen dabei im Fokus. Die wichtigen Prozesse, bei denen das Informationssicherheitsrisikomanagement zum Einsatz kommt, sind in der Abbildung 2 aufgelistet.

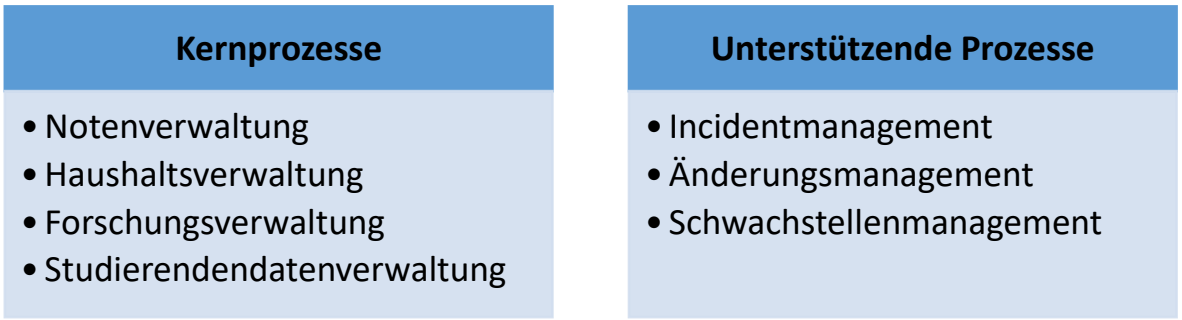

Abbildung 2: Mögliche Kern- und unterstützende Prozesse einer Hochschule (Quelle: F. Djumayev)

Nun sind die Anwendungsbereiche des Informationssicherheitsmanagements festgelegt, allerdings sagen die Prozesse nicht aus, was genau vor möglichen negativen Ereignissen geschützt werden sollen. Dafür ist jeder einzelne Prozess auf einer kleinräumigen Ebene zu untersuchen.

Bei der Festlegung der Anwendungsbereiche und Grenzen sollen alle Assets der Hochschule betrachtet werden, welche vor möglichen Risiken geschützt werden sollen. Die Bestimmung der zu schützenden Assets wird bei der Risikobewertung hilfreich sein. Das bedeutet, dass

unter Berücksichtigung aller bereits definierten Assets der Risikobewertungsvorgang später durchgeführt wird.

Festlegung und Inventarisierung der Informationswerte

Der Begriff „Wert“ oder „Unternehmenswert“ wird vielmals in der ISO/IEC 27001 verwendet. Er ist ein standardspezifischer Ausdruck und hat eine umfangreiche Bedeutung. Die Werte bezeichnen alle Assets einer Organisation, die wertvoll sind. Vor der Risikoidentifikation ist es sinnvoll, die vorhandenen Assets der Hochschule zu erkennen beziehungsweise zu inventarisieren. Die möglichen Asset-Typen sind in der folgende Abbildung 3 aufgelistet.

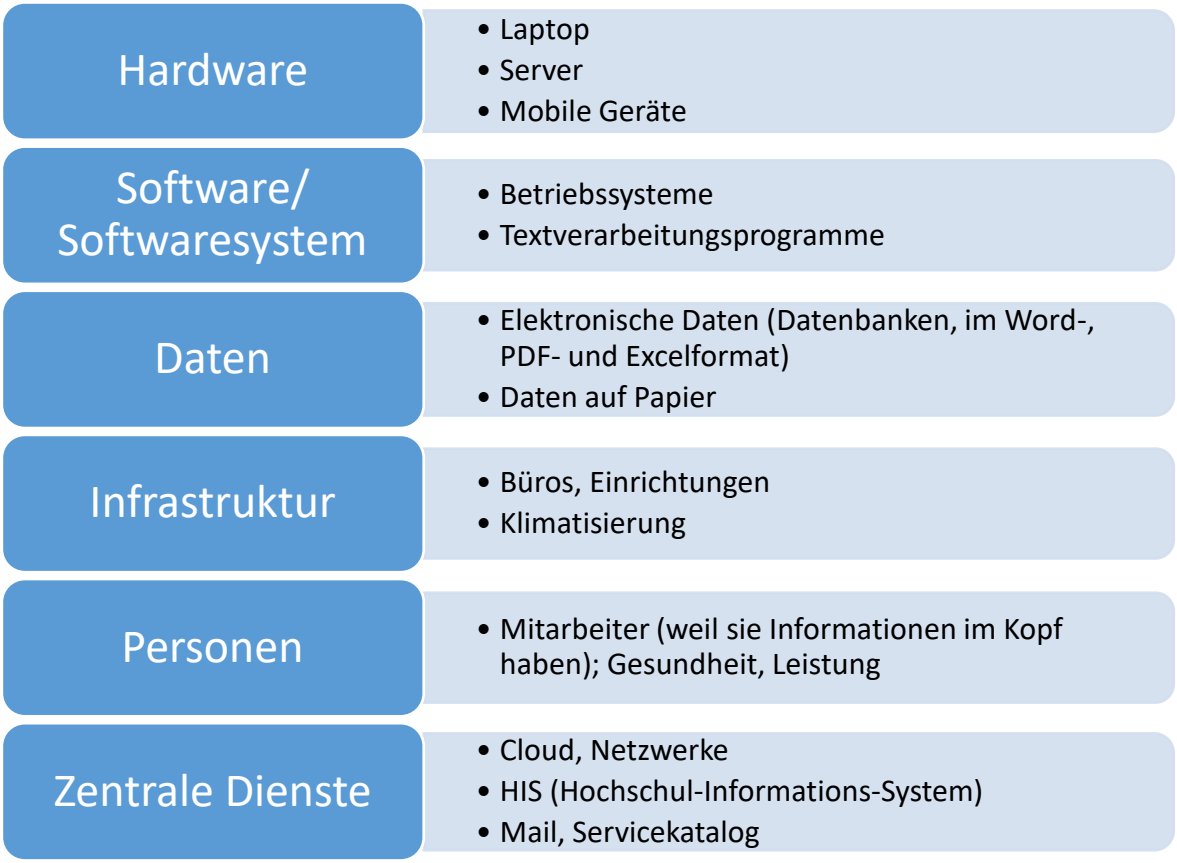

Abbildung 3: Mögliche (Informations-)Werte an Hochschulen (Quelle: F. Djumayev)

Die Asset-Inventarisierung soll die Informationen nicht nur über den Typ, sondern auch die Eigenschaften des Assets umfassen. Auf Basis der dokumentierten Asset-Eigenschaften werden in den nächsten Kapiteln die möglichen Bedrohungen und Schwachstellen, welche den Risikoauftritt begünstigen, festgestellt.

In den nächsten Abschnitten dieses Kapitels werden die einzelnen Asset-Tabellen mit wichtigen Asset-Eigenschaften dargestellt. Dafür sind die Fragen gesammelt, welche die

wichtigsten Eigenschaften eines Assets darstellen, und werden diese mit Beispielinformationen beantwortet.

Die unten folgenden Tabellen können einer Hochschule als eine Grundlage für die Inventarisierung von Assets dienen. Je nach Bedarf an Informationen über Assets können die Tabellen angepasst oder ergänzt werden.

Bei der Zusammenstellung der wichtigen Asset-Eigenschaften unten in den Tabellen wird die Sicherheit des jeweiligen Assets als Grundkriterium betrachtet.

Tabelle 2: Wichtige Informationen zur Software (Quelle: F. Djumayev)

Software/Softwaresystem	
Art der Software/des Softwaresystems?	*Textverarbeitungssoftware/Betriebssystem*
Name der Software/des Betriebssystems?	*MS Word /Windows 10 Education*
Hersteller der Software?	*Microsoft*
Welche Updatemethoden sind vorhanden oder werden angeboten?	*Microsoft-Updates*
Datum des letzten Updates/Version des Updates	*24.02.2017/KB4011681*
Welche Schnittstellen hat die Software/das Softwaresystem?	*Kalender, Drucker, Rechtschreiberkennung*
Welche Benutzer gibt es? (Wer hat Zugriff auf die Software?)	*Administrator, Benutzer mit Schreibrechten, Benutzer mit Leserechten*
In welchen Programmiersprachen ist die Software geschrieben? Auf welchen Programmiersprachen basiert die Software?	*JAVA, C++*

Bei der Durchführung des Risikomanagements für eine Software spielen die Informationen über die Softwarehersteller, die jeweilige Updateversion und die Benutzer eine entscheidende Rolle. Genauso wichtig ist die Information über die Softwaresprache, in welcher eine Software geschrieben bzw. programmiert ist.

Tabelle 3: Wichtige Informationen zur Hardware (Quelle: F. Djumayev)

Hardware	
Art der Hardware? (Laptop, mobile Geräte, Server)	*Laptop*
Name der Hardware?	*Apple MacBook*
Hersteller der Hardware?	*Apple*
Welche Anschlüsse sind auf der Hardware vorhanden? (Telefon, Maus, Drucker, USB)	*Maus, Drucker, Monitor, USB (universeller USB-Anschluss)*
Welche weitere eingebettete Software / Firmware ist auf der Hardware vorhanden?	*UEFI*

Wird eine Software vor der Installation geprüft? Durch welche Methoden und Tools?	*Ja, durch ein Antivirenprogramm*
Welche Art der Wechseldatenträger wird akzeptiert? Werden sie davor überprüft? Und wie (durch Virenscanner oder Antivirussoftware)?	*Alle Wechseldatenträger außer USB-Sticks werden nach der Virenüberprüfung akzeptiert*
Ist die Softwareinstallation auf HW eingeschränkt?	*Ja (auf firmeneigener Hardware sollte die Softwareinstallation nur eingeschränkt erfolgen)*
Wann wurde ein Sicherheitsupdate ausgeführt?	*01.01.2015*
Welche Verschlüsselungsmethoden werden angewendet (AES, RSA, digitale Zertifikate)?	*FileVault*

Genau wie die Software sollen die Informationen über die Hersteller, über die durchgeführten Sicherheitsupdates und weitere verbundene Geräte einer Hardware erfasst werden, damit die Hardwaresicherheit durch den Risikomanagementprozess gewährleistet werden kann.

Tabelle 4: Wichtige Informationen zu den Daten (Quelle: F. Djumayev)

Daten	
Art der Daten/Informationen	*Stundenplan (von WebUnits)*
Wer hat Zugriff auf die Daten?	*Lehrkräfte und Studenten*
Wer kann die Informationen ändern?	*Administrator*
Sind Back-ups vorhanden?	*Ja*
Wie wird der Zugang zu Informationen geschützt (durch ein Passwort oder andere Authentisierungsmethoden)?	*Passwort*
Wie wichtig ist die Verfügbarkeit der Daten?	*Sehr wichtig*
Wie wichtig ist die Vertraulichkeit der Daten?	*Sehr wichtig*
Wie wichtig ist die Integrität der Daten?	*Sehr wichtig*

Die Information „Sicherheit der Schutzziele“ zählt als besonders wichtiger Aspekt, der bei der Datensicherheit zu betrachten ist. Zur Gewährleistung der ständigen Verfügbarkeit von Daten ist es von Bedeutung, dass die Datensicherungen vorhanden sind. Im Standard ISO/IEC 27002 sind die Anforderungen für das Erreichen der Datensicherung bereits festgelegt. Ein modellierter Datensicherungsprozess wurde in der Bachelorarbeit von Muhamadova beschrieben und dies soll bei der Prozessumsetzung berücksichtigt werden. (*Quelle: F. Muhamadova, „Analyse und Ausarbeitung der in den ISO Standards 27001-27005 geforderten Prozesse zum Betrieb eines ISMS“, 2018*)

Tabelle 5: Wichtige Informationen zur Infrastruktur (Quelle: F. Djumayev)

Infrastruktur (Büro, Einrichtungen)	
Art der Infrastruktur	*Gebäude*
Name der Infrastruktur	*Rechenzentrum*
Ist ein Alarmplan für den Notfall vorhanden?	*Ja*
Wann wurde die letzte Notfallübung durchgeführt?	*20.09.2018*
Wie sind die Einrichtungen gegen Katastrophen oder Störungen (Feuer, Überschwemmung) geschützt?	*Durch den Rauchmelder, Feuerlöscher und Brandschutztüre*
Wann ist der Feuerlöscher das letzte Mal überprüft worden und wann wurden die Batterien der Rauchmelder getauscht?	*10.10.2015*
Ist das Rechenzentrum mit Kameras überwacht?	*Ja*
Ist der Eintritt des Personals kontrolliert und wie?	*Ja. Mit Chipkarte darf das Personal ins Rechenzentrum hineinkommen*

Die Einrichtungen zählen als Werte, weil sich in ihnen sich die wertvollen Assets wie Hardware, Rechenzentrum oder andere Dienste befinden. Zur Infrastruktursicherung sind im BSI die Hinweise und Anleitungen beschrieben. Zur Umsetzung der Hochschulinfrastruktursicherung sollen diese betrachtet werden. (Bundesamt für Sicherheit in der Informationstechnik, 2018)

Tabelle 6: Wichtige Informationen zu den Mitarbeitern (Quelle: F. Djumayev)

Personen	
Rolle der Person	*Datenschutzbeauftragter*
Ist die Qualifikation der Personen für die Mitarbeit im Bereich Informationssicherheit ausreichend?	*Ja*
Welche Schulungen haben die Personen besucht und wann zuletzt?	*IT-Sicherheitsschulung 10.09.2018*
Wie oft nehmen die Personen an den Schulungen teil?	*Alle 6 Monate*
Kennen die Personen ihre Verantwortlichkeiten und Rollen gut? Welche Unterlagen beweisen es?	*Ja. Arbeitsvertrag*
Wann werden die Zugangsrechte einer Person entzogen?	*Nach der Änderung der Abteilung/des Bereichs und nach der Kündigung*
Wer ist der Vertreter für den Sicherheitsbeauftragte?	*Keine*

Die Mitarbeiter der Hochschule können einen großen Beitrag für die Informationssicherheit leisten. Daher ist es sehr wichtig, dass die Mitarbeiter für die Informationssicherheit

sensibilisiert sind. Das bedeutet, die Mitarbeiter sollen mit den Informationen und anderen Assets bewusst umgehen. Zur Gewährleistung und Steigerung des Bewusstseins eines Mitarbeiters über die Informationssicherheit soll die Hochschule es ermöglichen, dass ihre Mitarbeiter in regelmäßigen Abständen an den erforderlichen Schulungen teilnehmen.

Für das Thema Personalsicherheit hat ISO/IEC die Anforderungen festgelegt. Die Anforderungen für Personalsicherheit, Registrierung und Deregistrierung von Benutzern, Zuteilung und Entziehung von Benutzerzugangsrechten wurden von Muhamadova (2018) modelliert und sollen berücksichtigt werden.

Tabelle 7: Wichtige Informationen zu den zentralen Diensten (Quelle: F. Djumayev)

Zentrale Dienste	
Netzwerk	
Welche Mittel werden für den Netzwerkzugang verwendet (VPN, WLAN)?	*WLAN*
Welche Verschlüsselungsmethoden werden verwendet?	*WPA2*
Wann wurde das letzte Sicherheitsupdate durchgeführt?	*01.01.2017*
Wer ist der Anbieter des Netzwerkes?	*Verein zur Förderung des deutschen Forschungsnetzes (DVN)*
Wie viele Benutzer hat das Netzwerk?	*Mehr als 8000 (an der Hochschule)*
Cloud	
Name des Anbieters von Cloud-Diensten	*Amazon*
Ist eine Verschlüsselung seitens des Cloud-Anbieters vorhanden? Welche Verschlüsselungsmethoden werden angewendet?	*Ja, End-to-End-Verschlüsselung bei der Übertragung der Informationen*
Wo befinden sich die Rechenzentren des Cloud-Services?	*Region Europa/Frankfurt*
Welche Datenschutzrichtlinien werden verfolgt? (DSVGO)	*DSVGO*
Welche Zertifizierungen werden vom Cloud-Provider angeboten (ISO 9000 oder ISO 27001)?	*ISO 27001*
Sind Backups vorhanden?	*Ja, bei einem anderen Cloud-Provider (IBM)*
E-Mail-Versand	
Welche Regelungen sind für ein sicheres Passwort vorhanden (Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen; Zwei-Faktor-Authentisierung)?	*Ein Passwort muss aus einer Kombination von Groß- und Kleinbuchstaben und mindestens aus 4 Zeichen bestehen.*
Werden Spam-Mails automatisch aussortiert?	*Ja, es wird eine intelligente Spamabwehr-Software verwendet.*

Welche Verschlüsselungsmethoden werden angewendet?	*TLS-Verschlüsselung*

Zu den möglichen zentralen Diensten einer Hochschule können, die Netzwerke, E-Mail und Cloud-Dienste gehören. Da diese interbasierend funktionieren, sollen sie besonders geschützt werden. Die Angriffe zu den meisten Assets erfolgen durch das Internet.

Grenzen des Informationssicherheitsrisikomanagements

Der Anwendungsbereich des Informationssicherheitsrisikomanagements beinhaltet die Prozesse mit den Assets, welche sich in den Prozessen beteiligten. In diesem Abschnitt sollen die Grenzen des Informationssicherheitsrisikomanagements festgelegt werden.

So wie jede Organisation verfügt die Hochschule über komplexe Prozesse. Manche von den komplexen Prozessen laufen außerhalb der Hochschule.

Da die Kontrolle und Überwachung der Prozesse, welche nicht intern laufen, schwierig sind, kann das Informationssicherheitsrisikomanagement für diese nicht durchgeführt werden. Deshalb gehören alle außerhalb durchgeführten Prozesse zu den Grenzen des Informationssicherheitsrisikomanagements.

3.1.2 Rollen und Verantwortlichkeiten

In diesem Abschnitt müssen die Organisation und die Zuständigkeiten für den Informationssicherheitsrisikomanagementprozess eingerichtet und gepflegt werden. Je nach Größe, Struktur und Schutzzielen der Organisation von Hochschulen kann sich die Informationssicherheitsorganisation unterscheiden.

Der Umfang der Risikoanalyse ist von der Anzahl der Mitarbeiter in einem Team abhängig. Aus diesem Grund muss man sich nur auf die kritischen, wichtigsten Prozesse und Werte konzentrieren, um den Risikomanagementprozess erfolgreich abzuschließen.

Die dafür spezialisierten Teams werden von der Organisationsleitung ausgewählt und die klaren Aufgaben der Teammitglieder definiert.

Bei der Festlegung der Rollen und Verantwortlichkeiten müssen nach der ISO/IEC 27005:2011 folgende Punkte berücksichtigt werden:

- Informationssicherheitsrisikomanagementprozess entwickeln
- Stakeholder identifizieren und analysieren
- Rollen und Verantwortlichkeiten der internen und externen Parteien der Organisation definieren

- Entscheidungs-Eskalationspfade definieren
- Aufzubewahrende Aufzeichnungen angeben
- Erforderliche Beziehungen zwischen der Organisation und den Interessengruppen sowie Schnittstellen zu den hochrangigen Risikomanagementfunktionen der Organisation festlegen

Unten werden die möglichen Rollen und Verantwortlichkeiten an den Hochschulen beschrieben und aus diesen Mitgliedern kann das Team gebildet werden. (Sicherheitskonzept und Sicherheitsmaßnahmen zur Informationssicherheitsorganisation an der Hochschule Augsburg, 2018):

Das Präsidium ist verantwortlich für die Informationssicherheit an den Hochschulen. Die Sicherheitsorganisation hilft dabei und übernimmt die Aufgaben des Informationssicherheitsmanagementsystems.

Eine wichtige Voraussetzung für die Durchführung der Risikoanalyse ist die Unterstützung der Hochschulleitung. Ohne Zusicherung von Ressourcen und ohne die Bereitschaft der Mitarbeiter, das Informationsrisikomanagementteam zu unterstützen, wird das Ergebnis nicht effektiv und effizient sein.

Zu den Führungskräften gehören die Leiter der Fakultäten und wissenschaftlicher und sonstiger Einrichtungen.

Informationssicherheitsbeauftragter der Hochschule

Der Informationssicherheitsbeauftragter zählt zu den von der Hochschule schriftlich bestellten Personen, die die Hochschule, die Vorstände, die Führungskräfte und die Fachkräfte für Arbeitssicherheit unterstützen. Zu seinen oder ihren Aufgaben gehören:

- Unterstützen bei der Erkennung, Behandlung und Beseitigung von möglichen Gefährdungen des Sicherheitskonzepts
- Erstellung, Pflege und Kontrolle eines Sicherheitskonzepts
- Erstellen der Sicherheitsanforderungen
- Steigern des Mitarbeiterbewusstseins
- Ansprechpartner für Fragen zur Informationssicherheit
- Planung und Koordination von Schulungs- und Informationsmaßnahmen,
- Beschreibung eines IT-Sicherheitskonzepts für den laufenden Betrieb
- Erstellung von Informationssicherheitsberichten für den IT-Arbeitskreis
- Einsatzplanung der für die IT-Sicherheit zur Verfügung stehenden Ressourcen
- Absprache mit dem Notfallteam des Präsidiums zur Ergreifung von fachlichen Gegenmaßnahmen

Datenschutzbeauftragter

Die Arbeit der Datenschutzbeauftragten können entweder Mitarbeiter der Hochschulen oder externe Datenschutzbeauftragte übernehmen. Ein Datenschutzbeauftragter überwacht die Einhaltung des Datenschutzes in der Hochschule. Seine wichtigsten Aufgaben sind die Kontrolle und Überwachung der ordnungsmäßigen Anwendung von Datenverarbeitungsprogrammen. Die mit den personenbezogenen Daten beschäftigten Mitarbeiter müssen die Datenschutzgesetze kennen und mit ihrer Umsetzung vertraut sein.

Die Anforderung für den behördlichen Datenschutzbeauftragten ist die Einhaltung des Bayerischen Datenschutzgesetzes (BayDSG) und anderer Vorschriften über den Datenschutz an der jeweiligen Hochschule. Er ist die Kontaktperson in Angelegenheiten des Datenschutzes an der Hochschule.

Rechenzentrum

Die Mitarbeiter des Rechenzentrums der Hochschule arbeiten eng mit dem Informationssicherheitsteam zusammen und unterstützen das Sicherheitskonzept bis hin zur Umsetzung der Risikomanagementmaßnahmen. Die Ausgabe der Karten (Campus Card Augsburg), die Verwaltung der Zutrittsrechte und Einrichtung und Betrieb der Videoüberwachung (CCTV) zählen zu den Aufgaben des Rechenzentrums.

Fakultäten

Die Führungskräfte der Fakultäten unterstützen die Teammitglieder des Risikomanagements, falls es nötig ist. Die Fakultäten können Zutrittsrechte für ihre gesicherten Bereiche, wie zum Beispiel die Campus Card vergeben. Die Erstellung der Karten übernimmt das Rechenzentrum.

Notfallmanagement

In den Notsituationen ist ein schneller, effektiver Umgang mit IT-Sicherheitsvorfällen wichtig. Dies ist eine der Anforderungen an ein Top-Management. Die Referentin oder der Referentin des Präsidiums koordiniert das Notfallmanagement an der Hochschule und arbeitet mit dem Informationssicherheitsteam zusammen.

Die Dokumentation bei der Risikoanalyse ist sehr wichtig. Alle Schritte müssen sauber dokumentiert werden. Diese Dokumentation wird zukünftig bei einer neuen Risikoanalyse immer benötigt, um die umgesetzten Maßnahmen nachvollziehen und die Risikoanalyse schnell durchführen zu können.

In dieser Tabelle 8 sind die Teammitglieder und der ausgewählte Geschäftsbereich zur Risikoanalyse kurz zusammengefasst. Die Tabelle beinhaltet fiktive Informationen.

Tabelle 8: Mögliche Formulare für Rollen und Verantwortlichkeiten (Quelle: F. Djumayev)

Mitglieder des Analyseteams		Angaben des (kleinen) Kernteams und der Personen, die das Team temporär unterstützen	
Kernmitglieder des Analyseteams		Zusätzliche Mitglieder	
Name	Rollen	Name	Fähigkeiten
Geschäftsbereiche: Studienverwaltung			
Fr. Richter	Fakultät Informatik		
Hr. Müller	Personalabteilung		
IT-Abteilung:			
Hr. Großer	Leiter IT Services	Hr. Klein	N-Solution GmbH
Hr. Gimpel	IT-SecBe		

3.1.3 Basiskriterien

Nach der Feststellung des Fachkontextes wird im nächsten Kapitel das Risiko-Assessment durchgeführt, wofür die Basiskriterien für das Risiko-Assessment erforderlich sind. Zu den Basiskriterien zählen die Kriterien für das Erreichen des Risikomanagements, Kriterien für die Risikobeurteilung, Auswirkungskriterien und Risikoakzeptanzkriterien.

Die grundlegenden Bedrohungen für die Hochschulen werden von der ISO/IEC 27005 im Annex C berücksichtigt. Die Bedrohungen sind folgendermaßen gegliedert:

1. Physische Schäden
2. Naturereignisse
3. Ausfall der wesentlichen Services
4. Beeinträchtigung durch Strahlung
5. Gefährdung von Informationen
6. Technisches Versagen
7. Unberechtigte Aktionen
8. Beeinträchtigung der Funktionen
9. Mensch

Die oben genannten Gruppen der Bedrohungen (1-9) dienen als Grundlage zur Klassifizierung der Bedrohungen. Die für die Hochschule relevanten Bedrohungen werden

in den nächsten Kapiteln detaillierter untersucht, den einzelnen Gruppen zugeordnet und bei der Risikobewertung betrachtet.

Aus den Bedrohungen, Schwachstellen und Verwundbarkeiten ergibt sich die Eintrittswahrscheinlichkeit der negativen Ereignisse. Die Eintrittswahrscheinlichkeit wird auf diese Weise klassifiziert:

Tabelle 9: Eintrittswahrscheinlichkeit der negativen Ereignisse (Quelle: F. Djumayev)

Typ	Eintrittswahrscheinlichkeit	Beschreibung
1	Unwahrscheinlich	Der Eintritt der negativen Ereignisse ist eher unwahrscheinlich. Der Angreifer kann keine oder kaum Schwachstellen finden, um sie auszunutzen. Die möglichen Schwachstellen werden durch die regelmäßige Kontrolle entdeckt und sofort behoben.
2	Möglich	Der Eintritt der negativen Ereignisse kann einmal im Jahr vorkommen. Dabei soll der Angreifer über Expertenwissen verfügen, um eine Schwachstelle ausnutzen zu können. Die entdeckten Schwachstellen werden schnell behoben.
3	Wahrscheinlich	Die negativen Ereignisse können mehrmals im Jahr vorkommen. Die zur Verfügung gestellte Patches des Herstellers sind nicht fähig, die entdeckten Schwachstellen vollständig zu beheben. Die Angriffspunkte sind im Internet veröffentlicht und können ausgenutzt werden.
4	Sehr wahrscheinlich	Die Eintrittshäufigkeit der negativen Ereignisse kann einmal im Monat oder öfters sein. Die entdeckten Schwachstellen werden sofort ausgenutzt (0-day exploits). Die Kontrollen sind nicht fähig, die Schwachstellen zu finden und sie zu beheben.

Auswirkungskriterien

Unter dem Begriff Schaden wird das negative Ergebnis eines Ereignisses verstanden. Die Auswirkung bedeutet hier die Einschätzung der von den unmittelbaren Schäden verursachten Beschädigungen. Durch die Auswirkungskriterien werden die Höhe eines Schadens sowie die damit verbundenen Kosten und der Imageschaden der jeweiligen Organisation bewertet. Unten werden in Tabelle 10 die Auswirkungskriterien klassifiziert und kurze Beschreibungen hinzugefügt.

Tabelle 10: Schadenauswirkung (Quelle: F. Djumayev)

Typ	Auswirkung	Beschreibung

1	Unbedeutend	Kosten unter 5000 EUR, keine negative Reputation, Betriebsunterbrechung, Verletzung der Schutzziele oder Verlust unwichtiger Daten
2	Begrenzt	Kosten unter 20.000 EUR, kaum Reputationsschaden, kurze Betriebsunterbrechung (< 3 Tage), Verluste einzelner Datensätze oder interner Informationen
3	Kritisch	Kosten über 20.000 EUR, negative Artikel in Lokalnachrichten, Betriebsunterbrechungen < 3 Tage, Verlust von Informationen, Projektkrise
4	Katastrophal	Verlust der Projektmittel, bayernweite Schlagzeilen, Unterbrechungen > Tag, Verlust streng vertraulicher Informationen, Projektabbruch

Risikoakzeptanzkriterien

Die Risikoakzeptanzkriterien sind wie folgt definiert:

- 1-4 Risiko ist akzeptiert
- 5-9 Risiko ist unter bestimmten Bedingungen akzeptiert
- > 9 Risiko ist nicht akzeptiert

Anhand der festgelegten Kriterien ergibt sich für die Hochschule folgende Risikomatrix-Tabelle:

Tabelle 11: Risikomatrix (Quelle: F. Djumayev)

Auswirkung / Eintritts-wahrscheinlichkeit	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

3.2 Risiko-Assessment

Das Ziel dieses Kapitels ist es, die bewerteten Risiken nach Risikobewertungskriterien an der Hochschule herauszufinden und zu priorisieren. Die kritischen, wichtigsten Risiken werden in den nächsten Kapiteln weiter analysiert und behandelt.

Nach der Festlegung des Kontextes (Anwendungsbereich und Grenzen, Rollen, Verantwortlichkeiten und Basiskriterien) besteht die Möglichkeit, diesen Schritt des Risiko-Assessments durchzuführen.

Ein Risiko ist eine Kombination von Eintrittswahrscheinlichkeit eines negativen Ereignisses und der Schadenauswirkung. Um die bewerteten Risiken herauszufinden, müssen die

Risiken in der Organisation identifiziert, quantifiziert oder quantitativ beschrieben werden. Die ernsthaften Risiken müssen nach den Basiskriterien priorisiert werden.

Das Risiko-Assessment wird oft in mehreren Iterationen durchgeführt, um zuerst die potenziellen Risiken zu identifizieren. Wenn es keine ausreichenden Informationen gibt, um die Risiken zu bewerten, werden weitere detaillierte Analysen und andere Methoden benötigt (ISO/IEC 27005).

3.2.1 Risikoidentifikation

Die Risikoidentifikation beantwortet die Frage, was die Ursache eines Verlustes ist und wo, wie und warum der Verlust an der Hochschule eintreten könnte? Anhand der Schritte der Risikoidentifikation werden Eingabedaten für die Risikoanalyseaktivität gesammelt.

Die Identifikation der Assets und Prozesse wurden im Abschnitt (3.1.1.1 Anwendungsbereiche und Grenzen) beschrieben.

3.2.1.1 Identifikation von Bedrohungen

Die wesentliche Aufgabe dieses Abschnittes ist die Identifizierung der Bedrohungen für die einzelnen Asset-Typen. Die Identifikation der Bedrohungen basiert auf den Informationen der Asset-Identifizierung, welche im vorherigen Abschnitt 3.1.1 dargestellt sind.

Außerdem lehnt sich die Identifikation der Bedrohungen an die ISO/IEC-Vorgaben wie Annex C an. Im Annex C sind die möglichen Bedrohungen nach Typ und Herkunft aufgelistet. (International Standard, ISO/IEC 27005:2011(E))

Zu den Bedrohungstypen zählen:

- Physische Schäden
- Naturereignisse
- Verlust von wesentlichen Dienstleistungen
- Störung durch Strahlung
- Beeinträchtigung der Informationen
- Technisches Versagen / Technische Fehler
- Unautorisierte Aktionen
- Beeinträchtigung bei den Funktionen

Nach ihrer Herkunft werden die Bedrohungen in drei unterschiedlichen Gruppen gegliedert.

- D (deliberate) – beabsichtigte Aktionen
- A (accidental) – zufällige, nicht geplante Aktionen

- E (environmental) – naturbedingte Aktionen

Im Folgenden werden die möglichen Bedrohungen nach Asset-Typ beschrieben und in der Tabelle 12 zusammengefasst. Die Information über die Assets sind bereits im Anschnitt 3.1.1 dargestellt.

Bedrohungen für Hardware

Manipulation der Hardware / Ausführung der Schadsoftware

Das UEFI beschreibt eine Schnittstelle zwischen der Firmware und den einzelnen Komponenten sowie des Betriebssystems des Computers. Mithilfe dieser Schnittstelle können das Betriebssystem und die Rechnerkomponenten mit einer Hardware kommunizieren. Es ersetzt das BIOS, welches für die Eingabe- und Ausgabeaufgaben zuständig war.

Im Vergleich zum alten BIOS ermöglicht das UEFI die Benutzung der Netzwerkkarten bereits vor dem Start des Betriebssystems. Es gehört zwar zu einer guten Funktion, aber kann zu großen Problemen führen.

Durch die Ausnutzung der UEFI-Netzwerkunterstützung können die Netzwerkressourcen dem Angreifer gesendet werden, was die Manipulation des Rechners oder Ausführung der Schadsoftware auf dem Rechner begünstigt. Dabei braucht der Nutzer des Rechners nicht einmal das Betriebssystem starten und im Internet surfen. (IP Insider, 2018)

Infizierung der Hardware durch die Schädlinge

Die bekannteste und sehr gefährliche Bedrohung ist die Infizierung der Hardware durch die Verwendung des USB-Interfaces. Wie bereits von vielen Berichten bekannt ist, haben Apple MacBooks und Google Pixel Laptops einen Typ C Anschluss umgesetzt.

Ein Type C Anschluss bietet die Möglichkeit, Aufladekabel oder USB-Sticks sowohl mit der oberen als auch mit der unteren Seite in den Laptop stecken zu können. Es gibt keine falsche Seite.

Der universelle USB-Anschluss von Apple und Google dient unter anderem für die Stromversorgung. An sich ist der Typ C Anschluss eine einfache und schnelle Funktion, hat jedoch seine Nachteile.

Er bietet die Möglichkeit, die schädlichen Codes in die USB-Controller zu injizieren. Firmwareattacken und Zugriffe auf den Speicher sind die möglichen Angriffsszenarien. Da das Aufladen durch den universellen Anschluss erfolgt, bereitet dies große Sorgen bezüglich

der Sicherheit. Ein durch die Schadsoftware injiziertes Ladegerät kann dem Angreifer helfen, das jeweilige Gerät vollständig zu übernehmen. (The Verge, 2018)

Unberechtigte Nutzung des Geräts

In diesem Abschnitt wird die Verschlüsselungsmöglichkeit einer Hardware betrachtet. In unserem Beispiel ist es der Laptop von Apple. Es ist zu beachten, dass alle Informationen in dieser Arbeit nur für Lernzwecke verwendet werden. Sie dienen lediglich der ausführlichen Darstellung des komplexen Informationssicherheitsrisikomanagements.

Die Verschlüsselung eines Rechners erfolgt wie üblich über die Verschlüsselung der Festplatte. Diese wird benutzt, um die ausgetauschten Signale in Echtzeit zu verschlüsseln.

Apple bietet die FileVault-Funktion, damit die Festplatte verschlüsselt werden kann. Diese Funktion kann unter den Einstellungen eines Geräts aktiviert werden. Der Zugang zu der verschlüsselten Festplatte bzw. zu den Informationen auf der Festplatte erfolgt nur über das Passwort.

Die FileVault-Verschlüsselungsmöglichkeit bietet mehr Sicherheit, jedoch hat die Funktion ihre Schwäche. FileVault ermöglicht keinen vollständigen Schutz gegen Brute-Force-Attacken. Eine Brute-Force-Attacke bezeichnet eine Angriffsart, bei der ein Hacker durch mehrmaliges Versuchen das Passwort herausfindet. Dabei kann er eine Software verwenden, welche alle möglichen Passwortkombinationen ausprobiert, um das richtige Passwort zu knacken.

Bei einem schwachen Passwort mit sechs Zeichen braucht ein Angreifer dazu nur fünf Stunden Zeit, wohingegen er für das Herausfinden der komplizierten Passwörter mehrere Jahre benötigt.

Aus diesem Grund ist es sehr wichtig, starke Passwörter zu benutzen. (McWelt, 2018)

Bedrohungen für Software

Manipulation der Software

Unter Botnetz wird die Fernsteuerung der zusammengeschlossenen Rechner verstanden. Öfters werden die Schwachstellen der Betriebssysteme und Android-Geräte ausgenutzt. Dabei können die Angreifer durch sogenannte DDoS-Angriffe Internetseiten lahmlegen oder SPAM-Mails unerkannt versenden. (BSI-Standard 200-3, Finale Version 15.11.2017)

Mögliche Maßnahmen gegen Botnetz-Angriffe:

1. Bereitgestellte Sicherheitsupdates installieren (Beispiel Internetbrowser, Office, Flash Player, Adobe Reader)
2. Virenschutzprogramm benutzen
3. Firewall-Sicherheitssystem benutzen, um Netzwerk besser zu kontrollieren
4. Benutzerkonto mit eingeschränkten Rechten
5. Sichere Passwörter und diese alle drei Monate ändern
6. Erstellung von Sicherheitskopien/Backups
7. Sichere Verbindung wie HTTPS//:
8. Sicherheitsstatus der Computer checken
9. Sichere WLAN-Verbindung, Verschlüsselung mit Verschlüsselungstandard WPA2

Anfälligkeit der Funktion des Windows Object Linking und Embedding (Windows OLE)

Objekt Linking and Embedding (Objekt-Verknüpfung und -Einbettung) ist ein Objektsystem und Protokoll, das von Microsoft entwickelt wurde. Das ermöglicht die Zusammenarbeit unterschiedlicher Applikationen und die Erstellung heterogener Verbunddokumente.

Die Angreifer haben zahlreiche E-Mails an Internetnutzer im August 2018 gesendet. Wenn die Internetnutzer das angehängte Dokument mit dem Office-Software oder mit dem Texteditor öffnen, könnte die dann gefährlich werden. Das könnte die Manipulation des Rechners führen.

Microsoft schlägt vor, schnell wie möglich neue Update zu installieren. Microsoft empfehlt die Daten aus vertraulichem Ort zu öffnen, sonst lieber den Geschützten Ansicht von Word nicht deaktivieren. (Manager Magazin, 2017)

Missbrauch der Rechte

Damit die Authentisierungsmechanismen richtig funktionieren, wird von den Mitarbeitern verlangt, dass sie sorgfältig mit den Passwörtern umgehen.

Häufig werden in einer Arbeitsgruppe gleiche Passwörter für die Anwendungen und Systeme benutzt, oder aus Bequemlichkeit werden die Standardpasswörter sowie Trivialpasswörter nicht geändert, obwohl viele wissen, dass dies ein hohes Sicherheitsrisiko ist. Manchmal ist es der Fall, dass der Benutzer sein Passwort unter die Tastatur oder als Klebezettel auf den Arbeitsplatz geklebt hat, welches das absolute No-Go ist.

Daher ist eine Regelung für den Umgang mit Passwörtern an der Hochschule notwendig. (Bundesamt für Sicherheit in der Informationstechnik, 2018)

Bedrohung für Daten

Daten bedeuten sehr viel für jede Organisation. In der Hochschule Augsburg werden während des Ablaufs von Prozessen Daten produziert, empfangen, gespeichert und bearbeitet.

Datenverlust

Der Verlust oder die Manipulation der Daten kann durch die Ausnutzung von Schwachstellen in Soft- oder Hardware oder das nicht vorhandene Informationssicherheits-bewusstsein der Personen, die mit den Daten arbeiten, vorkommen.

In diesem Abschnitt werden die häufigsten Ursachen für den Datenverlust und die Datenmanipulation beschrieben.

Ohne die benötigten Daten ist der Anwender machtlos. Jedoch kann eine einzige falsche Aktion des Benutzers den Datenverlust verursachen. Das bekannteste Beispiel dafür ist das schnelle Herausziehen eines USB-Sticks. Der USB-Stick wird schnell mit einem Laptop oder anderem Gerät verbunden; genauso schnell kann es wieder vom Gerät herausgezogen werden. Durch diese Aktion kann der Benutzer es verursachen, dass die Datenübertragung nicht vollständig abgeschlossen ist. Infolgedessen werden die Daten zerstört und sind nicht mehr benutzbar.

Ein anderes Beispiel für Benutzeraktionen, welche Datenverlust verursachen können, ist die Unaufmerksamkeit bezüglich Wasser am Schreibtisch, wo der Rechner steht, oder die Benutzung nicht wasserfester Laptoptaschen.

Neben dem Wasser kann eisige Kälte es begünstigen, dass die Daten auf dem Rechner verloren gehen. Laut Experten soll man dem Rechner genug Zeit für die Anpassung an die Zimmertemperatur lassen, wenn er lange Zeit in einer großen Kälte gewesen war.

Datenmanipulation bedeutet die Durchführung aller Prozesse zum Löschen der alten und Hinzufügen der neuen Daten.

Bedrohungen für Infrastruktur

Feuer

Der Diebstahl von Geräten, Datenträgern und Dokumenten ist eine weitere Bedrohung für die Hochschulen. Durch Diebstahl kommen hohe finanzielle Schäden für die Wiederbeschaffung sowie Wiederherstellung von Datenträgern und IT-Systemen zustande. Falls die gestohlenen Informationen sowie Studenten- und Mitarbeiterdaten, Prüfungs- und

Forschungsergebnisse offengelegt werden, könnte dies weiteren Schaden für die Hochschule bringen.

Durch den Mangel an etablierter Überwachung und Sicherheitsmaßnahmen gegen Diebstahl kann diese Bedrohung den Hochschulen sehr schaden.

Das Verschließen von Rechnergehäusen oder Schnittstellenanschlüssen könnte zum Schutz einzelner Systeme, Desktoprechner und Laptops dienen.

Wenn es um die IT-Infrastruktur sowie das Rechenzentrum der Hochschulen geht, könnte die Zutrittskontrolle mit elektronischem Zutrittscode, Magnetkarten oder biometrischen Daten helfen. (Sucurity Insider, 2018)

Diebstahl von Medien und Dokumenten

Der Diebstahl von Geräten, Datenträgern und Dokumenten ist eine weitere Bedrohung für die Hochschulen. Durch Diebstahl kommen hohe finanzielle Schäden für die Wiederbeschaffung sowie Wiederherstellung von Datenträgern und IT-Systemen zustande. Falls die gestohlenen Informationen sowie Studenten- und Mitarbeiterdaten, Prüfungs- und Forschungsergebnisse offengelegt werden, könnte dies weiteren Schaden für die Hochschule bringen.

Durch den Mangel an etablierter Überwachung und Sicherheitsmaßnahmen gegen Diebstahl kann diese Bedrohung den Hochschulen sehr schaden.

Das Verschließen von Rechnergehäusen oder Schnittstellenanschlüssen könnte zum Schutz einzelner Systeme, Desktoprechner und Laptops dienen.

Wenn es um die IT-Infrastruktur sowie das Rechenzentrum der Hochschulen geht, könnte die Zutrittskontrolle mit elektronischem Zutrittscode, Magnetkarten oder biometrischen Daten helfen. (Security Insider, 2018)

Wasserschäden

Eine weitere Bedrohung sind Wasserschäden, was bei der Planung der Räumlichkeiten beachtet werden muss. Wasserschäden können dazu führen, dass die gesamte IT schnell ausfällt.

Wassereinbrüche sind häufig die Ursache für das Eintreten dieser Bedrohung.

Neben der sicheren Planung der Räumlichkeiten des Rechenzentrums zählen die Auffangwannen und Gefahrenmeldeanlagen mit Feuchtigkeitssensoren zu den geeigneten Sicherheitsmaßnahmen.

Personalbezogene Bedrohungen

Personalausfall

Ein Geschäftsprozess besteht aus mehreren Aufgaben und Arbeitsabläufen, um ein bestimmtes geschäftliches Ziel zu erreichen. Der Ausfall von Personal kann sich negativ auf die Geschäftsprozesse der Hochschulen auswirken.

Gründe für den Personalausfall können Krankheit, Unfall, Tod oder Streik sein. Außerdem gibt es vorhersehbare Personalausfälle wie zum Beispiel Urlaub, Weiterbildung und weitere Bedingungen, was im Arbeitsvertrag drinsteht.

Als mögliche Maßnahme gegen den Ausfall von Personal gelten Vertretungsregelungen. Dies ermöglicht nicht nur, vorhersehbare, sondern auch unvorhersehbare Fälle des Personalausfalls zu regeln. Im Bereich der Informationsverarbeitung ist das sehr bedeutend, weil hier von dem Mitarbeiter spezielles Wissen gefordert ist. Noch eine weitere Möglichkeit ist es, externe Fachkräfte mit der Abstimmung des Managements zu beauftragen. Das könnte wiederum höhere Kosten verursachen. (BSI-Standard 200-3, Finale Version 15.11.2017)

Nichtbeachtung von Sicherheitsmaßnahmen

Es kommt häufig vor, dass Schäden aus einem mangelnden Sicherheitsbewusstsein der Mitarbeiter entstehen. Nachlässigkeit und fehlende Kontrollen sind der Grund, warum die Mitarbeiter Sicherheitsmaßnahmen nicht berücksichtigen.

Maßnahmen

Regelmäßig durchgeführte Schulungen können das Sicherheitsbewusstsein der Mitarbeiter vertiefen, weil jeder Mitarbeiter grundsätzlich ein unterschiedliches Verständnis über die Sicherheitsmaßnahmen hat. Einige Beispiele von Sicherheitsmaßnahmen:

- Sicherer Schutz von Dokumenten, USB-Sticks oder anderen Informationsträgern, indem die Mitarbeiter den eigenen Schreibtisch abschließen
- Zutrittskontrolle beim Eintritt zu einem Rechenzentrum (durch einen Chipkartenleser, PIN-Eingabe oder biometrische Verfahren)
- Keine fremden USB-Geräte an die IT-Infrastruktur mitbringen und anschließen
- Auf die SPAM-Mails aufpassen und sofort dem Sicherheitsmitarbeiter Bescheid geben
- Korruptionsverbot, Verbot der Geldwäsche und Terrorismusfinanzierung etc.

Jeder Mitarbeiter muss dahingehend geschult werden und dazu seine gesellschaftliche Verantwortung übernehmen. (BSI-Standard 200-3, Finale Version 15.11.2017)

Social Engineering

In der letzten Zeit kommt die Bedrohung des Social Engineering immer häufiger vor. Durch Social Engineering möchte der Angreifer den unberechtigten Zugang zu Informationen oder IT-Systemen erhalten.

Beim Social Engineering wird die Schwäche des Menschen ausgenutzt. Es gibt viele Fälle, welche es in vielen Unternehmen gegeben sind. Eine weitere Strategie des Social Engineering ist, über längere Zeit eine Beziehung zum Opfer aufzubauen.

Jeder Mitarbeiter muss darüber Bescheid wissen, welche Tricks die Angreifer beim Social Engineering verwenden. Bei einem Verdacht müssen die Mitarbeiter umgehend mit dem IT-Sicherheitsmitarbeiter eKontakt aufnehmen. Regelmäßige Schulungen der Mitarbeiter und die Zusammenarbeit mit dem IT-Mitarbeiter zeigen sich hierbei als erfolgreich. (BSI-Standard 200-3, Finale Version 15.11.2017)

Bedrohungen für zentrale Dienste

Ausspähen der Informationen/Fernspionage

In diesem Abschnitt wird zuerst die WLAN-Verbindung an der Hochschule Augsburg nach möglichen Bedrohungen untersucht. Sowie viele andere Hochschulen und Universitäten in Deutschland verwendet die Hochschule Augsburg die eduroam-WLAN-Verbindung.

Das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften hat die Sicherheitshinweise für eduroam beschrieben. Laut dem Leibniz-Rechenzentrum ist die eduroam-WLAN-Verbindung mit der WPA2-Verschlüsselung gesichert. (Leibniz-Rechenzentrum, 2016).

WPA2 soll sicherstellen, dass nur berechtigte Benutzer durch die Eingabe des Passworts den Zugriff auf das Netzwerk haben und die übertragenen Daten von Unbefugten nicht abgehört werden.

WPA2 galt als sicherste Verschlüsselungsmethode im Vergleich zu den alten Verschlüsselungsverfahren wie WPA und WEP. Nach den Angaben von Telekom im Jahr 2017 haben Forscher eine Sicherheitslücke bei der WPA2-Verschlüsselungsmethode entdeckt.

Die gefundene Sicherheitslücke ermöglicht dem Angreifer, die Informationen aus der Ferne auszuspionieren und diese sogar zu manipulieren, welche über den WLAN-Netzwerk gesendet und empfangen werden.

Nach den Angaben der Forscher liegt der Fehler bei der Kommunikation zwischen dem Sender und Empfänger. Das Passwort wird beim Kommunizieren drei Mal verschickt, was einen Angriff begünstigt.

Die WPA2-Sicherheitslücke kann mit der Passwortänderung nicht verhindert werden. Es hilft nur, die Updates zu installieren. Der Sicherheitsbeauftragter der Hochschule Augsburg soll dafür alle wichtigen Informationen zu dem vorhandenen Netzwerk definieren und anhand dieser kann er herausfinden, ob die aktuelle Version von Sicherheitsupdates für das Netzwerk bereits installiert wurde und die Fehler im Netzwerk vollständig behoben sind. (T - Online, 2017).

Stromausfall

Nicht nur die Hochschulen, sondern alle Unternehmen sind stark von der Stromversorgung abhängig. PCs, Aufzüge, automatische Türschließanlagen, Klimatechnik, Wasserversorgung, Beleuchtung, Rechenzentrum und viele andere Infrastruktureinrichtungen würden ohne Strom nicht funktionieren.

Trotz der gegenwärtigen Versorgungssicherheit sowie Verteilungsnetzanbieter und Energieversorgungsunternehmen gibt es häufige Stromunterbrechungen. Unterbrechungen von mehr als 10 Millisekunden könnten schon den IT-Betrieb stören. Bei Bauarbeiten sowie anderen nicht angekündigten Arbeiten könnte es zu Kabelbeschädigungen oder zum Ausfall der Stromversorgung im Versorgungsnetz kommen. (BSI-Standard 200-3, Finale Version 15.11.2017)

Vorbeugende Maßnahmen gegen Stromausfall sind zum Beispiel ein Reservenetzanschluss aus dem öffentlichen Stromnetz, ein Notstromdieselaggregat und Strom aus einem benachbarten Kraftwerk. (Bundesamt für kerntechnische Entsorgungssicherheit, 2018)

In der Arbeit wird davon ausgegangen, dass die Hochschule keine sichere Stromversorgung hat.

Lauschen

Mit dem Aufräumen des Posteingangs beginnt morgens meistens der Arbeitstag. Tagsüber werden viele E-Mails getauscht. Wenn es um die Sicherheit geht, kommt die Frage, ob der E-Mail-Versand eine vertrauliche Kommunikation ist?

Nach vielen Medienberichten ist der E-Mail-Versand nicht mehr sicher und die Sicherheitsexperten schlagen vor, dass nur noch verschlüsselte E-Mails getauscht werden

sollten. Besonders die vertraulichen Informationen/Daten sowie Studenten-, Personaldaten, Prüfungs- und Forschungsergebnisse an der Hochschule sollten nur noch verschlüsselt gesendet werden. Ein Beispiel: Laut Bundeskriminalamt wurde eine Sammlung von ca. 500.000.000 Zugangsdaten sowie E-Mail-Adressen und den dazugehörigen Passwörtern in einer Underground-Economy-Plattform ausgespäht. (Bayern Radio, 2017)

Die Verwendung sicherer Kennwörter, rechtzeitiges Blockieren von Spam-Mails, die Schulung der Mitarbeiter, Abwehr von Phishing-Angriffen und Überwachung und Filterung von E-Mail-Inhalten sowie die E-Mail-Verschlüsselung sind geeignete Maßnahmen für sichere Kommunikation.

Tabelle 12: Mögliche Bedrohungen bei Assets (Quelle: F. Djumayev)

Asset-Typ	ID der Bedrohung	Bedrohungsart	Bedrohungen	Ursache
Hardware	HWB-1	Beeinträchtigung der Informationen	Injizierung der Hardware durch die Schadsoftware	D
	HWB-2	Beeinträchtigung der Informationen	Manipulation der Hardware/Ausführung der Schadsoftware	D
	HWB-3	Unautorisierte Aktionen	Unberechtigte Nutzung des Geräts	D
Software/Systeme	SWB-1	Beeinträchtigung der Information	Manipulation der Software	D
	SWB-2	Beeinträchtigung der Information	Manipulation der Software	D
	SWB-3	Beeinträchtigung der Information	Manipulation der Software	D
Infrastruktur	IB-1	Physische Schäden	Feuer	A
	IB-2	Beeinträchtigung der Information	Diebstahl von Medien und Dokumenten	D
	IB-3	Verlust von wesentlichen Dienstleistungen	Wasserschäden	A, D, E
Personen	PB-1	Personal	Personalausfall	A, D
	PB-2	Personal	Nichtbeachtung von Sicherheitsmaßnahmen	A, D
	PB-3	Personal	Social Engineering	D

Netzwerk	BN-01	Beeinträchtigung der Informationen	Ausspähen der Informationen/Fernspionage	D
	BN-02	Verlust von wesentlichen Dienstleistungen	Stromausfall	A, D, E
	BN-03	Beeinträchtigung der Informationen	Lauschen	D

3.2.1.2 Identifikation bestehender Maßnahmen

Um doppelte Arbeit beim Risikomanagement zu vermeiden, muss der Schritt der Identifikation bestehender und bereits umgesetzter Maßnahmen überprüft werden. Besonders wichtig ist es, ob die umgesetzten Maßnahmen ordnungsgemäß funktionieren. Durch das Anschauen der ISMS-Prüfberichte könnten Zeitaufwand und die Aufgaben verringert werden. Wenn die umgesetzten Maßnahmen nicht ordnungsmäßig wirken und funktionieren, kann dies zu Sicherheitslücken führen. Um das festgelegte Risiko zu minimieren, muss man andere ergänzende Maßnahmen einsetzen.

Ob sich die Auswirkungen des Vorfalls und die Bedrohungswahrscheinlichkeit verringern, kann die Wirksamkeit der Maßnahmen festgestellt werden. Die Management-Reviews und Audit-Berichte geben die Möglichkeit, Informationen über die Wirksamkeit bestehender Maßnahmen zu verdeutlichen.

Die bestehenden und geplanten Maßnahmen könnte als effektiv, ineffektiv und nicht ausreichend identifiziert werden. Für die nicht ausreichenden Maßnahmen müssen gestrichen und durch andere effektive und effiziente Maßnahmen ersetzt werden.

Die Überprüfung der Dokumentation über das Informationssicherheitsrisikomanagement, die Überprüfung bei den für die Informationssicherheit verantwortlichen Personen und der beteiligten Personen bei der Umsetzung der Maßnahmen, die Vor-Ort-Überprüfung und die Überprüfung der Ergebnisse von Audits gehören zur Identifizierung bereits umgesetzter Maßnahmen.

3.2.1.3 Identifikation von Schwachstellen

In diesem Abschnitt wird versucht, die möglichen Schäden oder Konsequenzen für die Hochschulen durch ein mögliches Vorfallszenario zu identifizieren. Unter dem Begriff Vorfallszenario versteht man die Beschreibung einer Bedrohung, die eine bestimmte

Sicherheitslücke oder eine Reihe von Sicherheitslücken in einem Informationssicherheitsereignis ausnutzt (siehe ISO/IEC 27002: 2005, Klausel 13).

Ein Vorfallszenario kann sich auf ein oder mehrere Vermögenswerte auswirken. Eine Liste von Vorfallszenarien mit ihrer Auswirkung auf Assets und Geschäftsprozesse sind das Hauptthema dieses Abschnitts.

Tabelle 13: Schwachstellen Identifikation (Quelle: F. Djumayev)

Asset-Typ	Bed. ID	Bedrohungsart	Bedrohung	Ursache	Bestehende Maßnahmen	Schwachstellen/ Sicherheits-lücken
Hardware	HWB1	Beeinträchtigung der Informationen	Manipulation der Hardware	D	-	Einzelne USB-Anschlüsse fürs Aufladen und Daten
	HWB2	Beeinträchtigung der Informationen	Manipulation der Hardware	D	-	UEFI-Netzwerkkarten Unterstützung
	HWB3	Unautorisierte Aktionen	Unberechtigte Nutzung von Geräten	D	-	Schwache Passwörter
Software	SWB1	Beeinträchtigung der Informationen	Manipulation der Software (Botnetz)	D	Virenschutz-programme, Firewall, sichere WLAN-Verbindung mit Verschlüsselungsstandard mit WPA2 und sichere Internetverbindung https//:	Fehlende Sicherheitsupdates
	SWB2	Beeinträchtigung der Funktionen	Missbrauch der Rechte	D	-	Schlechte Passwort-verwaltung
	SWB3	Beeinträchtigung der Informationen	Manipulation der Software (Windows OLE)	D	-	Anfälligkeit der Funktion des Windows Object Linking und Embedding (Windows OLE)
Infrastruktur	IB1	Physische Schäden	Feuer	A	Blitzschutz	Mangel an formellen Richtlinien
	IB2	Beeinträchtigung der Informationen	Diebstahl von Medien und Dokumenten	D	Türsicherungen	Mangel an etablierter Überwachung
	IB3	Verlust von wesentlichen Dienstleistungen	Wasserschäden	A, D, E	-	Wasserschäden

Personen	PB1	Mensch	Personalausfall	A, D	-	Keine Vertretungs-regelung
	PB2	Mensch	Menschliche Fehlhandlung	A, D	-	Mangel an Sicherheits-bewusstsein
	PB3	Mensch	Social Engineering	D	-	Mensch
Netzwerk	NB1	Beeinträchtigung der Informationen	Ausspähen der Informationen/ Fernspionage	D	-	Fehler bei der Netzwerk-architektur
	NB2	Verlust von wesentlichen Dienstleistungen	Stromausfall	A, D, E	-	Instabiles Stromnetz
	NB3	Beeinträchtigung der Informationen	Lauschen	D	Zertifizierung CA	Ungeschützter vertraulicher Datenverkehr

3.2.1.4 Identifikation von Konsequenzen

Die Identifikation von Konsequenzen ist dafür da, um die Ursachen von Schaden und Konsequenzen für die Hochschule mithilfe eines Vorfallszenarios zu verdeutlichen.

Die Auswirkungen des Vorfallszenarios werden bestimmt, indem die definierten Auswirkungskriterien im Kontext berücksichtigt werden. An der Hochschule Augsburg wurde für das Vorfallszenario eine Belastbarkeitstabelle erstellt. Bei der Bestimmung der Belastbarkeitstabelle wurden die Konsequenzen des Vorfallszenarios berücksichtigt. (siehe Tabelle 14)

Tabelle 14: Belastbarkeitstabelle (Quelle: Hochschule Augsburg)

Beschreibung des Problems/Risiko	Level 1 nicht signifikant/wichtig	Level 2 ernst	Level 3 sehr ernst	Level 4 schwerwiegend, kritisch
Studentendaten über ihre Leistungen an der Hochschule oder weitere gespeicherte Unterlagen werden manipuliert (Noten, ECTS-Punkte, Zeugnisse)		Zulassungszeugnisse oder einzelne Noten sowie ECTS-Punkte werden manipuliert	Prüfungsergebnisse oder ECTS-Punkte werden mehrfach manipuliert	Abschlusszeugnisse oder Urkunden werden manipuliert oder vollständig nachgedruckt
Informationen über den Studienerfolg (Noten, Zeugnisse) werden unberechtigt veröffentlicht		Informationen über einen einzelnen nicht in der Öffentlichkeit bekannten Studenten werden veröffentlicht	Informationen über eine Gruppe unbekannter Absolventen werden veröffentlicht	Informationen über den Studienerfolg sind frei verfügbar. Informationen über einzelne oder mehrere prominente Personen sind verfügbar oder werden veröffentlicht
Direkter Verlust/Betrug/Strafen z. B. werden unberechtigte Zahlungen veranlasst	Bis 5.000 Euro	5.000 - 20.000 Euro	Verlust von Förderungen, systematischer Betrug disziplinarrechtliche Folgen für einzelne Mitarbeiter	Verlust von Drittmitteln oder Forschungsgeldern aus der Wirtschaft Disziplinarrechtliche Folgen für verantwortliche Mitarbeiter bzw. die Hochschulleitung

Informationen zu Studienzeiten oder Finanztransaktionen sind nicht verfügbar	Archivdaten einzelner Finanztransaktionen oder Studienabschlüsse und Zeugnisse sind nicht verfügbar	Archivdaten einzelner Finanztransaktionen oder Studienabschlüsse, Zeugnisse eines Jahrgangs (oder ähnlicher Umfang) sind nicht verfügbar	Es sind keine Archivdaten verfügbar bzw. Informationen müssen rekonstruiert wurden	
Personenbezogene Daten von Hochschulangehörigen oder vertrauliche Informationen der Hochschule werden veröffentlicht	Einzelne interne Dokumente mit Bezug zu Hochschulangehörigen werden veröffentlicht	Einzelne vertrauliche Informationen oder Kontaktinformationen zu Hochschulangehörigen werden veröffentlicht	Personenbezogene Daten (gemäß Art. 15 (7)) von Hochschulangehörigen oder große Datenmengen interner oder vertraulicher Informationen werden veröffentlicht	Personenbezogene Daten, die das Wohl von Hochschulangehörigen bedrohen, oder „geheime“ Informationen werden veröffentlicht
Verlust von Drittmitteln wegen Verletzung von Geheimhaltungsvereinbarungen		Interne Regelungen zum Schutz der Informationen im Bereich F&E werden verletzt, keine verwertbaren Daten dringen an die Öffentlichkeit	Vertragliche Vereinbarungen mit Partner zum Schutz der Informationen werden verletzt, Forschungsaufträge gehen verloren	Vertragliche Vereinbarungen mit Kunden zum Schutz der Informationen werden verletzt, Forschungsaufträge gehen verloren bzw. verwertbare Informationen gelangen an die Öffentlichkeit. Schadensersatzklagen gegen die HSA werden angezeigt
Missbrauch von Hochschulrechnern für Internetkriminalität	Ein infizierter Computer versendet SPAM-Mails	Mehrere Rechner aus dem Hochschulnetz beteiligen sich an Attacken gegen Internethosts (Bots)	Teilweiser Verlust der Kontrolle über Rechner der Hochschule, Teilnetze müssen abgeschaltet werden	Abschaltung des Hochschulnetzes wegen krimineller Beteiligung auf Anordnung der Exekutive
Ausfall der IT-Infrastruktur wegen eines Stromausfalls in den Hochschulgebäuden	Ausfall < 4 Std.	>= 4 Std. bis < 24 Std.	>= 24 Std. bis < 4 Tage	> 4 Tage

3.2.2 Risikoanalyse

Anhand der ISO/IEC 27005 kann die Risikoanalyse je nach der Kritikalität der Assets, dem Ausmaß der bekannten Sicherheitslücken und früheren Vorfällen in unterschiedlichem Detaillierungsgrad durchgeführt werden (ISO/IEC 27005, 2018).

Hierbei stehen eine quantitative und qualitative Risikoanalysemethodik zur Verfügung. Alternativ können die beiden Risikoanalysemethoden kombiniert werden. In dieser wissenschaftlichen Arbeit wird die quantitative Analysemethode eingesetzt. Bei der quantitativen Risikoanalyse werden die numerischen Werte für die Konsequenzen und die Wahrscheinlichkeiten genutzt. Der Vorteil der quantitativen Methode ist die direkte Verbindung mit den Zielen und Anliegen der Hochschule im Bereich Informationssicherheitsrisikomanagement.

3.2.2.1 Assessment der Auswirkung

Die Informationssicherheitsvorfälle haben einen negativen finanziellen Einfluss auf die Geschäftsziele der Hochschulen. Um die Auswirkung der Sicherheitsvorfälle zu beurteilen, müssen die Folgen einer Verletzung der Informationssicherheit sowie Vertraulichkeit, Integrität oder Verfügbarkeit der Vermögenswerte berücksichtigt werden (IEC 27001: 2005, Abschnitt 4.2.1 e).

Außerdem spielt der monetäre Wert aller Vermögenswerte eine große Rolle, um mehr Informationen für die Entscheidungsfindung zu liefern und einen effizienten Entscheidungsprozess zu ermöglichen.

Nach der Bedeutung der Vermögenswerte zur Erfüllung der Geschäftsziele der Hochschulen werden die Vermögenswerte bewertet und nach ihrer Kritikalität klassifiziert.

Es gibt zwei Bewertungsarten: der Wiederbeschaffungswert des Vermögenswertes und die Geschäftskonsequenzen eines Verlustes oder Bloßstellung der Vermögenswertes.

Die Bewertung ist aus einer Business-Impact-Analyse zu ermitteln. Die Bewertung von Vermögenswerten ist wichtig für die Folgenabschätzung eines Vorfallszenarios, da der Vorfall mehr als einen Vermögenswert oder einen Teil eines Vermögenswertes betreffen kann. Da es unterschiedliche Auswirkungen von verschiedenen Bedrohungen und Sicherheitslücken auf Ressourcen gibt, ist der Verlust der Vermögenswerte sowie von Vertraulichkeit, Integrität und Verfügbarkeit unterschiedlich. Bei der Folgenabschätzung werden die möglichen Auswirkungen auf das Geschäft berechnet.

Die Folgen basieren sauf monetären, technischen und menschlichen Auswirkungskriterien oder anderen Kriterien, welche für die Hochschule relevant sind.

Bei der Bestimmung der Auswirkungen sind die Informationen im Abschnitt Risikoidentifikation berücksichtigt. (siehe Tabelle 15)

3.2.2.2 Assessment der Wahrscheinlichkeit

In diesem Abschnitt wird die Wahrscheinlichkeit jedes auftretenden Szenarios und die Auswirkung mit quantitativen Analysetechniken bewertet. Unter Berücksichtigen vieler Faktoren werden die Wahrscheinlichkeiten jedes Szenarios bestimmt, indem gefragt wird, wie oft Bedrohungen auftreten und wie leicht die Sicherheitslücken ausgenutzt werden.

Nun werden die geschätzten Risiken aus der Wahrscheinlichkeit eines Vorfallszenarios und seiner Folgen geschätzt. Anhand der Informationen im Abschnitt Risikoidentifikation (3.2.1) wird die Wahrscheinlichkeit festgelegt. Das Risiko wird durch Multiplikation der Auswirkung mit der Wahrscheinlichkeit in der Tabelle 15 berechnet.

3.2.3 Risiko Bewertung / -analyse

Die geschätzten Risiken muss man mit den im Kontext definierten Kriterien für die Risikobewertung vergleichen. Die Risikobewertungskriterien sollten mit dem Informationssicherheitsrisikomanagementkontext übereinstimmen und die Ziele der Hochschulen berücksichtigen, um über die Risikobewertungstätigkeit zu entscheiden.

Die Entscheidung sollte beinhalten:

- ob eine Aktivität durchgeführt werden sollte
- Prioritäten für die Risikobehandlung

Vertragliche, rechtliche und aufsichtliche Anforderungen und Faktoren müssen die geschätzten Risiken berücksichtigen, um eine sinnvolle Risikobewertungsphase anzufangen.

Tabelle 15: Risikobewertungstabelle (Quelle F. Djumayev)

Asset-Typ	Bed. ID	Bedrohungsart	Bedrohung	Ursache	Bestehende Maßnahmen	Schwachstellen/Sicherheitslücken	C	I	A	Eintritts-wahrscheinlichkeit	Auswirkung	Risiko	Risiko-ID
Hardware	HWB1	Beeinträchtigung der Informationen	Manipulation der Hardware	D	-	Einzelne USB-Anschlüsse fürs Aufladen und Daten	x	x	x	sehr wahrscheinlich	kritisch	12	HWR1
	HWB2	Beeinträchtigung der Informationen	Manipulation der Hardware	D	-	UEFI-Netzwerkkarten Unterstützung	x	x	x	wahrscheinlich	kritisch	9	HWR2
	HWB3	Unautorisierte Aktionen	Unberechtigte Nutzung von Geräten	D	-	Schwache Passwörter	x	x	x	wahrscheinlich	kritisch	9	HWR3
Software	SWB1	Beeinträchtigung der Informationen	Manipulation der Software (Botnetz)	D	Virenschutzprogramme, Firewall, sichere WLAN-Verbindung mit Verschlüsselungsstandard mit WPA2 und sichere Internetverbindung https//:	Fehlende Sicherheitsupdates	x	x	x	wahrscheinlich	katastrophal	12	SWR1
	SWB2	Beeinträchtigung der Funktionen	Missbrauch der Rechte	D	-	Schlechte Passwortverwaltung			x	möglich	kritisch	6	SWR2
	SWB3	Beeinträchtigung der Informationen	Manipulation der Software (Windows OLE)	D	-	Anfälligkeit der Funktion des Windows Object Linking und Embedding (Windows OLE)	x	x	x	wahrscheinlich	kritisch	9	SWR3
Infrastruktur	IB1	Physische Schäden	Feuer	A	Blitzschutz	Mangel an formellen Richtlinien			x	wahrscheinlich	katastrophal	12	IR1
	IB2	Beeinträchtigung der Informationen	Diebstahl von Medien und Dokumenten	D	Türsicherungen	Mangel an etablierter Überwachung	x		x	möglich	begrenzt	4	IR2
	IB3	Verlust von wesentlichen Dienstleistungen	Wasserschäden	A, D, E	-	Wasserschäden		x	x	möglich	begrenzt	4	IR3
Personen	PB1	Mensch	Personalausfall	A, D	-	Keine Vertretungsregelung			x	wahrscheinlich	kritisch	9	PR1
	PB2	Mensch	Menschliche Fehlhandlung	A, D	-	Mangel an Sicherheitsbewusstsein	x	x	x	wahrscheinlich	kritisch	9	PR2
	PB3	Mensch	Social Engineering	D	-	Mensch	x	X		wahrscheinlich	kritisch	9	PR3
Netzwerk	NB1	Beeinträchtigung der Informationen	Ausspähen der Informationen/Fernspionage	D	-	Fehler bei der Netzwerkarchitektur	x			möglich	kritisch	9	NR1
	NB2	Verlust von wesentlichen Dienstleistungen	Stromausfall	A, D, E	-	Instabiles Stromnetz		x	x	möglich	kritisch	6	NR2
	NB3	Beeinträchtigung der Informationen	Lauschen	D	Zertifizierung CA	Ungeschützter vertraulicher Datenverkehr	x			möglich	kritisch	6	NR3

3.3 Risikobehandlung

Die Aufgaben der Risikobehandlung ist die Auswahl der Maßnahmen, die der Reduzierung, Beibehaltung, Vermeidung oder gemeinsamen Nutzung der Risiken dienen.

Die Risikomodifikation, Risikoübernahme, Risikovermeidung und Risikoteilung sind die möglichen Optionen für die Risikobehandlung.

Bei der Auswahl der Optionen für die Risikobehandlung sollen die Kosten für die Umsetzung und der erwartete Nutzen dieser Option auf Basis der Risikobewertungsergebnisse betrachtet werden.

Die schwerwiegenden und seltenen Risiken muss das Management besonders beachten und wenn nötig die aus wirtschaftlichen Gründen nicht gerechtfertigten Maßnahmen umgesetzt werden.

Nach der Prioritätenreihenfolge muss mit eindeutigem Zeitrahmen die Risikobehandlung durchgeführt werden. Anhand der Kosten-Nutzen-Analyse, des Risiko-Rankings und verschiedener Techniken werden die Prioritäten festgelegt. Es liegt in der Verantwortung des Managements, das Gleichgewicht zwischen den Kosten für die Durchführung der Maßnahmen und der Budgetvergabe zu bestimmen.

Nach der Planung der Risikobehandlung müssen die Restrisiken ermittelt werden. Wenn die Hochschule die Restrisiken nicht akzeptiert, ist eine weitere Iteration für die Risikobehandlung erforderlich. (International Standard, ISO/IEC 27005:2011(E))

3.3.1 Risikomodifikation

Die Risikomodifizierung dient durch die Einführung, Änderung und Entfernung der Maßnahmen einer Reduzierung eines Risikolevels, wodurch das Risiko akzeptabel werden kann. Die Maßnahmen bieten grundsätzlich folgende Schutzfunktionen:

- Verbesserung
- Vermeidung
- Minimierung der Auswirkung
- Erkennung
- Überwachung und Bewusstsein

Bei der Auswahl der Maßnahmen ist es wichtig, die Kosten für die Beschaffung, Wartung und Implementierung der Maßnahmen gegen zu schützende Werte abzuwägen. Die detaillierten Informationen zur Auswahl der Maßnahmen liefert die ISO/IEC 27005.

Laut der ISO gibt es verschiedene Restriktionen, die die Auswahl einer Maßnahme beeinflussen können. Dazu gehören die Kompatibilität, Performanceanforderungen und Verwaltbarkeit. Außerdem sollen bei der Einführung der Maßnahmen die weiteren Restriktionen berücksichtigt werden:

- Zeitliche Einschränkungen
- Budgeteinschränkungen
- Technische Grenzen
- Betriebseinschränkungen
- Rechtliche Einschränkungen
- Benutzerfreundlichkeit

Darüber hinaus stellt die ISO/IEC eine Liste der weiteren Einschränkungen zur Verfügung, welche bei der Einführung der Maßnahmen betrachtet werden sollen.

3.3.2 Risikoübernahme

Nach der Managemententscheidung erfolgt die Annahme des bestimmten Risikos. In diesem Fall soll das Risikolevel die Risikoakzeptanzkriterien erfüllen. Das Risiko wird ohne den Einsatz der Maßnahmen übernommen.

3.3.3 Risikovermeidung

Bei der Risikovermeidung sollen die Hochschulen es versuchen, diejenigen Aktivitäten, welche ein Risiko verursachen, zu verhindern, zum Beispiel die Gründung eines Hochschulrechenzentrums in der Nähe eines Sees oder irgendwo anders, wo Risiken durch die Natur bestehen. Dann sollen durch die Auswahl eines anderen Ortes für das Rechenzentrum diese Risiken verhindert werden.

3.3.4 Risikoteilung

Das Risiko soll mit einer externen Partei der Hochschule geteilt werden, um das Risiko effektiv verwalten zu können. Risikoteilung kann die bestehenden Risiken modifizieren, jedoch kann sie neue Risiken hervorrufen.

Zur Gewährleistung der sicheren Risikobehandlung kann die Risikoteilung durchgeführt werden. Sie erfolgt durch die Versicherung oder durch die Beauftragung eines externen Partners, der für die Überwachung der Informationssysteme zuständig ist und bei dem Risikoauftritt die erforderlichen Maßnahmen durchführt, bevor das Risiko die Schäden hervorrufen kann.

3.3.5 Beispiele für einen Risikobehandlungsplan an der Hochschule

Um die Risiken zu behandeln, wurde die drei hoch priorisierten Risiken aus der Tabelle 15 ausgesucht. Für alle drei Risiken wurde die Option Risikomodifikation ausgewählt, weil für alle drei Risiken die Maßnahmen zur Reduzierung des vorhandenen Risikos durchgeführt werden müssen. Hier wird ein Risikobehandlungsplan für einzelne Risikos erstellt und beschrieben, damit die Risikobehandlungspläne im nächsten Abschnitt der Risikoakzeptanz zur Entscheidung der Führungskräfte der Hochschule vorgelegt werden können.

In der Tabelle 16 ist der Risikobehandlungsplan für das Risiko „Die Manipulation des Rechners oder Ausführung der Schadsoftware auf dem Rechner durch die Ausnutzung der UEFI-Netzwerkunterstützung“ dargestellt. Einzige Maßnahme zur Reduzierung des bestehenden Risikos ist die Anwendung der originalen Aufladekabel und Geräte. Durch den Einsatz dieser Maßnahme wird das bestehende Risiko von 12 auf 8 reduziert.

Tabelle 16: Risikobehandlungsplan (Quelle F. Djumayev)

Risikobehandlungsplan		
Risiko ID	HWR1	Die Manipulation des Rechners oder Ausführung der Schadsoftware auf dem Rechner durch die Ausnutzung der UEFI-Netzwerkunterstützung
Potenzial	3	Der Hardware wird vertraut und alle weiteren Sicherheitsmechanismen gebaut
Auswirkung	4	Manipulation der Rechner
Risiko	12	Risiko ist nicht akzeptiert
Maßnahmen		Es gibt keine Sicherheitspatches zurzeit, die Original-Aufladekabel oder Geräte von Hersteller besorgen
Umsetzung		01.11.2018-31.12.2018
Restrisiko	6	Neues Potenzial: 2 Neue Auswirkung: 3

Das Risiko „Informationsdiebstahl durch fehlende Sicherheitsupdate der Software“ ist höher eingestuft, weil die Zero-Day- oder Sicherheitslücke der Software für den Angreifer interessant ist. Falls dieses an der Hochschule eintreten würde, könnten die vertraulichen Informationen der Hochschule manipuliert werden und dies zu großem Schaden führen.

Durch das Umsetzen der Maßnahmen sowie Firewall, Änderung der Passwörter alle drei Monate, Virenschutzprogramme und sichere Internetverbindung wird sich das Risiko von 12 auf 6 reduzieren. Der Risikobehandlungsplan für dieses Risiko ist in der Tabelle 17 zu sehen.

Tabelle 17: Risikobehandlungsplan (Quelle: F. Djumayev)

Risikobehandlungsplan		
Risiko ID	SWR1	Informationsdiebstahl durch fehlende Sicherheitsupdates der Software
Potenzial	3	Zero-Day-Angriffe oder Sicherheitslücken in der Software
Auswirkung	4	Diebstahl der vertraulichen Informationen
Risiko	12	Risiko ist nicht akzeptiert
Maßnahmen		Firewall, Virenschutzprogramm, Sicherheitsupdate, Änderung der Passwörter alle 3 Monate, sichere Verbindung mit Internet (https und WPA2)
Umsetzung		01.11.2018-30.01.2019
Restrisiko	6	Neues Potenzial: 2 Neue Auswirkung: 3

Die mangelnde Umsetzung der Richtlinien könnte katastrophale Schäden verursachen. In diesem Beispiel wurde mit der Zerstörung der gesamten IT-Landschaft gerechnet, wenn Brandschutz-Richtlinien nicht eingehalten werden. Durch den Einsatz der benötigten Maßnahmen wie Einhaltung der Normen und Vorschriften kann dieses Risiko modifiziert und das Restrisiko auf 8 gesetzt werden.

Tabelle 18: Risikobehandlungsplan (Quelle F. Djumayev)

Risikobehandlungsplan		
Risiko ID	IR1	Feuer
Potenzial	3	Natürliche Ereignisse oder fehlerhafte Handlung
Auswirkung	4	Zerstörung der IT-Infrastruktur
Risiko	12	Risiko ist nicht akzeptiert
Maßnahmen		Einhaltung einschlägiger Normen und Vorschriften, Blitzschutzmaßnahmen, Brandschutzübungen, Schulungen für Brandschutz organisieren
Umsetzung		01.11.2018-31.12.2018
Restrisiko	8	Neues Potenzial: 2 Neue Auswirkung: 4

3.4 Risikoakzeptanz

Die Behandlung der bewerteten Risiken muss in den Risikobehandlungsplänen beschrieben werden, um die Risikoakzeptanzkriterien zu erfüllen. Dies wurde bereits im vorherigen Abschnitt durchgeführt (siehe Tabellen 16, 17, 18). Die Aufgabe der verantwortlichen Manager ist die Überprüfung und Genehmigung der vorgeschlagenen Risikobehandlungspläne und der daraus resultierenden Restrisiken.

Es gibt die Fälle, bei denen das Restrisiko den Risikoakzeptanzkriterien nicht entsprechen könnte. Zum Beispiel: die höheren Risikokosten, die komplexe Umsetzung der Maßnahmen usw. Wenn das Management diese Risiken akzeptiert, die den üblichen Akzeptanzkriterien nicht entsprechen, muss die Begründung dokumentiert werden.

3.5 Risikokommunikation und Beratung

Bei der Risikokommunikation geht es um den Austausch aller Risikomanagementaktivitäten mit dem Entscheidungsträger oder anderen Interessengruppen. Die Risikokommunikation dient dazu, einen Umgangsplan mit den möglichen Risiken zu entwerfen, in dem alle Informationen über das Risiko ausgetauscht werden. Diese Informationen sollen die Art, Eintrittswahrscheinlichkeit, Auswirkung, Form, Behandlung und Akzeptanz von Risiken umfassen.

Die Kommunikation ist zwischen den Parteien sehr wichtig. Die Entscheidungsträger können auf Basis der gelieferten Informationen die erforderlichen oder passenden Entscheidungen treffen. Die Interessenten können anhand der Kommunikation verstehen, warum diejenige Entscheidung getroffen wurde.

Hauptsächlich sorgt die Risikokommunikation dafür, folgende Ziele zu erreichen:

- Sammeln von Risikoinformationen
- Sicherstellung der Ergebnisse von Risikomanagement der Organisation
- Unterstützung der Entscheidungsfindung
- Teilen der Ergebnisse von Risikobewertung und Präsentation des Risikobehandlungsplans
- Vermeidung oder Reduzierung der Vorfälle und Verstöße gegen die Informationssicherheit
- Verbessern des Bewusstseins

Risikokommunikationspläne soll sowohl für normalen Betrieb als auch für die Notfallsituationen erstellt werden.

Die Risikokommunikation trägt zur Verbesserung des Verständnisses über Informationssicherheitsrisikomanagementprozesse bei.

3.6 Überwachung, Überprüfung und Verbesserung des Risikomanagementprozesses

Die Überwachung des Risikomanagementprozesses soll kontinuierlich durchgeführt werden, um die Ergebnisse des Prozesses zu überprüfen und zu verbessern. Dabei sind alle Schritte des Risikomanagementprozesses zu betrachten.

Die Überwachung und Überprüfung sollen dafür sorgen, dass die Fehler bei der Bewertung der Risiken verhindert und die geplanten Aktivitäten umgesetzt werden. Darüber hinaus sollen die Überstimmung des Risikomanagementprozesses mit den Geschäftszielen und Strategien sichergestellt werden. Im Falle von Änderungen ist der Kontext des Risikomanagements zu ändern.

Zusätzlich werden die folgenden Felder bei der Überwachung und Überprüfung des Risikomanagementprozesses betrachtet:

- Risikobewertungsvorgehensweise
- Rechtlicher Kontext
- Risiko der Auswirkungskriterien
- Risiko der Bewertungskriterien
- Risikoakzeptanzkriterien
- Gesamtbetriebskosten
- Notwendige Ressourcen

Die Durchführung der Überwachung, Überprüfung und Verbesserung des Risikomanagementprozesses trägt zur Sicherstellung bei, dass der Informationssicherheits-risikomanagementprozess den Zielen der Hochschule entspricht und die entsprechenden Aktualisierungen beinhaltet.

4. Weitere Einsatzbereiche des Risikomanagementprozesses an den Hochschulen

4.1 Informationssicherheitsvorfallmanagement

Ein Sicherheitskonzept für die Sicherheitsvorfälle an der Hochschule Augsburg ist bereits vorhanden. Dieser Abschnitt möchte auf Basis des Sicherheitskonzepts für die Sicherheitsvorfälle einen Zusammenhang zwischen den Sicherheitsvorfällen und dem Risikomanagementprozessdarstellen.

Zuerst sollen Fragen beantwortet werden wie „Was ist eigentlich ein Sicherheitsvorfall?“ und „Was ist bei dem Auftritt des Sicherheitsvorfalls zu tun?“.

BSI definiert einen Sicherheitsvorfall als ein unerwünschtes Ereignis, welches die Vertraulichkeit, Verfügbarkeit und Integrität beeinträchtigen und dadurch große Schäden bei einer Organisation hervorrufen kann. (Bundesamt für Sicherheit in der Informationstechnik, 2018)

Die möglichen Arten von Sicherheitsvorfällen, die an der Hochschule Augsburg vorkommen können, sind im Sicherheitskonzept für Informationssicherheitsvorfälle beschrieben. Im Folgenden werden diese aufgelistet:

- Erhöhte Anzahl der unbefugten Zugriffe oder Zugriffsversuche auf die Systeme
- Nicht autorisierter E-Mail-Versand
- Zugriff auf die Mailboxen oder Datenbanken durch den Administrator ohne die Einwilligung der Informationseigentümer
- Verlust von Assets
- Unkontrollierte Änderungen im IT-System

Die Meldung der Informationssicherheitsvorfälle an die entsprechenden Stellen ist wichtig, um die Informationssicherheitsvorfälle zu verhindern oder zu reduzieren. Beim Auftritt eines Informationssicherheitsvorfalls soll dieser an den Rechenzentrumservice der Hochschule Augsburg gemeldet werden.

Anhand der gemeldeten Informationssicherheitsvorfälle können die zuständigen Personen den Risikomanagementprozess durchführen. Es wird dabei untersucht, welches Risiko der aufgetretene Sicherheitsvorfall hervorrufen und wie dieses behandelt werden kann.

Zur Identifizierung des auf Grundlage des Informationssicherheitsvorfalls entstehenden Risikos und Behandlung des Risikos sollen alle relevanten Informationen gesammelt werden.

4.2 Changemanagement

Um erfolgreich und wettbewerbsfähig zu bleiben, müssen sich die Hochschulen in kurzer Zeit an die ständig wachsenden Anforderungen anpassen. Ein funktionierendes Changemanagement ist eine gute Lösung dafür. Unter Changemanagement werden alle Aufgaben, Maßnahmen und Tätigkeiten verstanden, um die Änderung neuer Strategien, Strukturen, Systeme und Prozesse an den Hochschulen umzusetzen.

Ohne Risikomanagement gibt es keine Garantie, dass das Changemanagement erfolgreich ist. Vor allem dürfen die Führungskräfte die Risiken nicht aus den Augen verlieren.

Damit die Änderungen sicher und erfolgreich sind, sollen die möglichen Risiken der vorgenommenen Änderungen identifiziert und die Risikobewertung, Risikoanalyse und Behandlung anhand des festgelegten Risikomanagementkontextes durchgeführt werden.

Zur Identifizierung potenzieller Risiken, die durch die Änderungen verursacht werden können, sollen die folgenden Fragen beantwortet werden:

Welche Änderung wurden vorgenommen?

Welche Systeme, Prozesse oder Assets der Hochschule sind von den Änderungen betroffen?

Wer sind die verantwortlichen Personen für die Änderungen?

Wann werden die Änderungen umgesetzt?

Was sind die erwarteten Ergebnisse der Änderungen?

4.3 Projektmanagement

Die Hauptaufgabe des Projektmanagements besteht darin, eine neue Software oder ein neues Softwaresystem auf Basis der ausgewählten Ressourcen zu entwickeln. Da die Entwicklung der neuen Software oder des Systems unmittelbar mit den Risiken verbunden ist, soll das Projektmanagement ein effizientes Risikomanagement beinhalten.

Die Durchführung des Risikomanagements in einem Projekt erhöht das Erreichen der Projektziele und reduziert die potenziellen Risiken, welche das Scheitern des Projekts begünstigen können.

Vielmehr geht es beim Risikomanagement in einem Projekt darum, mehr mögliche Risiken zu erkennen, als nur die großen Risiken zu identifizieren.

Zur Identifizierung der möglichen Risiken können unterschiedliche Methoden eingesetzt werden. Dazu gehören Brainstorming, Checklisten und strukturierte Befragungen von Experten. In dieser Arbeit wird die Checklistenmethode zur Identifizierung der Projektrisiken verwendet. Dabei werden alle wichtigen Informationen über das Projekt gesammelt, die den Projekterfolg beeinflussen.

Folgende Fragen erheben eine Reihe von Informationen zur Risikoidentifikation. Je nach Größe, Struktur und Ziele des Projekts können diese von dem verantwortlichen Risikobeauftragten erweitert und angepasst werden und sollten formal erfasst werden.

Was sind die Projektziele?

Welche Programme werden angewendet?

Welche Rollen sind definiert?

Wer sind die Anwender?

Welche Gesetze sind vorhanden, die für das Projekt relevant sind?

Welche Vorgaben machen die AGB der ausgesuchten Dienstleister/Partner?

Was sind die geplanten Ressourcen (Budget, Zeit, Mitarbeiter)?

Wer sind die Entscheidungsträger?

Welche Assets werden angewendet?

Anhand der gesammelten Informationen kann eine Risikobewertung gestartet werden, indem die relevanten Risiken identifiziert, analysiert und priorisiert werden. Dabei können die in den Kapiteln von 3.2-3.6 definierten Vorgehensweisen angewendet werden, um den Risikomanagementprozess für ein Projekt durchzuführen.

5. Fazit

Die vorliegende Arbeit beschäftigte sich damit, eine Vorgehensweise für das Informationssicherheitsrisikomanagement für die Hochschulen zu erstellen, und versucht, die folgenden Forschungsfragen zu beantworten: „Wie kann der Informationssicherheitsrisikomanagementprozess an den Hochschulen praxisorientiert eingesetzt werden? Welche Methoden und Vorgehensweise sind von Normen und Standards vorgegeben? Welche Schritte des Risikomanagementprozesses sollen dabei detailliert betrachtet werden?“

Zur Beantwortung der Fragen wurde zuerst untersucht, welche Standards und Normen für die Durchführung des Risikomanagementprozesses existieren und welche Vorgehensweisen von den jeweiligen Standards für das Risikomanagement an den Hochschulen übernommen werden können. Von vorhandenen Standards und Normen werden ISO/IEC 27005, ISO/IEC 31000, BSI 200-3 und ITIL betrachtet.

Da das Ziel der vorliegenden wissenschaftlichen Arbeit die Darstellung einer praxisorientierten Vorgehensweise für das Risikomanagement ist, sollte dafür ein geeigneter Standard ausgewählt werden. ISO/IEC 31000 und ITIL konnten aufgrund ihrer komplexen Inhalte als geeignete Standards für die Risikomanagementvorgehensweise an den Hochschulen nicht ermittelt werden.

BSI 200-3 und ISO/IEC 27005 liefern hingegen dafür praxisorientierte Beispiele, weshalb diese als Grundlage für eine Risikomanagementvorgehensweise betrachtet worden sind.

Der gesamte Risikomanagementprozess auf Basis von ISO/IEC 27005 wurde im Kapitel drei beschrieben. Dabei wurde festgestellt, dass ISO/IEC 27005 gute Erklärungen zu den einzelnen Risikomanagementschritten und ausführliche Informationen zu den Arten von Bedrohungen und Schwachstellen liefert. Jedoch sollten die Festlegung des Kontextes und die Identifikation der Risiken ausführlicher betrachtet und beschrieben werden, damit ein sinnvolles und möglichst einfaches Bild des Informationssicherheitsrisiko-managementprozesses abgebildet wird.

Die Festlegung des Kontextes und Identifizierung der Risiken zählen zu den wichtigen Bausteinen des Risikomanagementprozesses, weil die weiteren nachfolgenden Vorgänge darauf basieren und deren erfolgreicher Ablauf von den erwähnten Vorgängen abhängt.

Zur Sicherstellung der praxisorientierten Vorgehensweise für einen Risikomanagementprozess an den Hochschulen wurde die Checklistenmethode verwendet und die benötigten Checklisten erstellt.

Zuerst wurden die durch das Risikomanagement zu schützendem Prozesse und Assets der Hochschule anhand der Checklisten beschrieben. Mithilfe der gesammelten Informationen an den Assets konnten die möglichen Bedrohungen und Schwachstellen identifiziert werden.

Im Kontext festgelegte Regeln dienten als wichtige Grundlage dazu, um die Eintrittswahrscheinlichkeit und Auswirkung einer entdeckten Bedrohung zu berechnen und das Risiko zu identifizieren. Bei der Berechnung des Risikos wurden die Eintrittswahrscheinlichkeit und Auswirkung der jeweiligen Bedrohung multipliziert.

Nach der Identifizierung der möglichen Risiken wurden die Priorisierung und Behandlung der Risiken durchgeführt. Bei der Risikobehandlung wurden die hohen Risiken ausgewählt und diese durch die passende Risikobehandlungsoption behandelt.

Schließlich wurden die verbleibenden Risiken im Risikoakzeptanzvorgang angenommen.

Zusätzlich wurden in dieser Arbeit die weiteren eigenständigen Hochschulprozesse untersucht, wo der Informationssicherheitsrisikomanagementprozess noch eingesetzt werden kann.

Zusammenfassend wurde der theoriebasierte und komplexe Informationssicherheitsrisikomanagementprozess in dieser wissenschaftlichen Arbeit übersichtlich und anhand der ausführlichen Checklisten möglichst praxisorientiert beschrieben. Die Hochschulen können sich bei Durchführung und Einsatz des Risikomanagementprozesses auf die vorliegende Arbeit stützen.

6. Literaturverzeichnis

Bayern Radio. (2017). *500 Millionen Email-Adressen und Passwörter ausgespäht*. Von 500 Millionen Email-Adressen und Passwörter ausgespäht abgerufen

Blog Avira. (09. 07 2018). *Cyberkriminalität steigt 2018 auf deutsches Rekordhoch - Avira Blog*. Von https://blog.avira.com/de/cyberkriminalitaet-steigt-2018-auf-deutsches-rekordhoch/ abgerufen

BSI-Standard 200-3. (Finale Version 15.11.2017). *Risikoanalyse auf der Basis von IT-Grundschutz. 2017.*

Bundesamt für kerntechnische Entsorgungssicherheit. (2018). *Vorbeugende Maßnahmen gegen Strom*. Von https://www.bfe.bund.de/DE/kt/sicherheit/massnahmen/stromausfall/stromausfall.html abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (05. 09 2018). *BSI - IT-Grundschutz-Kompendium - Umsetzungshinweise zum Baustein INF.1 Allgemeines Gebäude*. Von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/INF/Umsetzungshinweise_zum_Baustein_INF_1_Allgemeines_Geb%C3%A4ude.html abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (10. 10 2018). *Definition eines Sicherheitsvorfalls*. Von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m06/m06122.html abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2018). *Umgang mit Passwort*. Von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g03/g03043.html abgerufen

DFN-CERT. (2016). *Risikoanalyse mit OCTAVE. 2016.*

Gloria-feuerschutz. (1998). *Brandschutz*. Von http://www.gloria-feuerschutz.de/html/checkliste.html abgerufen

Hoschule Augsburg. (2017). *Rechenzentrum IT-Serverkatalog - 2017.*

International Standard. (ISO 31000:2009(E)). *Risk management - Principles and guidelines. 2009.*

International Standard. (ISO/IEC 27005:2011(E)). *Information security risk management. 2011*.

IP Insider. (2018). *Was ist UEFI ? -2018*. Von https://www.ip-insider.de/was-ist-uefi-unified-extensible-firmware-interface-a-751349/ abgerufen

Klipper, S. (1. Auflage 2011). *Information Security Risk Management.* Heidelberg: Vieweg+Teubner.

Königs, H.-P. (2013). *IT - Risikomanagement mit Systemen - 2013.* Springer Vieweg.

Leibniz-Rechenzentrum. (25. 01 2016). *Sicherheitshinweise*. Von https://www.lrz.de/services/netz/wlan/sicherheit/ abgerufen

M. Brenner, N. G. (2. Auflage - 2017). *Praxisbuch ISO/IEC 27001 - 2017.* München: Carl Hanser.

Manager Magazin. (12. 04 2017). Darum sollten Sie Microsoft Office jetzt updaten.

McWelt. (2018). *FileVault - Mac bombensicher oder leicht zu überlisten?* Von https://www.macwelt.de/news/Filevault-Mac-bombensicher-oder-leicht-zu-ueberlisten-9942974.html abgerufen

Romeike, F. (2018). *Risikomanagement.* Wiesbaden: Springer Gabler.

Security Insider. (20. 09 2018). *Was ist Botnetz ?* Von https://www.security-insider.de/was-ist-ein-botnetz-a-555722/ abgerufen

Security Insider. (01. 09 2018). *Was ist physische IT-Sicherheit?* Von https://www.security-insider.de/was-ist-physische-it-sicherheit-a-712152/+https://www.din.de/blob/75204/0581b8fa2d55e68a05fe238122e96665/2012-02-neue-normenreihe-din-en-1627-fuer-einbruchhemmende-bauprodukte-data.pdf abgerufen

Sucurity Insider. (2018). *Datacenter Security muss etlichen Gefahren trotzen*. Von https://www.security-insider.de/datacenter-security-muss-etlichen-gefahren-trotzen-a-93128/index3.html abgerufen

T - Online. (19. 10 2017). *Behörde warnt vor WLAN-Sicherheitslücke*. Von https://www.t-online.de/digital/internet/id_82502352/wpa2-sicherheitsluecke-so-surfen-sie-trotz-wlan-luecke-sicher.html abgerufen

The Verge. (2018). *The new MacBook's single port comes with a major security risk*. Von https://www.theverge.com/2015/3/16/8226193/new-apple-macbook-usb-type-c-security-risk-badusb abgerufen