Hochschule
Augsburg University of
Applied Sciences

Fakultät für
Informatik

Bachelorarbeit

Studienrichtung
Wirtschaftsinformatik

Firuza Muhamadova
Analyse und Ausarbeitung der in den ISO-Standards 27001-27005 geforderten Prozesse zum Betrieb eines ISMS

Prüfer: Prof. Dr. Clemens Espe
Zweitprüfer: Christian S. Fötinger
Abgabe der Arbeit am: 20.04.2018

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:
Firuza Muhamadova
Römerstädter Str. 3,
86199 Augsburg
Telefon: +4917621702482
firuza.muhamadova@gmx.de

Erklärung zur Bachelorarbeit

Hiermit versichere ich, die eingereichte Abschlussarbeit selbständig verfasst und keine andere 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

Abstrakt

Die vorliegende Bachelorarbeit befasst sich mit der Ausarbeitung der Prozesse aus den Maßnahmen, Maßnahmenzielen und Anforderungen, die die ISO/IEC-Standards 27001-27005 für den Aufbau eines Informationssicherheitsmanagementsystems (ISMS) vorgeben. Mit der Bereitstellung der Dokumentation und Modellen zu den einzelnen sicherheitsrelevanten Prozessen beabsichtigt die Arbeit, die Einführung und Umsetzung des ISMS in einem Hochschulumfeld zu erleichtern.

Die Bachelorarbeit ist sowohl für Hochschulen als auch für alle anderen Organisationen interessant, die ihre Informationssicherheit anhand der ISO/IEC 27001-27005 Familie verwalten möchten.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BPMN	Business Process Model and Notation
IEC	International Electrotechnical Commission
ISMS	Informationssicherheitsmanagementsystem
ISO	Internation Organisation for Standardization
IT	Informationstechnik
PDCA	Plan – Do – Check – Act
CSIRT	Computer Security Incident Response Team

Begrifflichkeiten nach den ISO/IEC-Standards und dem IT Grundschutz

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
Audit	Systematischer, unabhängiger, dokumentierter Prozess zum Erlangen
Bedrohung	Mögliche Ursache eines unerwünschten Vorfalls, der zu Schäden eines Systems oder einer Organisation führen kann
Integrität	Eigenschaft der Richtigkeit und Vollständigkeit
Informationssicherheit	Aufrechthaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
Informationssicherheitsvorfall	Einzelnes ungewolltes oder unerwartetes Informationssicherheitsereignis oder eine Reihe solche Ereignisse, die eine erhebliche Wahrscheinlichkeit besitzen Geschäftstätigkeiten zu gefährden und die Informationssicherheit zu bedrohen
Informationsverarbeitende Einrichtungen	Jedes informationsverarbeitende System, jeder informationsverarbeitende Dienst oder jede informationsverarbeitende Infrastruktur oder der physische Standort, der diese beherbergt
IT-Systeme	Technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden
Konformität	Erfüllung einer Anforderung

Maßnahme	Maßnahmen zur Veränderung der Risiken
Patch	Ein kleines Programm, das Softwarefehler wie z.B. Sicherheitslücken in Anwendungsprogrammen und Betriebssystemen behebt
Prozess	Satz zusammenhängender, sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt
Risiko	Auswirkung von Gewissheit auf Ziele
Risikomanagement	Koordinierte Tätigkeiten zum Zwecke der Führung und Steuerung einer Organisation in Bezug auf Risiken
Schwachstelle	Von einer oder mehreren Bedrohungen ausnutzbare Schwäche eines Wertes oder einer Maßnahme
Trojanisches Pferd	Ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung
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
Wurm	Eine Schadsoftware, ähnlich einem Virus, die sich selbst reproduziert und sich durch die Ausnutzung der Kommunikationsstellen selbständig verbreitet

1. Einleitung

Die revolutionären Folgen der Digitalisierung im 20. und verstärkt im 21. Jahrhundert haben die Bedeutung von Rechnern und des Internets sowohl im privatem als auch im öffentlichen Leben exponentiell gesteigert. Zur wichtigsten Aufgabe der EDV-Anlagen gehört die Generierung von Daten. Jede Organisation, die von der digitalen Revolution betroffen ist, verfügt über zahlreiche Daten. Die durch sie vermittelten Informationen bzw. die informationsverarbeitenden Einrichtungen sind für die Geschäftsführung und Betriebskontinuität eines Unternehmens wesentlich. Aus diesem Grund sind diese mithilfe von geeigneten Maßnahmen vor möglichen Risiken zu schützen. Dazu sollen die Informationssicherheitsmaßnahmen definiert, umgesetzt, regelmäßig überwacht und hinsichtlich der Organisationsziele und -struktur verbessert werden.

Ein Informationssicherheitsmanagementsystem stellt die erforderlichen Richtlinien, Vorgehensweisen und Anweisungen bereit, um die Informationssicherheit einer Organisation zu gewährleisten.

1.1 Problemstellung

Die informationssicherheitsrelevanten Angaben sind in den ISO/IEC-Standards 27001-27005 in Form von Maßnahmen und Anforderungen beschrieben. Daher liefern die ISO/IEC-Normen einen allgemeinen Überblick darüber, was eine Organisation bei ihren betrieblichen Abläufen beachten soll.

Manche Organisationsabläufe werden sich oft wiederholen. Zum Beispiel kann die Einstellung eines neuen Mitarbeiters so oft durchgeführt werden, bis der Organisationsbedarf für neue Mitarbeiter gedeckt ist. Die zuständige Person für die Steuerung dieses Ablaufs soll daher darüber Bescheid wissen, was er gemäß den ISO/IEC-Standards für die Einstellung eines Mitarbeiters zu beachten hat.

Es kann durchaus vorkommen, dass der Zuständige bei der Durchführung dieses (oder eines anderen) Ablaufs einen Fehler begeht. In diesem Fall ist es schwierig nachzuweisen, wo genau die Fehler im Ablauf liegen.

Auch kann die Fortsetzung eines beliebigen Ablaufs verhindert werden, weil die für den Ablauf zuständige Person aufgrund einer Krankheit nicht arbeitsfähig ist.

1.2 Zielsetzung

Eine ausführliche Prozessdokumentation gibt an, welche Aktivitäten innerhalb eines Prozesses durchzuführen sind und wer für die Ausführung der einzelnen Aktivitäten zuständig ist. Außerdem zeichnet sie die Kommunikation zwischen den Prozessteilnehmern auf.

Die Prozessdokumentation dient ferner als eine Grundlage dafür, einen Überblick über die wiederkehrenden Organisationsprozesse zu bekommen.

Für die Erstellung der beabsichtigten Prozessdokumentation fragt die vorliegende Arbeit nach, welche Maßnahmen in ISO/IEC 27001-27005 sich als Prozesse darstellen lassen.

Dazu werden die einzelnen Maßnahmen mit ihren Zielen und der Umsetzungsanleitung analysiert. Jeder abgeleitete Prozess wird in der Arbeit Schritt für Schritt erläutert. Zusätzlich erfolgt für jeden einzelnen Prozess eine Prozessvisualisierung und Beschreibung, um seinen Ablauf im Detail betrachten zu können.

1.3 Aufbau der Arbeit

Diese Arbeit besteht aus vier Teilen. Im ersten Teil werden die für die Einführung eines ISMS wichtigen Standards aus der ISO/IEC- 27000- Reihe vorgestellt.

Der zweite Teil der Arbeit beschäftigt sich mit der Ermittlung grundlegenden Wissens über das Prozessmanagement und dessen Wichtigkeit Außerdem gibt dieser Teil einen Überblick über die wesentlichen Prozessmodellierungswerkzeuge.

Der dritte Teil umfasst alle aus den ISO/IEC-Standards 27001-27005 abgebildeten Prozesse. Für jeden Prozess werden zuerst seine zugehörigen Aktivitäten beschrieben und diese mithilfe der Modelle visualisiert.

Mit einer exemplarischen Prozessbeschreibung aus dem Hochschulumfeld befasst sich der letzte Teil der Arbeit, in dem der Prozess der Benutzerkennungsverwaltung an der Hochschule Augsburg untersucht wird.

Die Arbeit schließt mit einem Fazit.

2. Die ISO/IEC 27000- Familie und deren Inhalte

ISO bedeutet Internationale Organisation für die Standardisierung. Sie beschäftigt sich mit der Erstellung von Dokumenten, welche die Anforderungen, Spezifikationen und Eigenschaften zu einem bestimmten Sachgebiet umfassen. Diese sollen als eine Mustervorlage für die sich wiederholenden Prozesse gelten. Das Hauptziel, welches die ISO mit der Standardisierung erzielen möchte, ist das Erreichen eines einheitlichen Verständnisses über ein bestimmtes Ziel. Zum Beispiel ist es wichtig, wenn zwei Gesprächspartner über das Thema Informationssicherheit sprechen, dass sie darunter das Gleiche verstehen.

Zu einem der bekanntesten Standards gehört die ISO/IEC 27000- Familie, die für die Sicherheit der Informationssysteme geeignet ist. Wenn von ISO/IEC 27000 gesprochen wird, dann ist damit eine vereinheitlichte Darstellung der Anforderungen und deren Umsetzung, der Messungen und des Risikomanagements für ein ISMS gemeint. Im Folgenden werden die einzelnen Teile der ISO/IEC 27000- Reihe mit ihren umfassenden Aufgaben definiert.

ISO/IEC 27000 beinhaltet die grundlegenden Fachbegriffe und deren Erklärung, die für den Bereich der Informationssicherheit relevant sind.

2.1 ISO/IEC 27001

ISO/IEC 27001 ist ein standardisiertes Handbuch, welches sich mit den Mindestanforderungen auseinandersetzt. Mithilfe der Anforderungen wird beschrieben, welche Voraussetzungen eine Organisation für den Aufbau, die Inbetriebnahme und Instandhaltung des ISMS erfüllen soll. Um dies erreichen zu können, bietet die ISO/IEC 27001 eine gründliche Vorgehensweise, wodurch die Einrichtung und Umsetzung des ISMS erfolgreich geschieht. Die unten folgenden Aufzählungen beziehen sich auf das genannte Verfahren.

- Konformität der ISO/IEC 27000 Normen mit den für die Verwirklichung des einzelnen Managementsystems zur Verfügung stehenden Normen
- Einsatzgebiete der ISO/IEC 27000 Normen unabhängig der Eigenschaften einer Organisation
- Feststellung der Rollen für die Informationssicherheit beziehungsweise für die Protokollierung der ISMS-Fähigkeiten

- Bereitstellung der erforderlichen Ressourcen und Wissen, was eine dauerhafte Existenz des ISMS gewährleistet

Darüber hinaus definiert ISO/IEC 27001 die wichtigsten Maßnahmen, die die Unternehmensprozesse mit bestimmten Vorgaben unterstützen. Dank der Einhaltung und Einführung der Maßnahmen soll das Eintreffen der sicherheitsbezogenen Risiken für Informationen vermieden werden. (Michael Brenner, 2017, S. 29-63)

2.2 ISO/IEC 27002

Die heutige Zeit der Globalisierung verursacht eine enge Vernetzung der Unternehmenswerte. Zu den Werten einer Organisation gehören nicht nur die Geschäftsziele und Strategien, sondern auch die Informationswerte, die sich auf die zusammenhängende Beziehung zwischen den Informationen und deren Verarbeitungsmitteln basieren. Das bedeutet, dass die Organisationen die notwendigen Maßnahmen für den Schutz der eigenen Werte konzipieren und durchführen sollen, damit sie bei ihrer Geschäftsführung weiterhin erfolgreich bleiben zu können. Die Einführung der Sicherheitsmaßnahmen wird dafür sorgen, dass die Risiken im Gebiet Informationssicherheit reduziert und im besten Fall komplett vermieden werden. Für die Sicherstellung ihrer Werte gegen die bösartigen Angriffe bietet ISO/IEC 27002 den Organisationen eine Sammlung von Maßnahmen an. Dabei sind zuerst die folgenden Schritte durchzuführen:

- Definition der sicherheitsbezogenen Anforderungen eines Unternehmens
- Auswahl der geeigneten Maßnahmen und Gewährleistung deren Umsetzung und Handhabung (DIN, ISO/IEC 27002, 2015)

2.3 ISO/IEC 27003

Die allein in einer Sprache der Standardisierung beschriebenen Mindestanforderungen, welche ISO/IEC 27001 enthält, sind wertlos oder wenig nützlich, bis ihre Bedeutung nicht genau erläutert ist. Die Anforderungen vermitteln zwar eine Vorstellung über die geplante Einführung des ISMS, aber diese Vorstellung ist nicht konkret. Sie sagt dem Lesenden nichts darüber, was genau unter der angegebenen Anforderung zu verstehen und wie genau diese Anforderung zu erfüllen ist. Um ein lückenloses Bild von den vorgegebenen Voraussetzungen schaffen zu können, widmet sich ISO/IEC 27003 der Erklärung von Mindestanforderungen und beantwortet die Frage, wie das erzielte ISMS erreicht werden kann. Dafür betrachtet ISO/IEC 27003 die Anforderungen in diesen Feldern:

- Kontext der Organisation

- Führung, Planung und Umsetzung
- Betrieb
- Bewertung der Leistung
- Verbesserung (DIN, ISO/IEC 27003, 2017)

2.4 ISO/IEC 27004

Die Festlegung der Richtlinien für die Bewertung der Informationssicherheitsleistung zählt als Hauptaufgabe von ISO/IEC 27004. Die Unternehmen können davon profitieren, indem sie sich an die allgemein geltenden Informationssicherheitsregeln halten und die Effektivität ihres ISMS bei der Verwirklichung der Anforderungen, welche in ISO/IEC festgelegt sind, überprüfen zu können. Weitere Teilaufgaben von ISO/IEC 27004 sind:

- Messung und Überwachung der Informationssicherheitsperformance
- Messung und Überwachung der Wirksamkeit des ISMS und deren Prozesse
- Analyse und Bewertung der Überwachungs- und Messergebnisse (DIN, ISO/IEC 27004, 2016)

2.5 ISO/IEC 27005

Die ISO/IEC 27005 hat mit der Beschreibung des Risikomanagements im Bereich Informationssicherheit und seiner Prozesse zu tun. Der international geltende Standard gibt in ersten Linie die Erläuterungen zu den jeweiligen zum Risikomanagement gehörenden Begrifflichkeiten.

Das Risikomanagement gilt als enorm wichtiger Bestandteil nicht nur bei der ISMS-Einführung, sondern es ist auch bei der kontinuierlichen Anwendung des ISMS unerlässlich. Zu den Prozessen des Risikomanagements gehören folgende Aktivitäten:

- Identifizierung des Risikos
- Bewertung des Risikos bezüglich der Auswirkungen
- Festlegung der Prioritäten für die Risikobehandlung
- Priorisierung der Aktivitäten für die Reduktion des Risikoeintritts
- Überwachung der Ergebnisse der Risikobehandlung (DIN, ISO/IEC 27005, 2011)

3. Das Prozessmanagement

Betrachtet die Situation der Geschäftsausführung eines Unternehmens für die Zeit vor Globalisierung, stellt sich heraus, dass Unternehmen damals mit ganz anderen Marktbedingungen zu rechnen hatten. Die Märkte waren regional abgegrenzt, die Wettbewerber waren einem Unternehmen bereits bekannt und die Anforderungen an den Markt waren nicht dynamisch. Die Unternehmen stellten sich auf die kontinuierlich gleichbleibende Produktion und auf ein statisch geprägtes Marktumfeld ein.

Heutzutage ist der Markt für ein Unternehmen mit immer mehr Herausforderungen verknüpft, welche eine schnelle Reaktion auf die Veränderungen und eine rasche Anpassung an die wechselnde Marktatmosphäre verlangen. Das oberste Ziel jedes Betriebs ist natürlich, bei der Ausführung seines Geschäftes erfolgreich zu sein. In der gegenwärtigen Zeit ist der Unternehmenserfolg nicht allein von der Vielfältigkeit und Qualität seiner produzierten Waren oder angebotenen Dienstleistungen abhängig. Darüber hinaus wird vorausgesetzt, dass sich das Unternehmen gegenüber den Marktveränderungen dynamisch verhält. Mit größtmöglicher Flexibilität können die sich verändernden Kundenanforderungen erfüllt werden. (Jörg Becker, 2012, S. 3-6)

Für die Beherrschung des ökonomischen Wandels müssen Struktur und Strategie eines Unternehmens modifiziert werden. Dazu sind eine Beobachtung und Umgestaltung der internen Betriebsaktivitäten sehr sinnvoll. Unter den umzustrukturierenden Aktivitäten sind alle betrieblichen Abläufe zu verstehen, die für die Entwicklung eines Produktes oder einer Dienstleistung durchgeführt werden. Dies beinhaltet der Fachbegriff der „Prozessorientierung“ (oder Prozessmanagement), der im Sinne der Unternehmensgestaltung die dafür benötigten wichtigen Schritte enthält.

3.1 Verwendungszeile des Prozessmanagements

In den bisherigen Absätzen wurde versucht, die Rolle des Prozessmanagements zu verdeutlichen. Um das Prozessmanagement selbst genauer verstehen zu können, bietet es sich an, dessen Ziele und Einsatzgebiete zu beschreiben. Das Prozessmanagement eines Unternehmens kann unterschiedliche Funktionen übernehmen. Häufig wird der Begriff Prozessmanagement für drei verschiedene Ziele verwendet. In erster Linie bezeichnet Prozessmanagement die Einführung einer Software für die Prozessoptimierung. Zunächst werden unter Prozessmanagement also die Verbesserungsprogramme verstanden, die eine temporäre Verbesserung erzielen.

Obwohl die oben geführten Bezeichnungen miteinander zusammenhängen, dienen sie entgegengesetzten Funktionen. Die Aufgabe einer Unternehmenssoftware besteht darin, die Prozesse des Unternehmens zu untersuchen, um diese später zu automatisieren. Hierfür werden die einzelnen Prozesse zum IT-System des Unternehmens hinzugefügt.

Eine Prozessverbesserung beschäftigt sich mit der Auswahl der verbesserungswürdigen Prozesse und deren Optimierung. Da die Prozessverbesserung bislang nicht alle Geschäftsprozesse abdeckt, entsteht durch diese Lücke ein Bedarf für ein Entwicklungsprogramm, das die Prozessverbesserung für die gesamten Unternehmensprozesse ausführt und die Optimierung langfristig und dauerhaft fortsetzt.

Die untenstehende Abbildung stellt die einzelnen Schritte des Entwicklungsprogramms bezüglich des Prozessmanagements und der dafür einzusetzenden Methoden beziehungsweise Werkzeuge dar.

Somit kann die Einführung des Prozessmanagements die Wettbewerbsfähigkeit und das erfolgreiches (Weiter-)Bestehen eines Unternehmens auf dem Wirtschaftsmarkt gewährleisten. (Füermann, 2014)

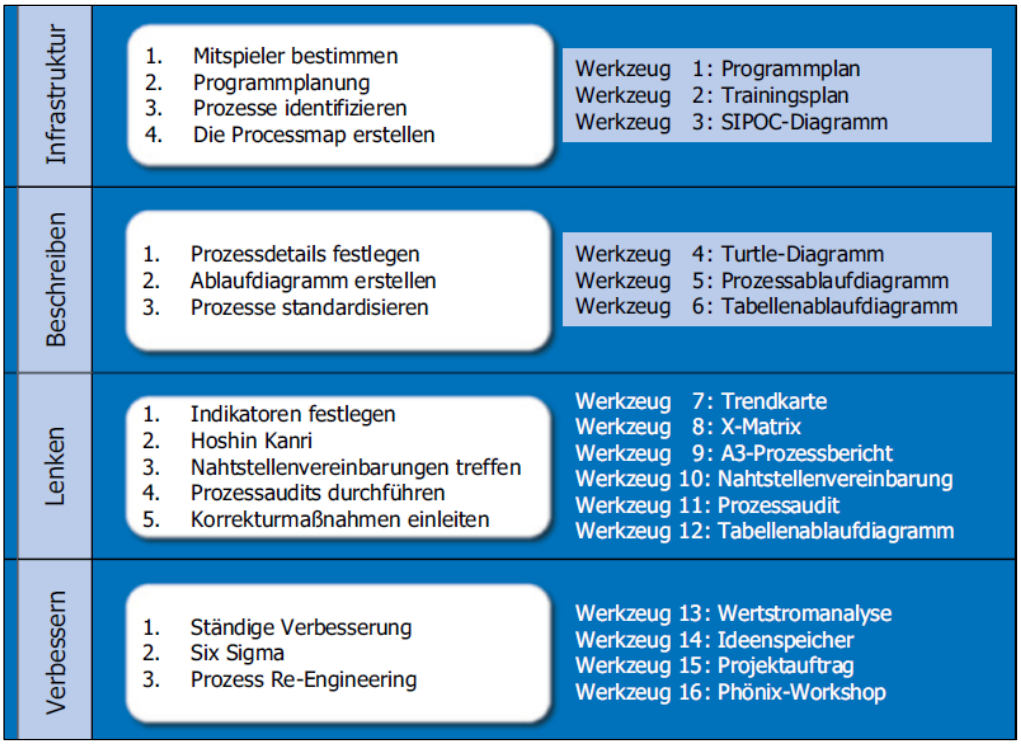

Abbildung 1: Gliederung des Programms

Quelle: vgl. Füermann, 2014.

3.2 Die Notwendigkeit und Vorgehensweise des Prozessmanagements im Bereich IT-Sicherheit

In den vorigen Abschnitten wurde die große Bedeutung des Prozessmanagements für jeden Betrieb erläutert und wie die Durchführung des Prozessmanagements hierbei aussehen kann. Im Folgenden geht es darum, wie das Prozessmanagement im Bereich IT-Sicherheit in einem ISMS verankert sein kann.

Bestandteile des ISMS

Grundlegende Elemente für die Entwicklung eines Informationssicherheits-managementsystems (ISMS) sind:

- Definition der zu schützenden Informationen-Assets
- Erstellung oder Auswahl der passenden Anweisungen für das gesetzte Ziel (Richtlinie)
- Planung und Darstellung der Aktivitäten, welche aufeinanderfolgen und aus mehreren Inputs ein Output erzeugen (Prozess)
- Durchführung der geplanten Vorgänge für die Datensicherheit (Verfahren) (Michael Brenner, 2017)

Um das Ziel und die Aufgaben eines ISMS genauer zu verstehen, sollen die oben genannten Punkte detailliert betrachtet werden. Als wesentlicher Baustein, welcher für die Verwirklichung der weiteren Schritte erforderlich ist, gilt die Identifizierung der Informationswerte. Dabei werden diejenigen Werte definiert, deren Sicherheit für eine Organisation oder für ein Unternehmen unverzichtbar ist. An erster Stelle gehören die Daten dazu, die sich unmittelbar auf die Informationen beziehen. Dies können Hard- und Software, Einrichtungen und Anlagen sein.

Nach der Auflistung der zu schützenden Werte ist festzulegen, welche Richtlinien für die Realisierung der Wertesicherheit verfolgt oder angelegt werden sollen. Es ist möglich, diese Vorgaben in einer Organisation intern zu definieren oder die vorhandenen Standards als Grundlage dafür zu benutzen.

Eine schrittweise Darstellung der Vorgaben, welche bereits als Richtlinie definiert wurden, gehört zu einem wesentlichen Bestandteil des ISMS. Weiterhin gehört eine übersichtliche Dokumentation für die Umsetzung der gezielten Abläufe dazu, in der klar beschrieben wird, welche Aktivitäten in welcher Reihenfolge und von wem durchgeführt werden sollen. Durch die Prozessorientierung werden die Vorgänge gesteuert.

Allerdings sind Definition und Steuerung der Vorgänge für die Gewährleistung der Sicherheit von Informationswerten nicht ausreichend. Zusätzlich werden die einzelnen Aktivitäten eines bestimmten Prozesses der zugehörigen Abteilung beziehungsweise dem zuständigen Mitarbeiter zugeordnet, um deren effiziente Ausführung sicherstellen zu können.

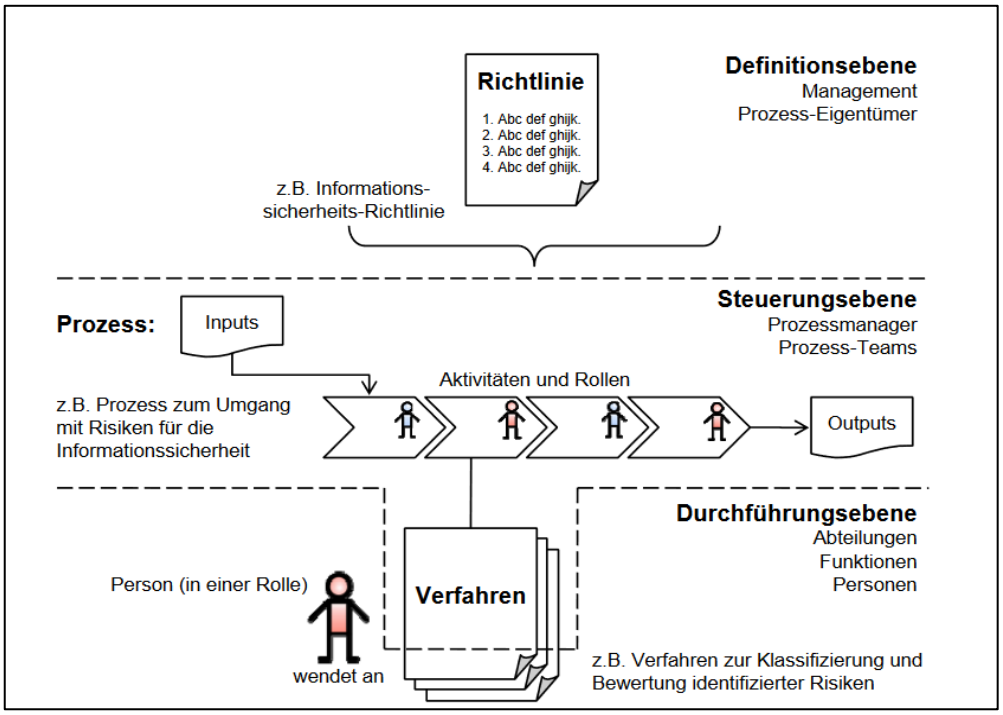

Abbildung 2: Zusammenhänge zwischen Richtlinien, Prozessen und Verfahren

Quelle: vgl. Brenner, Gentschen Felde, Hommel, Metzger. Reiser, Schaaf, 2017, S. 19.

Im ISO-Standard 27001 wurden die Hauptbestandteile eines ISMS wie Richtlinie, Prozesse und Verfahren auf drei Ebenen platziert. Dementsprechend liegen die Richtlinien auf der Definitionsebene und Prozesse befinden sich auf der Steuerungsebene, indem sie die einzelnen Aktivitäten, die dafür Verantwortlichen und die Abhängigkeiten zwischen den Vorgängen festlegen. Das Verfahren gehört sich zur Durchführungsebene. Die Zusammenhänge zwischen den genannten Bestandteilen des ISMS werden anhand von Abbildung 2 ersichtlich. (Michael Brenner, 2017, S. 17-19)

PDCA – Darstellung des Prozesslebenszyklus

Damit die Prozesse volle Leistung bringen zu können, fehlen allerdings noch wesentliche Voraussetzungen. Dazu sollen die Prozesse von einem Prozessmanager überwacht, gesteuert und ständig verbessert werden.

ISO/IEC 27000 verweist auf die PDCA-Methodik, welche die Optimierung und Verbesserung von Prozessen ermöglicht, indem die entsprechenden Richtlinien,

Verfahren und Prozesse für den Schutz der Unternehmenswerte aufgrund der wechselnden Marktanforderungen mehrmals definiert und kontinuierlich angepasst werden.

Der PDCA-Zyklus ist für das Qualitätsmanagement von ISMS-Bestandelementen geeignet und leistet dabei eine leistungsorientierte Weiterentwicklung der betrachteten Objekte. Abbildung 3 gibt eine Übersicht über diese Methodik.

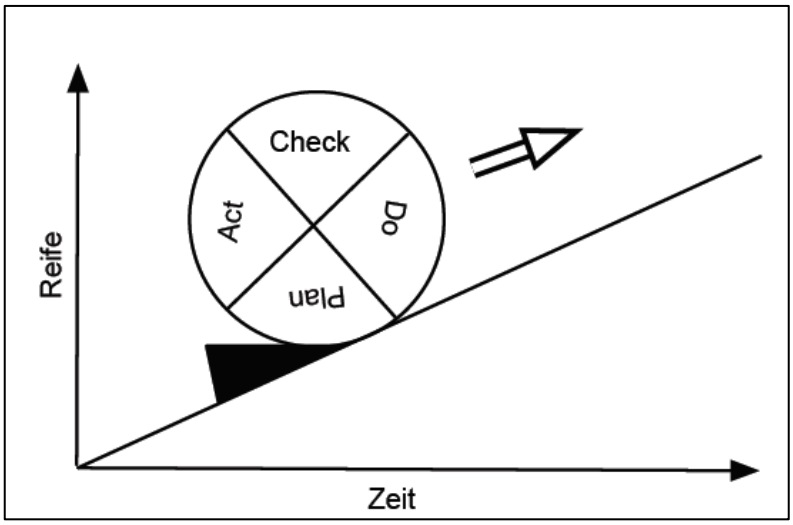

Abbildung 3: Die Plan-Do-Check-Act-Methodik

Quelle: vgl. Brenner, Gentschen Felde, Hommel, Metzger. Reiser, Schaaf, 2017, S. 24.

Das Rad ist in die vier Phasen der PDCA-Vorgehensweise gegliedert und zeigt eine Aufwärtsbewegung mit dem Zeitverlauf, damit die optimalen Verbesserungen erzielt werden können. Eine geplante Aktivität soll umgesetzt, die Umsetzungen überprüft und die Überprüfungen nach den zu erreichenden Zielen korrigiert werden. Die Korrekturen zählen wiederum als verbesserte Pläne und verfolgen ihrerseits die eben erwähnten Phasen des PDCA-Zyklus.

Jede Phase des PDCA-Modells hat seine bestimmten Anwendungsfälle. Diese werden ausführlich erklärt, wann welches Vorgehen angewendet wird.

Plan – **Planungsphase** kann durchgeführt werden:

- für die Planung des neuen ISMS
- für die Planung von Verbesserungen des vorhandenen ISMS

Für die Realisierung der vorgenommenen Planungsziele definiert ISO/IEC 27001 die erforderlichen Mindestanforderungen und wesentlichen Aspekte.

Die Planungsphase nach PDCA beinhaltet hauptsächlich zwei große Bausteine. Diese sollen gemäß den definierten Mindestanforderungen geplant werden.

Planung der Maßnahmen zum Umgang mit Risiken und Chancen

Die Einführung eines ISMS zeigt die potenziellen Möglichkeiten, welche die systematische Erreichung der Informationssicherheit darstellt. Diese werden als Chancen bezeichnet. Dennoch kann das Ziel eines ISMS ohne Veränderungen in der Organisation nicht erreicht werden, sondern es ist durchaus möglich, dass die Organisationen ihre Struktur und Unternehmenskultur umstellen müssen. Die Umstrukturierung kann die Risiken verursachen. Zum Beispiel: Die Einführung des ISMS verlangt, dass alle relevanten Prozesse, Verfahren und Richtlinien gut dokumentiert sind. Die Dokumente sind ständig zu pflegen. Das beutet mehr Aufwand für Mitarbeiter und Verlangsamung der Arbeitsabläufe.

Für die Reduzierung der Risiken und Nutzung der Chancen, welche durch die Umsetzung eines ISMS ausgelöst werden, sollen Maßnahmen geplant werden. Dieser Planungsschritt befasst sich vor allem mit der Frage, wie die geplanten Maßnahmen in die Prozesse des ISMS mit einbezogen und ihre Einwirkung gemessen werden können.

In der Planungsphase werden darüber hinaus die Risikobewertung und Risikobehandlung für die Informationssicherheit geplant.

Planung der Erreichung von Zielen für die Informationssicherheit

Die Informationssicherheitsziele dienen dafür, die Erwartungen von der Einführung des ISMS zu erfüllen. Damit die beabsichtigten Ziele für die Informationssicherheit erreicht werden können, soll eine Planung für

- die Feststellung der notwendigen Schritte
- die Definition der Verantwortlichen
- die Festlegung der Ressourcen
- die Bewertung der Ergebnisse

zustande kommen.

Do – Umsetzungsphase

Die Planungsergebnisse werden in dieser Phase mithilfe der relevanten Elemente umgesetzt. Die Rolle der unterstützenden Elemente ist dabei äußerst wichtig. Dazu zählen die Fähigkeiten und Bereitschaft der für den Bereich Informationssicherheit zuständigen

beschäftigten Personen. Spezifische Kompetenz und Bewusstsein für das Konzept des ISMS sind die Voraussetzungen, die die Mitarbeiter beziehungsweise das Management einer Organisation zu erfüllen haben.

Da sich die Implementierung wie auch andere Phasen des PDCA-Zyklus wiederholt ausführen lassen, ist es daher sinnvoll, diese Ressourcen für die ISMS immer bereitzustellen und ausreichend vorrätig zu haben.

Die Mindestanforderungen von ISO/IEC 27001 definieren, dass alle festgelegten Pläne umgesetzt und gut dokumentiert werden sollen. Die Dokumente halten fest, was und wie umgesetzt wurde.

Check – Überprüfungsphase

Die Checkphase entspricht den sogenannten Testaktivitäten, die durchgeführt werden sollen, um zu prüfen, ob die Implementierungsergebnisse mit den angestrebten Zielen übereinstimmen. Eine fortlaufende Überprüfung basiert auf der Überwachung, Messung, Analyse und Bewertung der wesentlichen Faktoren wie Effektivität, Effizienz und Konformität der Umsetzungen.

Die Konformität bezeichnet die Einhaltung der Planung bezüglich der definierten Prozesse, Verfahren und Maßnahmen. Diese sollen gemäß der im Plan festgelegten Reihenfolge umgesetzt sein. Wenn die planmäßige Einhaltung der Vorgaben erfolgreich geschehen ist, wird im nächsten Schritt überprüft, ob die Prozesse, Maßnahmen und Verfahren auch das erwartete Ergebnis leisten. Letztlich wird die Effizienzüberprüfung ausgeführt, indem der Ressourcenverbrauch während der Durchführung der Maßnahmen, Prozesse und Verfahren betrachtet wird.

Abbildung 4: Anforderungen für die Messung, Überwachung, Analyse und Bewertung während der Überprüfungsphase
Quelle: Firuza Muhamadova in Anlehnung an Brenner, Gentschen Felde und andere, 2017.

Wie aus der Abbildung 4 erkennbar ist, setzt die Norm ISO/IEC 27001 voraus, dass die Überwachung, Messung, Analyse und Bewertung anhand der im Standard definierten Anforderungen durchzuführen sind.

Die Abbildung liefert die Informationen über die grundlegenden Anforderungen von Überwachung, Messung, Bewertung und Analyse.

Zu den weiteren Überprüfungspunkten gehören auch die Planung und Durchführung des Auditprogramms und der Managementbewertung. Auch hierzu sind die Mindestanforderungen durch ISO/IEC 27001 festgelegt.

Act – Verbesserungsphase

Im Fall der Nichteinhaltung der vorgegebenen Erfordernisse aus der Planungsphase sollen die Korrektur und Verbesserungsmaßnahmen erfolgen. Die Identifizierung, ob eine Maßnahme zur Korrektur oder Verbesserung dient, erfolgt in der Act-Phase des PDCA-Modells. Die erforderlichen Schritte, die auf Nichtkonformität hinweisen, werden dabei von dem Standard festgehalten.

Die ständige Verbesserung gilt als eine Eigenschaft des prozessorientierten Managements für die Informationssicherheit. (Heinrich Kersten, 2013, S. 45-84) (DIN, ISO/IEC 27001, 2014)

3.3 Die Arten der Prozesse

In diesem Abschnitt geht es um die Untergliederung von Prozessen. Hier ist es wichtig zu wissen, wie ein „Prozess“ definiert ist. Der Begriff „Prozess“ wird in unterschiedlichen Quellen mit wenig abweichenden Bezeichnungen definiert.

Definition von „Prozess“

Unter dem Begriff „Prozess“ versteht man eine Reihe von Aktivitäten, die miteinander verbunden sind und mehrere Eingaben in einem Ergebnis umwandeln.

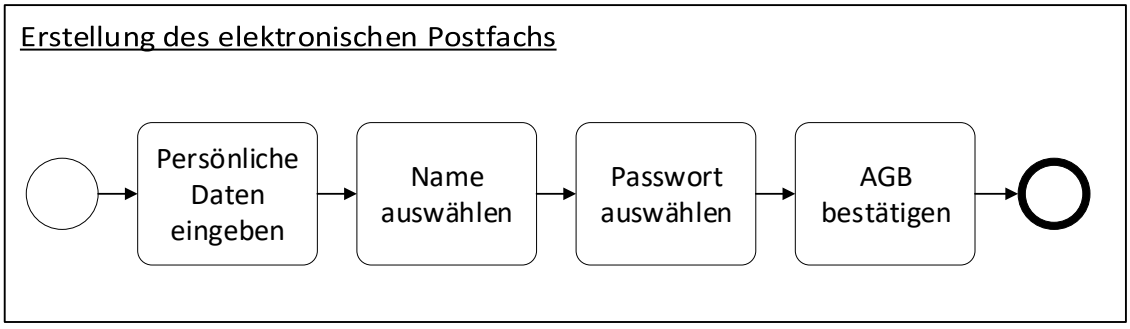

Abbildung 5: Beispiel für einen Prozess
Quelle: Firuza Muhamadova

Der Prozess beginnt mit dem Bedarf des Benutzers an einem E-Mail-Account. Dafür soll der Benutzer einige Daten als Eingaben in ein elektronisches Formular eintragen. Die möglichen Schritte des Prozesses sind aus der Abbildung zu erkennen. Nachdem diese Aktivitäten gemäß der beschriebenen Reihenfolge durchgeführt wurden, bekommt der User als Output ein elektronisches Postfach.

Funktionen des Prozesses

Jeder Prozess verfügt über drei verschiedenen Funktionen. An erster Stelle ist der Prozess ein Leistungsträger, der aus Kundensicht die gewünschten Anforderungen beinhaltet. Zunächst wird der Prozess als Verarbeiter der Leistungen betrachtet und durch diese Funktion trägt er zur Wertschöpfung bei. Letztendlich liefert er die bisherigen empfangenen Ergebnisse an die nächstfolgenden Prozesse weiter.

Klassifizierung der Prozesse

Nach ihren Eigenschaften werden die Prozesse einer bestimmten Klasse zugeordnet. Für die Unterteilung spielen die Aspekte wie Häufigkeit, Objekt, Dimension und Auslösung eine entscheidende Rolle. Beim Häufigkeitskriterium werden die Prozesse in einmalige oder sich wiederholende Prozesse unterteilt. Die Objekte beschreiben das Mittel, mit dem die Prozesse zu tun haben. Das bedeutet, dass sich der Prozess während seiner Ausführungsphase mit zwei unterschiedlichen Arten von Objekten beschäftigt: den Informationen und Materialien. Die Prozesse lassen sich außerdem nach ihrer Form in unternehmens-, bereichs- und personenübergreifenden Prozesse gliedern.

Während die unternehmensübergreifenden Prozesse die Abläufe zwischen zwei Unternehmen beschreiben, beziehen sich die bereichsübergreifenden Prozesse auf zwei oder mehrere Bereiche. Die Abteilungen eines Unternehmens können auch als Bereich angesehen werden.

Ein letzter Aspekt für die Gliederung der Prozesse ist der jeweilige Auslöser von ihnen. Dementsprechend gibt es Prozesse, die immer in einer bestimmten Zeit oder zufällig vorkommen. (Füermann, 2014, S. 1-6)

Abbildung 6 zeigt zusammenfassend die Unterscheidung der Prozesse des Prozessmanagements.

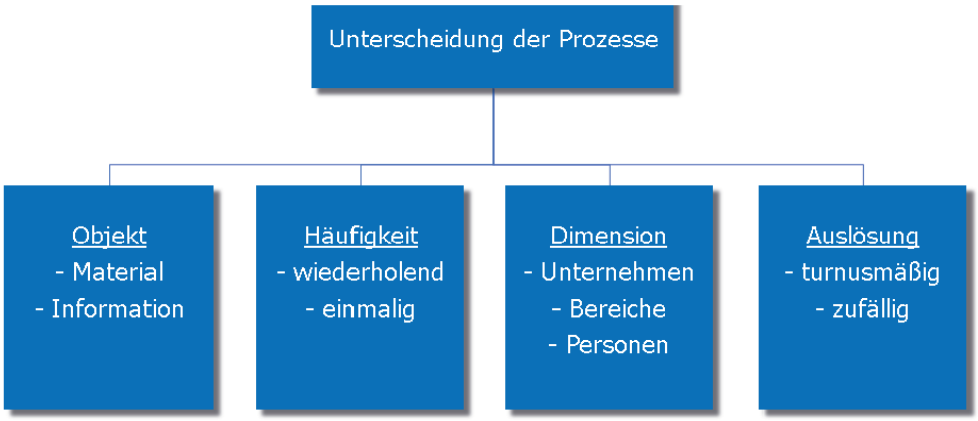

Abbildung 6: Arten der Prozesse.

Quelle: Fuermann, 2014, S. 5.

3.4 BPMN-Werkzeuge für die Prozessmodellierung

BPMN (Business Process Model and Notation) ist eine standardisierte Sprache für die Geschäftsprozessmodellierung. Sie stellt die Modellierungswerkzeuge zur Verfügung und ermöglicht dadurch eine einheitliche Prozessdarstellung. Im Folgenden werden die Symbole von BPMN erläutert, welche bei der Abbildung von Prozessen in den späteren Kapiteln zum Einsatz kommen.

Ein Prozess kann Aufgaben und Unterprozesse beinhalten. Ein Unterprozess ist ein eigenständiger Prozess, der für die Durchführung eines anderen Prozesses verwendet werden kann. Die Unterprozesse werden in BPMN als Quadrate mit Pluszeichen dargestellt. Während diese in einzelne Aktivitäten untergliedert sind, sind die Aufgaben eines Prozesses nicht weiter unterteilbar.

Eine Aktivität bezeichnet eine Aufgabe, welche innerhalb eines Prozesses erledigt werden soll. Die Aktivitäten-Symbole sind die wichtigsten Symbole in BPMN, weil sie bei der Prozessmodellierung oft angewendet werden. Eine Kombination aus Objekt und Verb sorgt für die sinnvolle Beschriftung einer Aktivität, wie zum Beispiel: „Schwachstellen beheben“. In BPMN werden die Aktivitäten mit einem Rechteck mit abgerundeten Ecken dargestellt.

Darüber hinaus beinhaltet ein Prozess die Ereignisse, welche durch kreisförmige Elemente symbolisiert sind. BPMN bietet eine Reihe von Ereignis-Symbolen für die Darstellung des Anfangs und des Endes eines Prozesses, des Empfangs und Versands einer Nachricht, der einzuhaltenden Zeit und Termine und der stattgefundenen Systemfehler. In der vorliegenden Arbeit werden von ihnen die Start- und End-Ereignisse verwendet. In der Modellierung dienen die Start-Ereignisse für die Darstellung der

Prozessauslöser. Aus diesem Grund können ein oder mehrere Start-Ereignisse innerhalb eines Prozesses angewendet. Der Unterschied zwischen Start- und End-Ereignissen liegt in der Linienstärke des Symbols: Ein Start-Ereignis ist mit einer dünnen Linie und ein End-Ereignis mit einer dicken Linie dargestellt.

Die End-Ereignisse werden in den meisten Fällen eingesetzt, um das Beenden oder Abbruch eines Prozesses darzustellen. Ähnlich den Start-Ereignissen können ein oder mehrere End-Ereignisse in einem Prozess angewendet werden.

Ein Prozess kann während seines Ablaufs auch Verzweigungen und Zusammenführungen haben. Diese werden Gateways genannt und dienen der Verwaltung und Kontrolle der Prozessdurchführung. Das Symbol für ein Gateway ist ein auf der Spitze stehendes Quadrat mit verschiedenen Beschriftungen in der Mitte. Es existieren XOR-, inklusive, exklusive und ereignisbasierte Gateways.

XOR-Gateways werden in der Prozessmodellierung eingesetzt, um eine OR-Funktion darzustellen. Gemäß der Bedingung eines XOR-Gateways können entweder die eine oder die andere Aktivität durchgeführt werden. Die Zusammenführung der Aktivitäten ist hier nicht erforderlich.

Im Vergleich zu XOR werden die Aktivitäten von parallelen Gateways zusammengeführt. Ein paralleles Gateway dient der Darstellung einer UND-Funktion zwischen zwei oder mehreren Aktivitäten. Die Bedingung von parallelen Gateway erfordert, dass alle von der Gateway-Bedingung abhängigen Aufgaben durchgeführt werden sollen.

Das inklusive Gateway stellt mehrere Bedingungen dar, von denen mindestens eine richtig sein soll. Das heißt, die Verzweigung bietet mehrere Optionen für unterschiedliche Fälle. Zum Beispiel: Ein Kunde kann bei seinen Fragen zu den Details eines bestimmten Produktes per Telefon, E-Mail oder Post den Produktanbieter kontaktieren und wählt somit eine aus mehreren Möglichkeiten für die Kontaktaufnahme aus.

Folgende Abbildung vermittelt einen detaillierten Überblick über die einzelnen BPMN-Elemente.

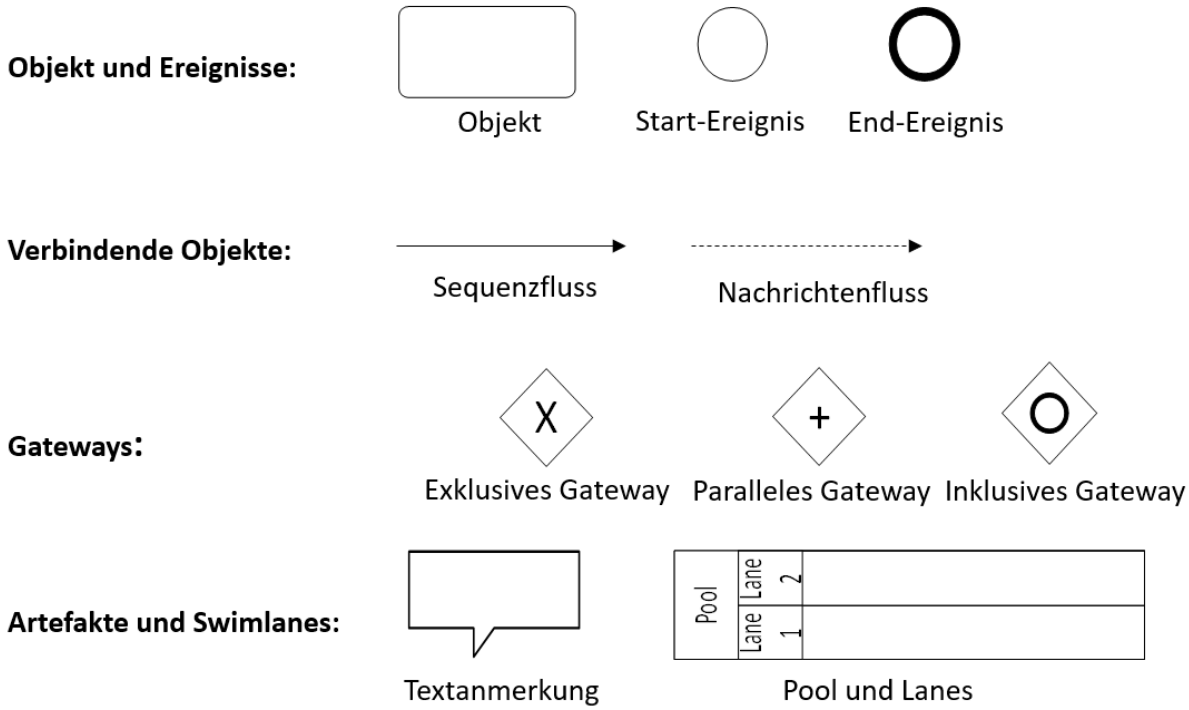

Abbildung 7: Symbole der Prozesselemente in BPMN.

Quelle: Firuza Muhamadova, angelehnt an Göpfert und Lindenbach, 2013, S. 5.

An einem Prozess können sich beliebig viele Teilnehmer beteiligen. Für die Darstellung unterschiedlicher Prozessteilnehmer dient ein Pool. Angenommen, ein Prozess hat zwei Teilnehmer; einer ist der Unternehmer, welcher seine Produkte verkaufen will, der andere ist der Kunde, der sich für die Produkte interessiert. Diese Teilnehmer lassen sich in der Modellierungssprache anhand der einzelnen Pools abbilden.

Die Pools können aus mehreren Lanes bestehen. Die Lanes werden für die Darstellung der einzelnen Aufgabenträger innerhalb eines Pools eingesetzt. In den meisten Fällen können Lanes die Abteilungen einer Organisation oder die Rollen sein.

Für die Verbindung einzelner Prozesselemente innerhalb eines Pools dienen die Sequenzflüsse. Sequenzflüsse dürfen nicht außerhalb des Pools verwendet werden. Jeder Sequenzfluss verfügt über eine Quelle und ein Ziel. Nachrichtenflüsse tragen hingegen zu einer Kollaboration zwischen den Pools bei. Sie werden benutzt, um Nachrichten zu senden und zu empfangen. Es soll bei der Verwendung von Nachrichtenflüssen beachtet werden, dass die Gateways nicht über Nachrichtenflüsse zu verbinden sind. So wie die Sequenzflüsse haben die Nachrichtenflüsse genau einen Anfang und ein Ende. (Jochen Göpfert, 2013)

4. Die wichtigsten Prozesse der ISO/EC 27001-27005

Dieses Kapitel nennt die wichtigsten Themenbereiche für die Einrichtung eines ISMS an einer Hochschule, welche an späterer Stelle dieses Kapitels detailliert erläutert werden. Für einen groben Überblick über das Kapitel sind diese im Folgenden aufgelistet.

- Die Betriebssicherheit beschäftigt sich mit der Frage, wie der kontinuierliche Betrieb von informationsverarbeitenden Einrichtungen sichergestellt werden kann.
- Die Benutzerzugangsverwaltung gewährleistet, dass die dazu berechtigten User Zugang zu den Informationen und informationsverarbeitenden Systemen haben. Mithilfe der empfohlenen Maßnahmen aus ISO/IEC 27002 können die Benutzerzugänge verwaltet werden.
- Die Personalsicherheit liefert Informationen darüber, was bei der Einstellung eines Beschäftigten oder Auftragnehmers zu beachten ist.
- Die Handhabung von Informationssicherheitsvorfällen beschreibt die Maßnahmen für den Umgang mit ihnen.
- Das Risikomanagement stellt fest, welche Risiken bei der Durchführung der Projekte oder Änderungen berücksichtigt werden sollen und wie die Organisation mit den möglichen Risiken umgehen kann.

Außerdem umfasst dieses Kapitel die BPMN-basierten Darstellungen von Anforderungen und Maßnahmen aus der ISO/IEC 27000- Familie. Anhand der Modellierungselemente wird versucht, aus den ISO-Vorgaben die Prozesse abzubilden. Jeder der folgenden Abschnitte, der einen Prozess beschreibt, beinhaltet eine Prozessmodellierung und eine Tabelle für die Prozessbeschreibung, wodurch der Ablauf und die Aufgabe des Prozesses verdeutlicht werden.

4.1 Personalsicherheit

Der Prozess „Personalsicherheit“ beschäftigt sich mit der Einstellung neuer Mitarbeiter. Im Rahmen des Prozesses wird die einzustellende Person nicht nur als ein künftiger Mitarbeiter, sondern auch als ein Auftragnehmer betrachtet. Der Auftragnehmer soll zuerst mit den Regelungen in einer Organisation vertraut gemacht werden.

Die erste Voraussetzung für ein erfolgreiches Informationssicherheitsmanagement in einer Organisation ist die Gewährleistung des Sicherheitsbewusstseins eigener Mitarbeiter. Technische Sicherheitsmaßnahmen allein sind wenig erfolgreich, wenn die Benutzer nicht um die Wichtigkeit von Daten- und Informationsschutz wissen. Ein

falsches Verhalten bezüglich der Sicherheit von informationsverarbeitenden Geräten und Informationen kann große Schäden verursachen. Als negative Folgen solcher unbewusst durchgeführten Handlungen können nicht nur finanzielle Verluste auftreten, sondern es wird auch das individuelle Image eines Unternehmens geschädigt. Deshalb ist es wichtig, dass die Arbeitnehmer einer Organisation mit den Informationen aus Sicherheitssicht richtig umgehen können und dafür ihre Verantwortung zur Kenntnis nehmen.

Das vorliegende Kapitel verweist auf Abschnitt sieben der ISO/IEC 27002 und befasst sich mit der Darstellung der wichtigsten Vorgänge für den Einstellungsprozess. Die einzelnen Prozessschritte sind dabei:

Bewerbung verschicken

Dieser Vorgang dient als ein Auslöser für den Einstellungsprozess. Der Bewerber, der sich für die Arbeitsstelle interessiert, schickt seine vollständigen Bewerbungsunterlagen.

Sicherheitsprüfung durchführen

Nach dem Empfang der Bewerbungsunterlagen hat der zuständige Mitarbeiter aus der Personalabteilung eine Sicherheitsüberprüfung gemäß ISO/IEC 27001 und 27002 durchzuführen. Hierbei soll das Führungszeugnis des Bewerbers hinsichtlich seines bisherigen Verhaltens überprüft werden und ob irgendeine Vorstrafe registriert worden ist. Darüber hinaus soll untersucht werden, ob der vorgelegte Lebenslauf richtig und die Bewerberqualifikation für die Arbeitsstelle ausreichend ist.

Für einen Bewerber entscheiden

Bei positiven Sicherheitsüberprüfungsergebnissen wird dem Bewerber eine Zusage zugeschickt. Im gegenteiligen Fall erfolgt eine Absage. Dann wird der Einstellungsprozess abgebrochen.

Melden/Nachricht verschicken

In beiden Fällen – sowohl bei der Absage als auch bei der Zusage – wird der Bewerber durch eine Nachricht informiert. Die Fortsetzung des Prozesses hängt von der Entscheidung der Personalabteilung ab.

Arbeitsvertrag unterschreiben/zurückschicken

Unter den Unterlagen für den Arbeitsvertrag soll sich auch eine Verpflichtungserklärung oder Geheimhaltungsvereinbarung befinden, welche die Richtlinien der Organisation bezüglich der Informationssicherheit beinhaltet. Diese Unterlagen sind von dem Bewerber zu unterzeichnen.

Mitarbeiter einstellen

Der Prozess wird mit der Einstellung eines kompetenten und geeigneten Arbeitnehmers beendet. (DIN, ISO/IEC 27001, 2014) (DIN, ISO/IEC 27002, 2015)

In folgender Abbildung sind die Prozessvorgänge nach einer logischen Anordnung zu sehen.

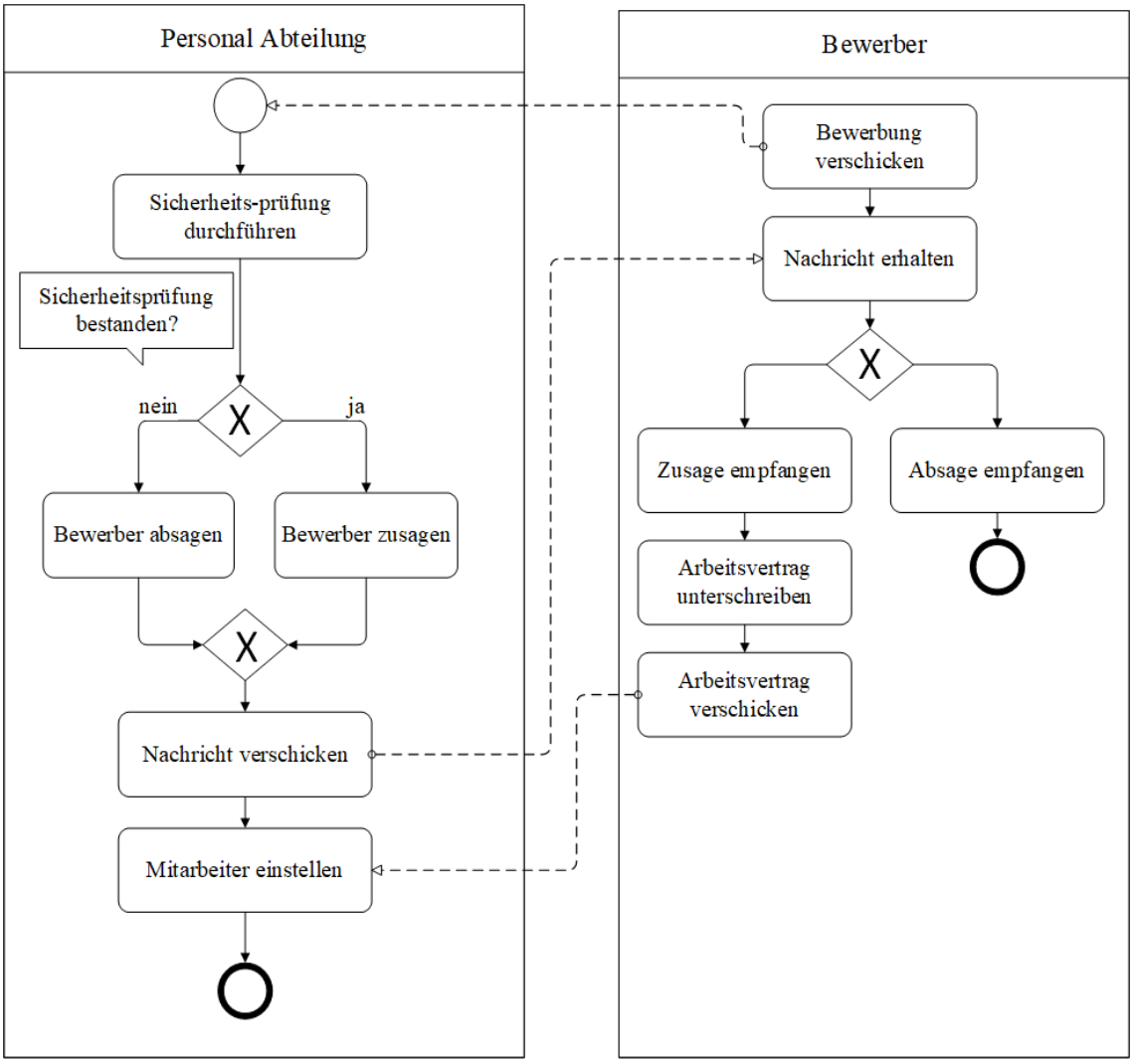

Abbildung 8: Prozessmodell der Personalsicherheit

Quelle: Firuza Muhamadova

Weitere Informationen über den Personalsicherheitsprozess liefert die nachstehende Tabelle.

Tabelle 1: Prozessbeschreibung der Personalsicherheit.

Prozessname: Personalsicherheit	
Zweck: „Es ist sichergestellt, dass Beschäftigte und Auftragnehmer ihre Verantwortlichkeiten verstehen und für die für sie vorgesehenen Rollen geeignet sind.“	
Prozessverantwortlicher: Personalabteilung	**Mitwirkende Personen:** Führungskraft/Leiter der Organisation, Bewerber
Input: Empfang der Bewerbungsunterlagen	
Output: Einstellung geeigneter und kompetenter Person für eine bestimmte Position	
Anforderungen: Die Sicherheitsüberprüfung ist für jede Person durchzuführen, welche ihre Bewerbungsunterlagen für die Einstellung vorgelegt hat.	
Mindestanforderung: Die Organisation muss für Personen, die sie im Bereich Informationssicherheit beschäftigen möchte, die erforderliche Kompetenz festlegen. Diese Personen haben auf Basis ihrer abgeschlossenen Ausbildung ihre Kompetenz für diese Beschäftigung nachzuweisen.	
Mitwirkende Dokumente: Interne Richtlinien der Organisation, Führungszeugnis, Reisepass/Ausweis, Lebenslauf, Nachweise akademischer Qualifikation.	
Schnittstellen des Prozesses: Registrierung und Deregistrierung von Benutzern, Zuteilung und Entziehung von Benutzerzugängen	

Quelle: Firuza Muhamadova

4.2 Benutzerzugangsverwaltung

In diesem Kapitel geht es um die Verwaltung von Benutzerzugänge. Der Begriff Zugang bezeichnet eine Möglichkeit, in die Systeme, Einrichtung und Dienste hineinkommen zu können. Die zentrale Frage der Benutzerzugangsverwaltung lautet, wer auf welche Systeme oder Informationen einen Zugang bekommen darf. Außerdem beschäftigt sich dieser Kapitel mit der Verwaltung von administrativen Zugangsrechten und geheimer Authentifizierungsinformationen von Benutzern.

ISO/IEC 27001 liefert die wichtigsten Maßnahmen und Maßnahmenziele, wodurch die Verwaltung von Benutzerzugängen und der für einen Zugang erforderlichen Informationen erfolgreich durchgeführt werden kann. Eine Anleitung für die Umsetzung der von ISO/IEC 27001 bestimmten Maßnahmen wird von ISO/IEC 27002 bereitgestellt.

Sowohl die Maßnahmen als auch die Anleitungsinformationen sollen das Erreichen des Zieles gewährleisten, welches in den Standards festgelegt ist.

„Ziel: Es ist sichergestellt, dass befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird.“

Mit der Verwaltung von Benutzerzugängen können diejenigen Benutzer die für ihnen berechtigte Informationen und Ressourcen benutzen, die einen Zugang bekommen haben. Einem Benutzer oder Externer, der keinen Zugang erworben hat, darf es nicht gelingen, die Systeme, Dienste und Informationen nutzen zu können.

Die einzelnen Maßnahmen aus der ISO/IEC 27002 lassen sich als Prozesse darstellen. Der Hauptprozess der Benutzerzugangsverwaltung beinhaltet vier Unterprozesse, die eigene Aktivitäten durchführen, jeweils einen Prozessverantwortlicher besitzen und aus mehreren Eingaben die Ergebnisse produzieren. Die Abbildung sieben gibt einen Überblick über die Untergliederung des Benutzerzugangsverwaltungsprozesses.

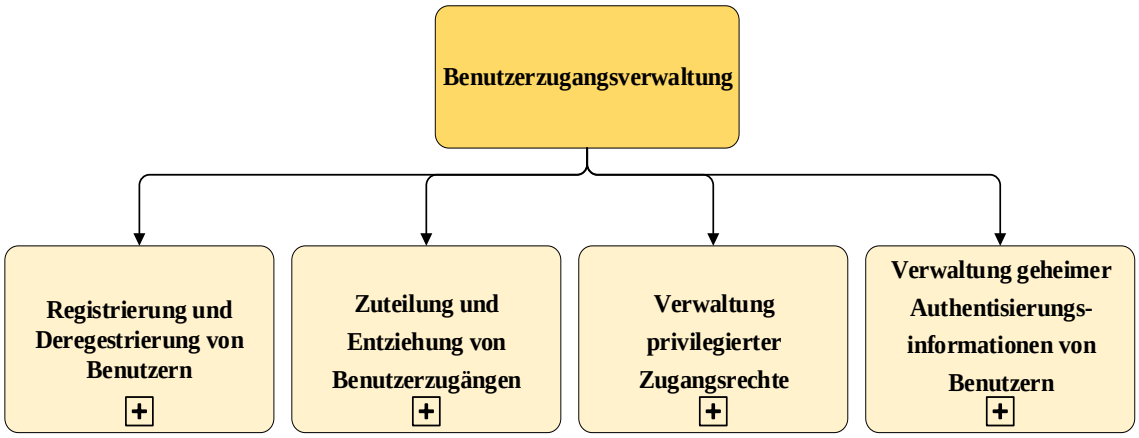

Abbildung 9:Benutzerzugangsverwaltungsprozess mit den vier dazugehörigen Unterprozessen
Quelle: Firuza Muhamadova

In den weiteren Abschnitten der Arbeit folgen die Prozessdarstellungen einzelner Unterprozesse, die sich auf die BPMN basieren. Die Prozessmodelle sind als ein Versuch anzusehen, wodurch die logischen Zusammenhänge zwischen den Prozessaktivitäten deutlich erkennbar werden. (DIN, ISO/IEC 27002, 2015)

4.2.1 Registrierung und Deregistrierung von Benutzern

Der Prozess „Registrierung und Deregistrierung der Benutzer“ ist ein Unterprozess der Benutzerverwaltung, der als erster durchgeführt werden soll. Denn ohne Registrierung der Benutzer beziehungsweise der Benutzerkennung können keine weiteren Aktivitäten hinsichtlich der Benutzerzugangsverwaltung vorgenommen werden.

ISO/IEC 27002 stellt dazu eine Anleitung zur Verfügung, um diesen Unterprozess umzusetzen. Die vorgegebenen Schritte der Anleitung lassen sich in einer logischen Reihenfolge innerhalb des „Registrierung und Deregistrierung“ - Prozesses zuordnen. Die Aktivitäten dieses Prozesses werden von der Personalabteilung und einem Zuständigem, der für die Registrierung und Deregistrierung eines Users verantwortlich ist, durchgeführt. Im Folgenden sind die Vorgänge des Prozesses beschrieben.

Benutzerantrag schicken/erstellen

Der Prozess beginnt mit der Erstellung eines Benutzerantrags von der Personal- oder Fachabteilung. Der Antrag dient der Registrierung oder Deregistrierung einer Benutzerkennung.

Eine Benutzerkennung ist eine spezielle Kennung und wird von dem Administrator angelegt oder deaktiviert. In Kombination mit einem Passwort ermöglicht sie einen Zugang in das geschlossene System.

Bei der Einstellung eines neuen Mitarbeiters wird mit dem Benutzerantrag angefordert, eine Benutzerkennung für den Mitarbeiter anzulegen. Im Gegensatz wird die zugewiesene Benutzerkennung deaktiviert oder gelöscht, wenn ein Mitarbeit die Organisation verlässt.

Antrag prüfen

Der Administrator überprüft den vorgelegten Antrag. Bei einem Benutzerantrag kann es sich von der Registrierung oder Deregistrierung von Benutzern handeln. Je nach der Art des Antrages kann sich der Administrator für unterschiedliche Aktivitäten entscheiden.

Benutzerkennung löschen/deaktivieren

Bei der Beendigung der Beschäftigung wird eine Meldung von der Fach- oder Personalabteilung geschickt, damit die bislang geltende Benutzerkennung des Users gelöscht, deaktiviert werden kann.

Die Aufgabe des Administrators besteht außerdem darin, die vorhandenen Kennungen regelmäßig zu überprüfen. Wenn die Kennung nicht mehr nötig ist, soll diese deaktiviert oder gelöscht werden.

Benutzerkennung zuweisen

Der Administrator überprüft die Benutzerkennung, bevor sie verwendet wird. Bei der Überprüfung ist sicherzustellen, dass die zuweisende Benutzerkennung nicht bereits genutzt wurde. Die Benutzerkennung soll eindeutig definiert sein.

Benutzerdatenbank aktualisieren

Nach dem eine Benutzerkennung zugewiesen oder deaktiviert ist, wird die zentrale Benutzerdatenbank auch vom Administrator aktualisiert. (DIN, ISO/IEC 27002, 2015, S. 33-37)

Im nächsten Verlauf dieses Unterkapitels folgt das Prozessmodell für die Registrierung und Deregistrierung von Benutzern. Das Modell ermöglicht eine bildliche Darstellung der bereits beschriebenen Prozessvorgänge. Darüber hinaus ist eine Prozessbeschreibungstabelle weiter unten zu finden, wodurch die wichtigsten Prozessinformationen zusammengefasst sind.

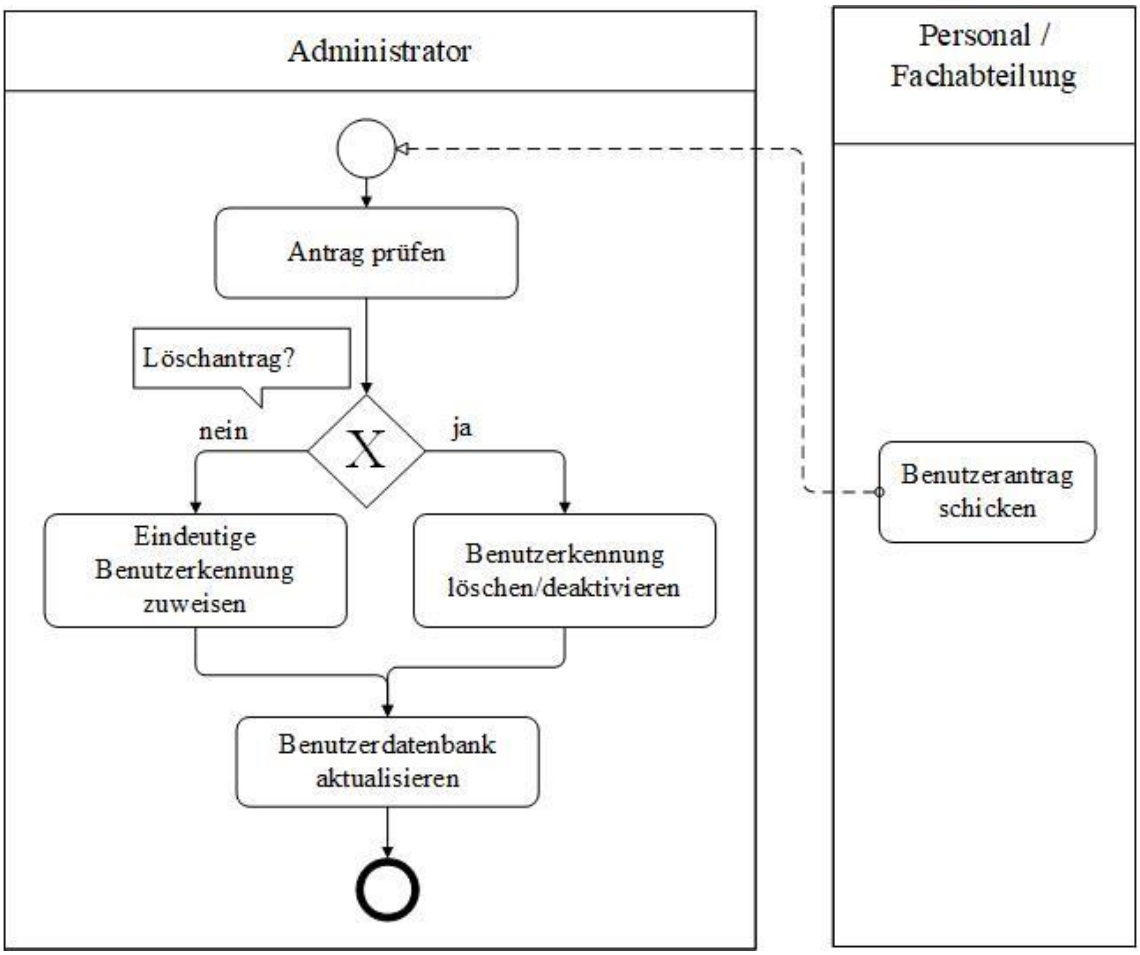

Abbildung 10: Prozessmodell der Registrierung und Deregistrierung von Benutzern

Quelle Firuza Muhamadova.

Tabelle 2: Prozessbeschreibung der Registrierung und Deregistrierung von Benutzern

Prozessname: Registrierung und Deregistrierung von Benutzern
Zweck: Die Umsetzung des Prozesses soll die Zuordnung von Zugangsrechten ermöglichen.

Verantwortlicher: Administrator	**Mitwirkende Personen:** Personalabteilung, Fachabteilung
Input: Die Antragstellung für die Registrierung/Deregistrierung eines Benutzers	
Output: Aktuelle Benutzerdatenbank, zugewiesene/deaktivierte Benutzerkennung	
Anforderungen: Die zuweisende Benutzerkennung soll eindeutig sein, damit ein User durch seine Handlungen verantwortlich gemacht werden kann.	
Mitwirkende Dokumente: Zugangssteuerungsrichtlinien, Benutzerantrag	
Schnittstellen des Prozesses: Zuteilung und Entziehung von Benutzerzugangsrechten, Verwaltung privilegierter Zugangsrechte, Personalsicherheit	

Quelle: Firuza Muhamadova

4.2.2 Zuteilung und Entziehung von Benutzerzugangsrechten

Der zweite Unterprozess, welcher sich dem Hauptprozess der Benutzerverwaltung zuordnen lässt, ist die Zuweisung und Entziehung von Benutzerzugängen. Dieser Prozess beschreibt eine Reihe von Aktivitäten, damit die vorschriftmäßige Zuweisung und Entziehung der Zugangsrechte zu den Systemen und Diensten gewährleistet werden.

Für den Erfolg des Prozesses ist die Kommunikation zwischen dem Prozessverantwortlichen, der Personalabteilung und dem für die Zugangsrechte zuständigen Mitarbeiter sehr wichtig. Durch die regelmäßige Kommunikation wird der Schutz gegen den Missbrauch von Zugangsrechte sichergestellt.

In den nächsten Absätzen werden die Prozessvorgänge beschrieben, welche für die Entziehung oder Zuweisung einer Zugangsrecht durchgeführt werden sollen.

Antrag erstellen/schicken

Ähnlich dem vorherigen Prozess wird bei der Zuweisung oder Entziehung der Zugangsrecht einen Antrag von Personal- oder Fachabteilung erstellt. Mit der Antragsstellung wird die Entziehung der Zugangsrecht gefordert, wenn ein Mitarbeiter seine Position innerhalb der Organisation geändert oder seine Beschäftigung gekündigt hat. Der Zugangsrechtzuweisungsantrag dient dafür, dass eine Zugangsrecht einer Benutzerkennung zugewiesen wird.

Antrag überprüfen

Beide Arten von den erstellten Anträgen werden von einem Administrator bearbeitet. Beim Vorlegen eines Zugangsrechtentziehungsantrags deaktiviert er die bereits

zugewiesene Zugangsrecht. Die Zuweisung einer Zugangsrecht soll von der für die Informationssysteme oder Dienste zuständigen Person genehmigt werden. Der Administrator soll dabei beachten, dass die beantragten Zugangsrechte erst nach der Genehmigung aktiviert werden.

Berechtigungsstufe überprüfen

Die Überprüfung der Berechtigungsstufe zählt als ein wesentlich wichtiger Vorgang. Die Angemessenheit des Berechtigungsgrads mit den bereits festgelegten Richtlinien und Anforderungen soll dabei untersucht werden. ISO/IEC 27002 empfiehlt den großen Organisationen, ihre Zugangsrechte entsprechend den Funktionen beziehungsweise Aufgaben zu trennen. Eine solche Aufgabentrennung verhindert, dass einer Person alle Zugangsrechte zur Verfügung stehen und diese ihre Zugangsrechte missbrauchen könnte, ohne dabei das Einverständnis von anderen einzuholen.

Zuweisung ablehnen

Falls das zuweisende Recht den festgelegten Zugangsrichtlinien nicht entspricht, wird die Zuweisung dieses Rechts abgelehnt. Mit der Ablehnung wird der Prozess abgebrochen.

Zuweisung genehmigen

Die zuständige Person für Informationssysteme oder Dienste genehmigt die Berechtigung, falls die Überprüfung der Berechtigungsstufe positive Ergebnisse liefert. Das bedeutet, dass die angeforderte Zugangsrecht den Zugangsrichtlinien und Anforderungen der Organisation angemessen ist.

Zugangsrecht zuweisen

Nach der empfangenen Genehmigung für die Zuweisung weist der Administrator das Zugangsrecht einer Benutzerkennung zu.

Verzeichnis aktualisieren

Außerdem beschäftigt sich der Administrator mit der Anfertigung und Pflege eines zentralen Verzeichnisses, in dem alle Zugangsrechte nach der Benutzerkennung zugeordnet sind. Sowohl bei der Zuweisung als auch bei der Entziehung einer Zugangsrecht soll das zentrale Verzeichnis aktualisiert werden. (DIN, ISO/IEC 27002, 2015, S. 33-34)

Eine graphische Darstellung des Prozesses ermöglicht die Abbildung 11.

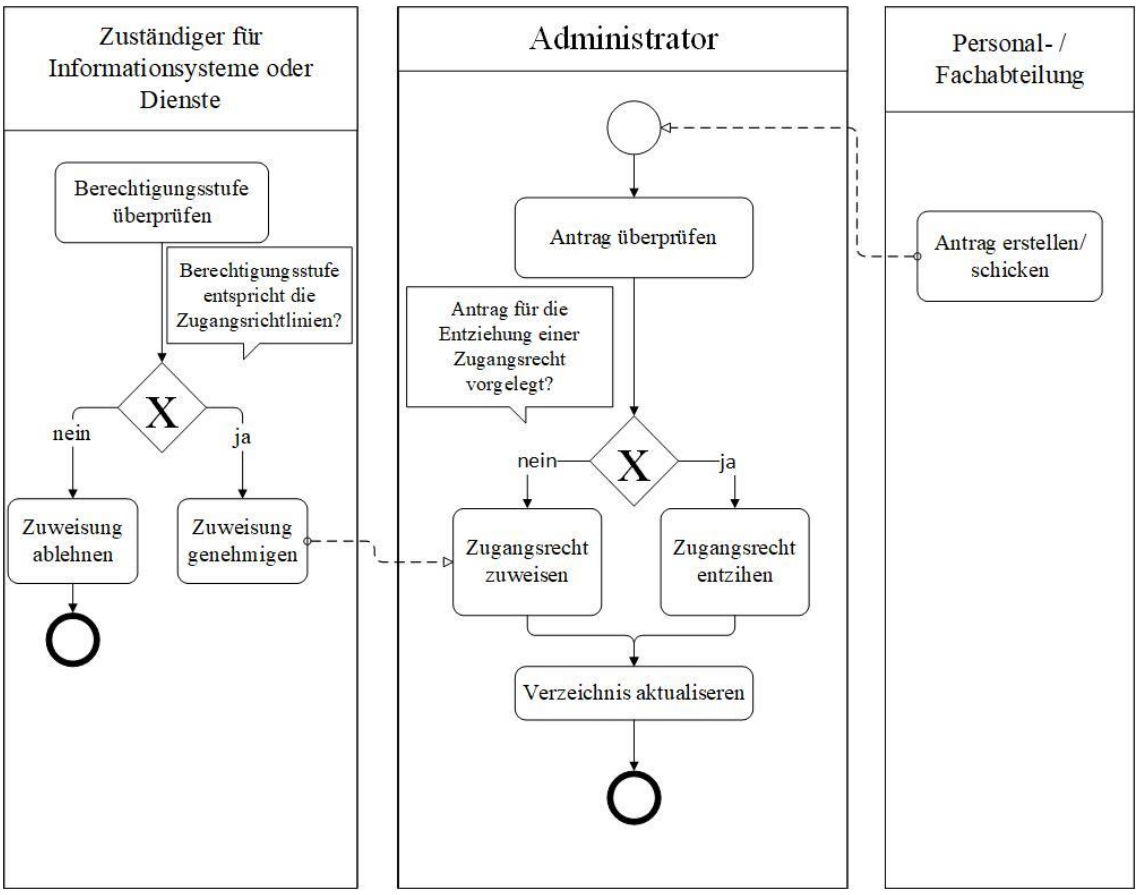

Abbildung 11: Prozessmodell der Zuweisung und Entziehung von Zugangsrechten

Quelle: Firuza Muhamadova

Die wesentlichen Informationen über den Prozess Zuweisung und Entziehung von Zugangsrechten beschreibt folgende Tabelle.

Tabelle 3:Prozessbeschreibung der Zuweisung und Entziehung von Zugangsrechten.

Prozessname: Zuteilung und Entziehung von Benutzerzugangsrechten	
Zweck: Die Umsetzung des Prozesses soll ermöglichen, Zugangsrechte für alle Benutzerarten zu allen Systemen und Diensten zuzuweisen oder zu entziehen.	
Verantwortlicher: Administrator	**Mitwirkende Personen:** Personal-/Fachabteilung, zuständige Personen für Informationssysteme und Dienste/Genehmiger
Input: Antragstellung für die Zuweisung oder Entziehung von Zugangsrechten	
Output: Aktuelles Verzeichnis für Zugangsrechte, zugewiesene/entzogene Zugangsrechte	
Anforderungen: Die Benutzerzugangsrollen sind festzulegen und die Anzahl von Zugangsrechten zu typischen Benutzerzugangsprofilen zusammenzufassen.	

Die Zugangsrechte sollen zusammen mit den Eigentümern der Informationssysteme und Dienste regelmäßig überprüft werden.
Mitwirkende Dokumente: Richtlinien für die Zugangssteuerung, Berechtigungsantrag
Schnittstellen des Prozesses: Verwaltung privilegierter Zugangsrechte, Personalsicherheit

Quelle: Firuza Muhamadova

4.2.3 Verwaltung privilegierter Zugangsrechte

Der dritte Unterprozess dient der Verwaltung privilegierter Zugangsrechte.

Das Unternehmen Verizon veröffentlichte im Jahr 2016 einen Bericht über Untersuchungen von Verstößen und Störungen im Bereich der IT-Sicherheit. Die Untersuchungsergebnisse lassen erkennen, dass die Mehrheit der in 2015 erfolgten Verstöße auf den Missbrauch privilegierter Rechte zurückzuführen ist. Von den untersuchten Missbrauchsfällen fielen 172 auf Vorfälle bei privilegierten Zugangsrechten. Folgende Grafik gibt einen Überblick über die Verstöße, die nach der Angriffsart klassifiziert sind.

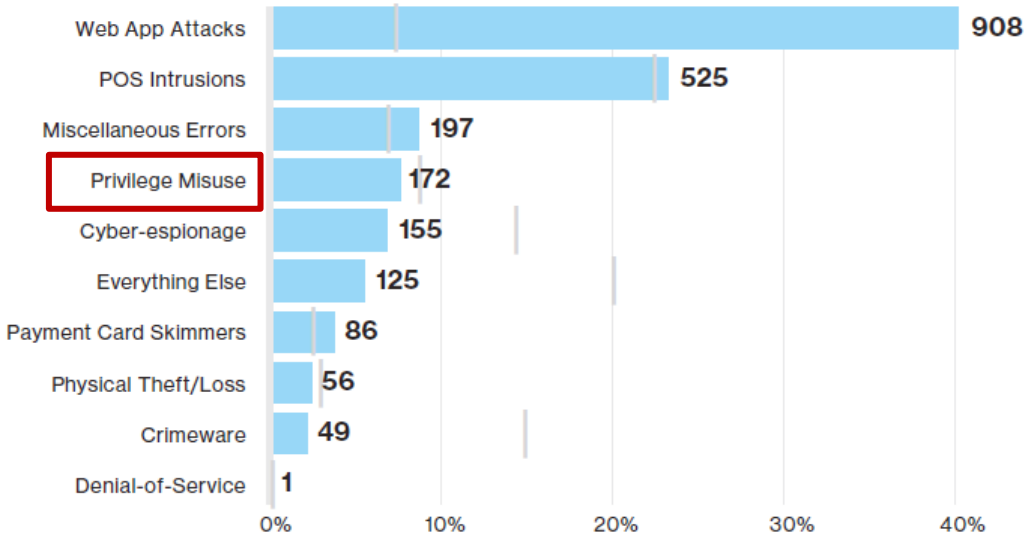

Abbildung 12: Percentage of breaches

Quelle: vgl. Verizon; Untersuchungsbericht für Datenverstöße 2016, S. 23.

Verizon entdeckte insgesamt 2260 Verstöße mit unterschiedlichen Charakteristiken. Die blau dargestellten Balken zeigen die Anzahl der Verstöße pro Angriffsart. Die grauen senkrechten Linien in der Abbildung beschreiben prozentuale Zahlen im Verhältnis zu den gesamten Verstoßformen. Es ist erstaunlich, dass die Missbräuche von privilegierten Zugangsrechten sehr oft vorkommen. (www.verizonenterprise.com, 2018)

Privilegierte Benutzer wie Datenbank- und Systemadministratoren oder Supportmitarbeiter besitzen die administrativen Rechte für mehrere Ressourcen einer Organisation.

Der Verwaltungsprozess privilegierter Zugangsrechte folgt eine Vorgehensweise, die dem Prozess für die Zuweisung und Entziehung der Zugangsrechte ziemlich ähnlich ist. Die Unterschiede liegen in den ISO Anforderungen, welche einen sicheren Umgang mit den administrativen Zugangsrechten ermöglichen.

Dementsprechend sind an erster Stelle die privilegierten Zugangsrechte und deren User und Anwendungen, welche administrative Zugänge besitzen sollen, zu identifizieren. Vor der Zuweisung privilegierter Zugangsrechte sollen die erforderlichen Kriterien erfüllt werden. Ein privilegiertes Zugangsrecht darf einem User zugeteilt werden, wenn diese für die Ausführung seiner Aufgaben notwendig sind.

Wie von den Anforderungen der ISO/IEC 27002 bereits bekannt ist, werden die Zugangsrechte nach der Funktionsart unterteilt. Eine Unterteilung der Rechte auf diese Art und Weise hat viele Vorteile für die Informationssicherheit. Im Falle eines Angriffes auf ein einfaches Benutzerkonto wird einer Organisation weniger Schaden zugefügt, wohingegen die Schäden bei der Manipulation privilegierter Rechte gravierend sein können.

Ein weiteres Kriterium bei der Zuweisung privilegierter Zugangsrechte beschäftigt sich damit, wann ein Konto mit privilegierten Zugangsrechten zu benutzen ist. Der Benutzer ist verpflichtet, seine administrativen Rechte für die „normalen Geschäfte“ nicht zu verwenden. Dafür besitzt der User zwei Arten von Benutzeraccounts. Der eine Account dient für die Durchführung von administrativen Aktivitäten. In diesem Fall werden die privilegierten Zugangsrechte der Benutzerkennung, welche für die Ausführung der normalen Geschäfte geeignet ist, nicht zugeordnet.

Zusätzlich ist eine Gültigkeitsfrist für die privilegierten Zugangsrechte festzulegen, bevor diese Rechte einem Benutzer zugeteilt werden.

Ein wichtiger Vorgang innerhalb des Prozesses ist die Überwachung der Genehmigung von privilegierten Zugangsrechten. Die administrativen Zugangsrechte sollen erst nach deren Genehmigung aktiviert werden.

Da die Benutzerkonten mit den privilegierten Zugangsrechten für eine Organisation von großer Bedeutung sind, sollen diese in kurzen Abständen immer überprüft werden. Wenn

ein User mit privilegierten Zugangsrechten die Organisation verlassen hat, sind seine administrativen Zugangsrechte so schnell wie möglich zu deaktivieren oder zu blockieren. Durch solche durchgeführten Maßnahmen wird der Missbrauch der administrativen Rechte vermieden. (DIN, ISO/IEC 27002, 2015, S. 34-35)

Da der Verwaltungsprozess der privilegierter Zugangsrechte gleiche Vorgänge wie der Prozesse für die Zuweisung und Entziehung der Zugangsrechte durchführt, ist die zusätzliche Darstellung seines Prozessmodells ist nicht notwendig.

Folgende Prozessbeschreibungstabelle definiert die Merkmale, Ziel und die Schnittstelle des Prozesses. Darüber hinaus beinhaltet sie die grundlegenden Anforderungen zu dem Steuerungsprozess der administrativen Rechte.

Tabelle 4: Prozessbeschreibung der Verwaltung privilegierter Zugangsrechte.

<table>
<tr><td colspan="2">Prozessname: Verwaltung privilegierter Zugangsrechte</td></tr>
<tr><td colspan="2">Zweck: Mit der Umsetzung des Prozesses sollen die Zuteilung und der Gebrach privilegierter Zugangsrechten eingeschränkt und gesteuert werden.</td></tr>
<tr><td>Verantwortlicher:

Verwalter administrativer Zugangsrechte/Rechenzentrumleiter</td><td>Mitwirkende Personen:

Mitarbeiter/Antragssteller, Genehmiger</td></tr>
<tr><td colspan="2">Input: Antragsstellung für die privilegierter Zugangsrechte</td></tr>
<tr><td colspan="2">Output: Aktualisiertes Verzeichnis, in dem alle Zugangsrechte gepflegt sind</td></tr>
<tr><td colspan="2">Anforderungen: Die Anwendungen und Benutzer, denen privilegierte Zugangsrechte zugeordnet werden, sind zu identifizieren.

Privilegierte Zugangsrechte sollen einem Benutzer im Bedarfsfall für die Ausführung seiner dienstlichen Aufgaben zugeteilt werden.</td></tr>
<tr><td colspan="2">Mitwirkende Dokumente: Zugangssteuerungsrichtlinien, Berechtigungsantrag</td></tr>
<tr><td colspan="2">Schnittstellen des Prozesses: Registrierung und Deregistrierung von Benutzern</td></tr>
</table>

Quelle: Firuza Muhamadova

4.2.4 Verwaltung geheimer Authentisierungsinformationen von Benutzern

Der vierte Teilprozess der Benutzerzugangsverwaltung ist die Verwaltung geheimer Authentisierungsinformationen. Das Wort „Authentisierung“ bezeichnet einen Vorgang, bei dem der Benutzer seine Identität nachweisen soll. Durch ihn wird beabsichtigt, dass die dazu erlaubten User einen Zugang zu den informationsverarbeitenden Einrichtungen und Informationen haben. Ein dazu unbefugter User darf keinen Zugang zu diesen Ressourcen erhalten.

Je nach Auswahl der Authentisierungsmittel werden unterschiedliche Arten vom Identitätsnachweisen bzw. Authentisierungsinformationen verwendet, welche das gleiche Ziel verfolgen.

- Authentisierung durch ein Passwort

  Dies gehört zu der üblichen Art einer Identitätsbestätigung. Dabei benutzt der befugte Benutzer ein Passwort, um in das System oder in die Einrichtung einzutreten. Im Hintergrund des Anmeldungsprozesses läuft ein automatisiertes Verfahren ab. Es überprüft in einer Datenbank alle Benutzer und deren Passwörter. Wenn die Suche erfolgreich abgelaufen ist, kann der Benutzer in das System zugelassen werden. Das bedeutet, der Benutzer und sein Passwort wurden in der Datenbank gefunden und er ist berechtigt, einen Zugang in das System zu haben.

  Die Passwörter dienen für den Schutz eines Systems, Ortes oder eines Dienstes. Daher ist es wichtig, starke Passwörter zu definieren. Es ist nicht erlaubt, existierende Wörter als Passwörter zu benutzen. Ein definiertes Passwort soll in einem Wörterbuch nicht zu finden sein.
- Authentisierung durch Smart Card

  Smart Cards sind Chipkarten mit den Informationen über die Identität eines Benutzers. Um einen Zugang zu bekommen, soll der User die Chipkarte in das Gerät einstecken oder durchziehen. Nach der automatischen Erkennung seiner Daten soll er seinen PIN eingeben.

  Die Chipkarten basieren sich auf dem kryptischen Verfahren und gewähren dadurch große Sicherheit.
- Biometrische Authentisierung

  Diese benutzt die eindeutigen biologischen Eigenschaften eines Menschen, um ihn zu identifizieren. Solche einzigartigen Eigenschaften können die Stimme, der Fingerabdruck oder die Netzhaut sein.

  Die biometrischen Authentisierungsgeräte scannen die oben erwähnten Eigenschaften ein. Dadurch zeichnen sie sich als eine komplexe Methode aus. (www.techrepublic.com, 2018)

Die ISO 27002 beschreibt die Vorgaben für die Verwaltung der Authentisierungsinformationen. Dementsprechend soll ein Prozess mit den folgenden Aktivitäten durchgeführt werden, um die Verwaltung der Authentisierungsinformationen sicherzustellen.

Authentisierungsinformationen anfordern

Der Verwaltungsprozess geheimer Authentisierungsinformationen startet mit der Forderung der Authentisierungsinformation von einem Benutzer.

Benutzeridentität überprüfen

Vor der Zustellung neuer Authentisierungsinformation überprüft der Administrator die Identität des Benutzers. Mit der Identitätsprüfung werden alle bisherigen geheimeren Authentisierungsinformationen des Benutzers kontrolliert.

Darüber hinaus soll in diesem Vorgang festgestellt werden, ob der User die Authentisierungsinformationen selber verwalten darf oder nicht.

Temporäre Authentisierungsinformationen bereitstellen

Eine temporär gültige Authentisierungsinformation wird angelegt, wenn der User seiner geheimen Authentisierungsinformation selbst verwaltet. In diesem Fall soll die Authentisierungsinformation geändert werden, nachdem sie einmal benutzt wurde. Die temporären Authentisierungsinformationen sind also einmalig zu verwenden.

Temporäre Authentisierungsinformationen übermitteln

Da es bei einem Passwort bzw. einer Authentisierungsinformation um die sensible Daten geht, sollen die deshalb durch die sicheren Kommunikationskanäle übermittelt werden. Der verschlüsselte Nachrichtenaustausch ist dafür sehr geeignet.

Empfang von Authentisierungsinformationen bestätigen

Nachdem der Benutzer eine Authentisierungsinformation bekommen hat, soll er den Empfang bestätigen.

Temporäre Authentisierungsinformationen ändern

Da eine temporäre Authentisierungsinformation einmal verwendet werden kann, soll diese nach erster Benutzung geändert werden.

Authentisierungsinformationen verwalten

Falls ein Benutzer für die Verwaltung seiner geheimen Authentisierungsinformation nicht berechtigt ist, wird die Authentisierungsinformation von dem Administrator verwaltet. Unter der Berücksichtigung von Berechtigungen kann die geheimen Authentisierungsinformationen entweder von dem User selbst oder von Administrator verwaltet. Daher können sowohl der Benutzer als auch der Administrator als Prozessverantwortlicher dargestellt werden.

Authentisierungsinformationen dokumentieren

Am Ende des Prozesses werden die Authentisierungsinformationen dokumentiert. (DIN, ISO/IEC 27002, 2015, S. 35-36)

Im weiteren Verlauf dieses Abschnittes folgen das Prozessmodell und die Prozessbeschreibung.

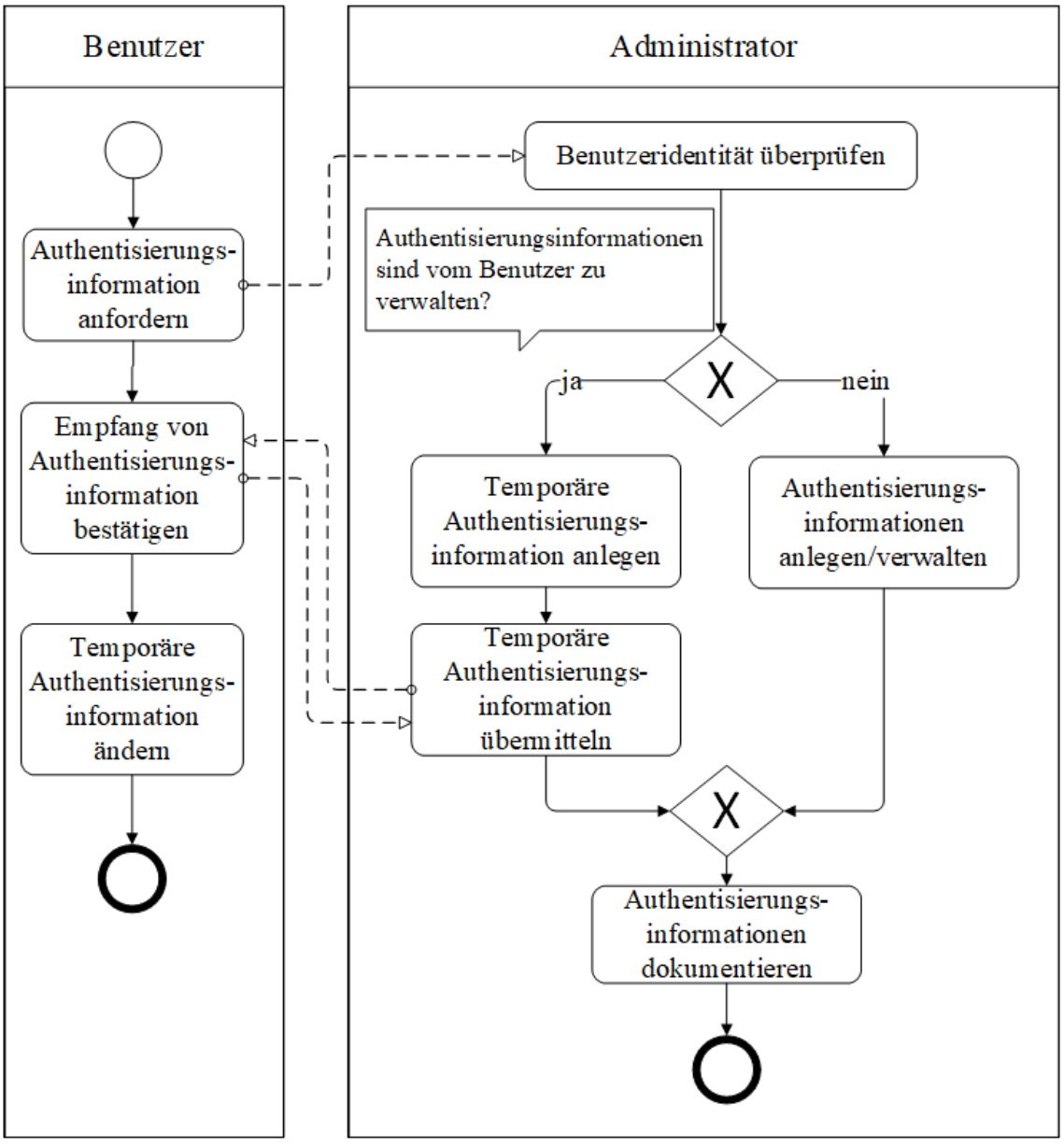

Abbildung 13:Prozessmodell der Verwaltung geheimer Authentisierungsinformationen.

Quelle: Firuza Muhamadova

Tabelle 5: Prozessbeschreibung der Verwaltung geheimer Authentisierungsinformationen.

Prozessname: Verwaltung geheimer Authentisierungsinformationen

Zweck: Mit der Umsetzung des Prozesses soll die Zuordnung geheimer Authentisierungsinformationen gesteuert werden.	
Verantwortlicher: Administrator, Benutzer geheimer Authentisierungsinformation	**Mitwirkende Personen:**
Input: Anforderung der Authentisierungsinformationen	
Output: Die Authentisierungsinformationen sind durch die sorgfältige Aufbewahrung vor ihrem Verlust geschützt.	
Anforderungen: Es solle die starken Passwörter angelegt werden. Bei der Verwendung temporärer Authentisierungsinformationen sollen die User angefordert werden, die Authentisierungsinformation zu ändern.	
Mitwirkende Dokumente: Unterzeichnete Erklärung für den sorgfältigen Umgang mit Authentisierungsinformationen, verschlüsselte Nachrichten	

Quelle: Firuza Muhamadova

4.3 Betriebssicherheit

Informationstechnische Systeme (IT-Systeme) sind heute das wesentliche Mittel für die tägliche Informationsverarbeitung einer Organisation. Zu den typischen IT-Systemen gehören Server, Clients, Rechner, End- und Mobilgeräte.

Da die IT-Systeme eine wichtige Rolle für ein Unternehmen spielen, sind sie gleichzeitig ein interessantes Angriffsziel für Hacker. Bewertet man die möglichen Bedrohungen für IT-Systeme, stellt man schnell fest, dass nicht nur die Hackerangriffe selbst, sondern auch die fehlende Mitarbeiterkompetenz eine grundlegende Gefahr für die Betriebsfähigkeit der IT-Systeme darstellt. Das heißt, zuerst einmal sollten die Mitarbeiter einer Organisation für die Sicherheitsthemen sensibilisiert und die Verantwortlichkeiten für die Betriebsabläufe festgestellt sein, wenn es um die Sicherheit der IT-Systeme geht.

Die ISO/IEC 27001 und 27002 geben die erforderlichen Maßnahmen vor, damit die Betriebssicherheit der Systeme beziehungsweise der IT-Infrastruktur sichergestellt ist.

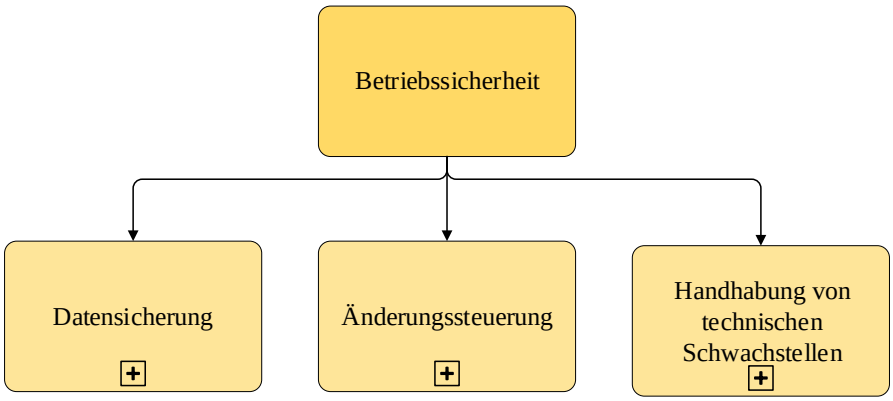

Abbildung 14:Betriebssicherheitsprozess mit den dazugehörigen Unterprozessen

Quelle: Firuza Muhamadova

Dieses Kapitel beinhaltet die Umsetzungsvorgaben von Maßnahmen für das Änderungsmanagement, die Datensicherung und die Handhabung technischer Schwachstellen. Darüber hinaus werden die wesentlichen Informationen über die Schadsoftware ermittelt. Außerdem ist bei der Durchführung des Betriebssicherheitsprozesses das Thema Informationssicherheitsvorfälle zu beachten, weil die Vorfälle Auslöser der Betriebsunfähigkeit von Informationssystemen sein können. (DIN, ISO/IEC 27002, 2015)

4.3.1 Datensicherung

Ein Backup steht für die Sicherheitskopien von Daten und Datenbanken. Die Informationen, Software und Systemabbilder werden kopiert, damit sie bei Notfällen oder Systemausfällen wiederhergestellt werden können. Dafür ist ein Datensicherungskonzept erforderlich.

Im Prozess „Datensicherung“ sind die benötigten Schritte für die Datensicherungsausführung enthalten.

Datensicherungsrichtlinien erstellen/anpassen

Ein wichtiger Vorgang ist dabei das ausführliche Dokumentieren der Datensicherung. Die Dokumentation soll ein genaues Bild der Vorgehensweise von Backups ergeben. Außerdem ist schriftlich festzulegen, wie eine Wiederherstellung der Informationen geschehen kann.

Eine Priorisierung der Systeme und Informationen ermöglicht es, den Umfang und die Häufigkeit der Datensicherung zu bestimmen. Alle betriebsrelevanten Anwendungen, Systeme und Daten werden bei der Sicherung zuallererst berücksichtigt.

Datensicherung planen

In diesem Vorgang plant der Administrator die Durchführung der Datensicherung entsprechend der festgelegten Datensicherungsrichtlinien

Sicherheitskopien erstellen

Nachdem die Vorbereitungsmaßnahmen für die Datensicherung getroffen sind, können die Sicherheitskopien von Information, Anwendungen und Systemen erstellt werden.

Datensicherungen überprüfen/überwachen

Für die Gewährleistung der Verwendung von Sicherheitskopien im Notfall sind nicht nur die Sicherheitskopien selbst, sondern auch die Medien, auf denen die Kopien gespeichert sind, regelmäßig zu überprüfen. Mit der Überprüfung soll festgestellt werden, ob die umgesetzten Datensicherungsvorkehrungen die Organisationsanforderungen hinsichtlich der Betriebskontinuität erfüllen. Es werden zum Beispiel untersucht, ob die festgelegte Häufigkeit und Umfang des Backups genüg sind, um Daten schützen zu können.

Datensicherungsmangeln melden

Falls die Sicherheitskopien mangelhaft sind oder den Organisationsanforderungen nicht entsprechen, werden diese der zuständigen Personen gemeldet, die für die Feststellung der Datensicherungsrichtlinien verantwortlich sind.

Datensicherung aufbewahren/schützen

Es empfiehlt sich, die Sicherheitskopien an einem externen Ort zu bewahren. Falls die ursprünglichen Informationen einmal angegriffen werden und nicht mehr verwendbar sind, können die Kopien aus diesen externen Speicherstellen benutzt werden.

Zusätzlich sind die Sicherungskopien mit dem Verschlüsselungsverfahren zu schützen.

Das nachfolgende Prozessmodell stellt den ganzen Datensicherungsprozess in BPMN dar. Im Weiteren sind die wichtigen Merkmale des Datensicherungsprozesses in Form einer Tabelle beschrieben. (DIN, ISO/IEC 27002, 2015, S. 60-61)

Tabelle 6: Prozessbeschreibung der Datensicherheit

Prozessname: Datensicherung	
Zweck: „Daten sind vor Verlust geschützt“	
Verantwortlicher: Administrator	**Mitwirkende Personen:** Rechenzentrumleiter, alle für die Datensicherung zuständigen Personen
Input: Datensicherungsrichtlinien	

Output: Geschützte Sicherheitskopien der Informationen, Systeme und Anwendungen
Anforderungen: Gemäß den definierten Datensicherungsrichtlinien sollen die Sicherheitskopien der Informationen, Systeme und Anwendungen erstellt und ständig getestet werden.
Mitwirkende Dokumente: Datensicherungsrichtlinien, Business-Continuity-Pläne
Schnittstellen des Prozesses: Änderungssteuerung, Handhabung von Informationssicherheitsvorfällen

Quelle: Firuza Muhamadova

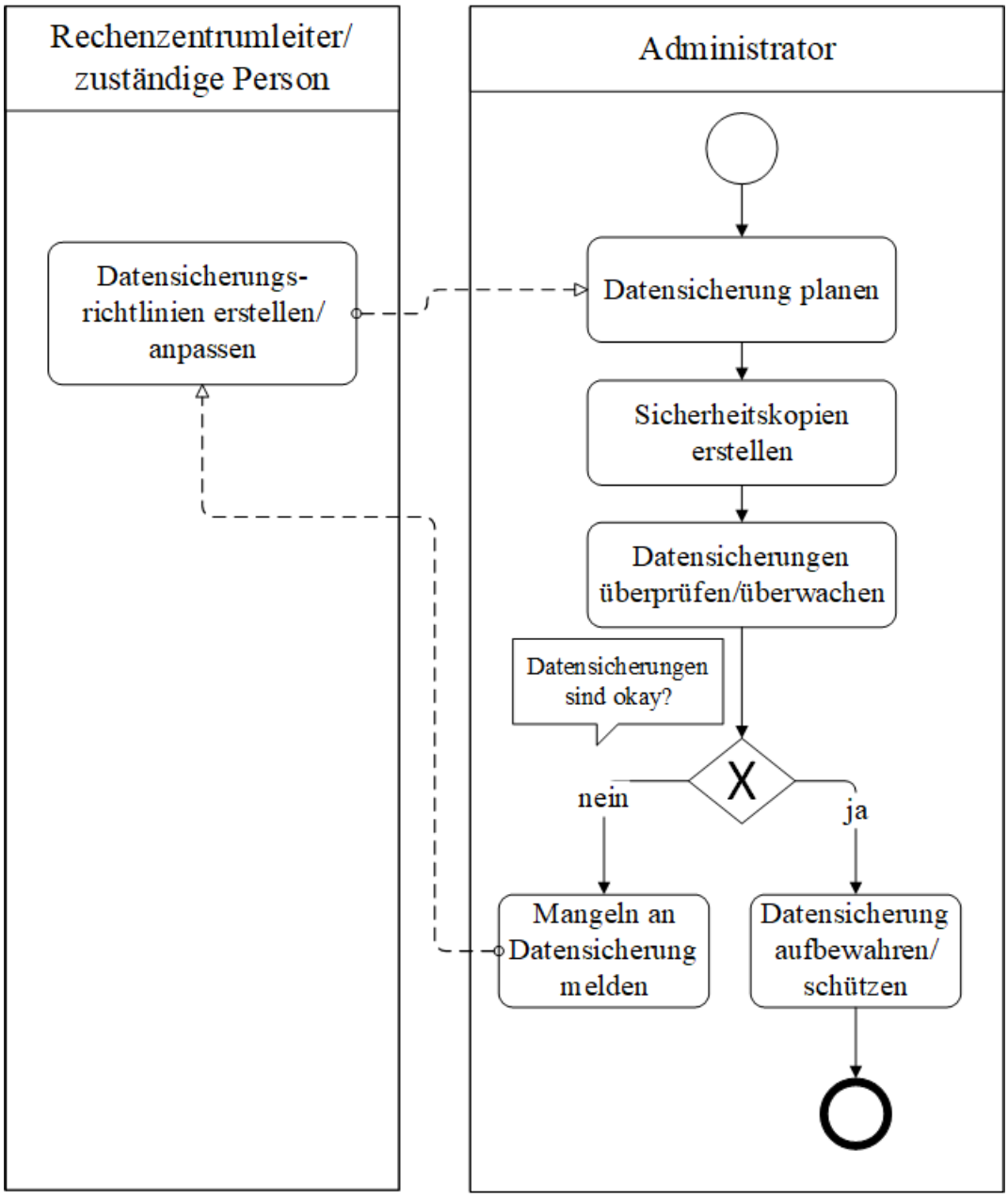

Abbildung 15: Prozessmodell der Datensicherung
Quelle: Firuza Muhamadova

4.3.2 Änderungssteuerung

Jede Organisation hat das Ziel, ihre Existenz und Wettbewerbsfähigkeit dauerhaft sicherzustellen. Aus diesem Grund ist sie dazu verpflichtet, auf die vom Markt bestimmten Voraussetzungen schnell zu reagieren. Oft lässt sich diese Herausforderung mithilfe der Durchführung von erforderlichen Änderungen bewältigen.

Die marktbedingten Veränderungen können die Struktur, Strategie oder Arbeitskultur eines Unternehmens sowie dessen IT-Systeme betreffen.

Nicht nur die Anpassung an die neuen Voraussetzungen an sich ist von großer Bedeutung, sondern die Veränderungen sollen dem Unternehmen auch einen Nutzen bringen. Daher soll jede einzelne Änderung durch einen Change-Management-Prozess gesteuert werden.

Die ISO/IEC 27002 stellt eine Anleitung für die Umsetzung der geforderten Maßnahmen bereit, indem die Änderungen der Organisation, der Geschäftsprozesse und an den informationsverarbeitenden Einrichtungen verwaltet werden. Die Hauptaufgaben sind dabei die Vermeidung und Reduzierung der möglichen Risiken, welche durch die Veränderungen ausgelöst werden können. Der Prozess „Änderungssteuerung“ umfasst alle Vorgänge, die für die Durchführung der erfolgreichen Informationssystems- und Organisationsänderungen benötigt werden.

Änderungen festlegen/protokollieren

Im ersten Schritt sollen die vorzunehmenden Änderungen festgelegt werden. Die wichtigste Frage ist dabei, was genau geändert werden soll. Es empfiehlt sich, die beabsichtigte Änderungen immer zu dokumentieren.

Risiko beurteilen

Als Nächstes gilt es herauszufinden, welche Auswirkungen die Änderungen verursachen können. Was sind die denkbaren Folgen, wodurch die Informationssicherheit beeinträchtigt werden könnte? Als Beispiele zu den möglichen Auswirkungen zählen die Verlangsamung der Systeme, die Entstehung unbekannter Schwachstellen oder fehlende Kompetenz und fehlende Einarbeitungsmaßnahme für die neuen Veränderungen.

Änderungen vorschlagen

Zur Vermeidung der Risiken ist es erforderlich, dass die Änderungen nicht allein von einem Administrator vorgenommen und durchgeführt werden. Jede Änderung sollte im Detail mit den Experten oder dafür zuständigen Mitarbeiterinnen und Mitarbeitern besprochen werden.

Änderungsvorschläge überprüfen

Die Änderungsvorschläge sollen von Experten oder für die Änderung zuständigen Personen überprüft werden. Dabei ist es nicht außer Betracht zu lassen, ob die beabsichtigten Änderungen den Informationssicherheitsanforderungen entsprechen. Nach diesem Kriterium können die Änderungen entweder durchgeführt oder abgelehnt.

Änderungen genehmigen

Die Durchführung der Änderungen wird genehmigt, wenn sie die Informationssicherheitsanforderungen angemessen sind.

Änderungen ablehnen

Im anderen Fall werden die vorgeschlagenen Änderungen abgelehnt, wenn sie die Anforderungen hinsichtlich der Informationssicherheit nicht erfüllen. Mit der Ablehnung wird der Änderungssteuerungsprozess abgebrochen.

Änderungen planen

In diesem Vorgang werden die Vorbereitungsmaßnahmen für die Ausführung einer Änderung durchgeführt.

Rollback definieren

Zusätzlich sollen auch alternative Maßnahmen geplant sein, wenn die durchgeführten Änderungen nicht das beabsichtigte Ergebnis liefern. In diesem Fall werden die Änderungen rückgängig gemacht oder der Änderungsvorgang abgebrochen.

Darüber hinaus wird ein Notfallprozess definiert, falls die Informationssicherheitsvorfälle durch die Veränderungen ausgelöst werden. In diesem Fall ist es erforderlich, auf die aufgetretenen Vorfälle in geeigneter Weise zu reagieren. Kapitel 4.2 liefert detaillierte Informationen darüber, was unter dem Begriff Informationssicherheitsvorfall zu verstehen ist und wie sich diese umgehen lassen.

Änderungen dokumentieren

Gemäß den Vorgaben von ISO/IEC 27002 sind alle Informationen bezüglich der Änderungen in einem Audit-Protokoll festzuhalten. (DIN, ISO/IEC 27002, 2015, S. 56)

Anhand des folgenden Prozessmodells lassen sich die bereits beschriebenen Vorgängen graphisch darstellen.

Einen Überblick über die bildliche Prozessdarstellung liefert die nachfolgende Abbildung.

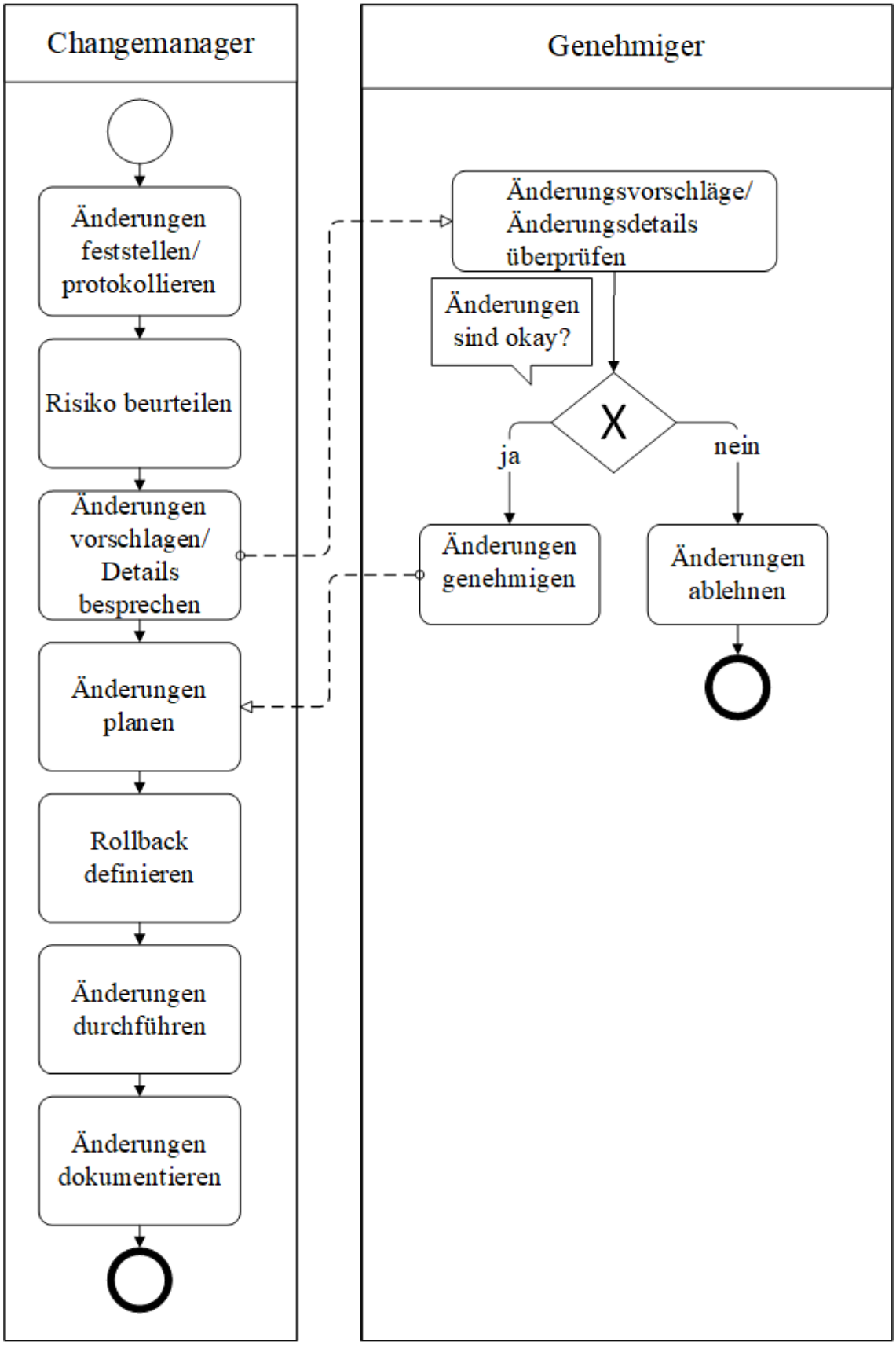

Abbildung 16:Prozessmodell der Änderungssteuerung

Quelle: Firuza Muhamadova

Die weiteren Prozessdetails lassen sich mithilfe der folgenden Tabelle darstellen.

Tabelle 7: Prozessbeschreibung der Änderungssteuerung

Prozessname: Änderungssteuerung	
Zweck: Die Steuerung der Änderungen von Organisation, Geschäftsprozessen, informationsverarbeitenden Einrichtungen und Systemen, um die System- oder Sicherheitsausfälle zu vermeiden.	
Verantwortlicher: Changemanager	**Mitwirkende Personen:** Genehmiger, alle relevanten Personen
Input: Erforderliche Änderungen	
Output: Dokumentation der durchgeführten Änderungen	
Anforderungen: Für die Sicherstellung aller Änderungen sollen die Verantwortlichkeiten und Verfahren für die Handhabung der Veränderungen festgelegt sein.	
Mitwirkende Dokumente: Richtlinien der Organisation für das Changemanagement	
Schnittstellen des Prozesses: Handhabung von Informationssicherheitsvorfällen, Risikomanagement	

Quelle: Firuza Muhamadova

4.3.3 Schutz vor Schadsoftware

Zu einer der beliebtesten Angriffsmethode gehört die Schadsoftware. Für die Gewährleistung des kontinuierlichen Betriebs von ISMS ist erforderlich, die bekannten Typen der Schadsoftware zu wissen und sich mit ihrer Vorgehensweise vertraut zu machen.

Schadsoftware bezeichnet diejenigen Programme, welche speziell entwickelt worden sind, um Geräte oder Systeme zu beschädigen.

Der deutsche Digitalverband Bitcom e.V. berichtete über die Bedrohungen, die die Sicherheit der Geräte und Daten durch Schadsoftware gefährden können.

- Trojaner und Würmer zählen zu einer weitverbreiteten Art von Schadsoftware. Die Gemeinsamkeit zwischen Trojanern und Würmern besteht darin, dass sie der User des Gerätes nicht bemerkt. Ein Trojaner oder „trojanisches Pferd“ führt die schädlichen Aktionen im betroffenen Gerät aus. Trojaner können die sensiblen Daten manipulieren, indem sie Daten ändern oder löschen.

Die Würmer nutzen die Möglichkeit der Internetverbindung aus, um die Geräte zu infizieren. Die infizierten Rechner dienen als Opferobjekte, wodurch der Hacker sein Ziel erreichen kann.

- Botnetz beschreibt eine Reihe der infizierten Computer. Zuerst findet die Infizierung an einem Rechner statt und sie verbreitet sich nach und nach auf weitere Geräte.

  Ein (unbewusstes) Klicken auf einen in der Spam-E-Mail mitgeschickten Link oder das Herunterladen von Apps und Software aus nicht vertrauenswürdigen Webseiten sind die bekanntesten Ursachen zur Übertragung von Schadsoftware. Die Botnetze werden für die Ausspionierung der sicherheitsrelevanten Informationen wie Passwörter verwendet.
- Denial-of-Service-Attacken sind eine Bedrohung, die die Verfügbarkeit eines Systems betrifft. Der Angreifer schickt dabei mehr Datenpakete oder Abfragen, als der Server eigentlich bearbeiten kann. Dies führt zur Auslastung des Servers. Ein oder mehrere durch das Schadprogramm infizierte Rechner sind dann die Grundlage für die Ausführung von Denial-of-Service-Attacken.

Tausende Organisationen sind jährlich weltweit von den Angriffen betroffen, die mithilfe von Schadsoftware durchgeführt werden. Manche Schadprogramme sind sogar sehr geschickt entwickelt und bleiben auf den Computern oder Computersystemen unentdeckt und haben schwerwiegende Schäden zur Folge. (www.bitkom.org/, 2018)

Damit die Betriebsabläufe sicher und ordnungsgemäß ablaufen können, ist es wichtig, dass die Informationen und die informationsverarbeitenden Einrichtungen vor Schadsoftware geschützt sind.

Der Standard ISO/IEC 27002 und 27001 setzt für den Schutz vor Schadsoftware voraus, die Benutzer von Informationen dahingehend zu sensibilisieren. Die Durchführung unzähliger Maßnahmen und Verfahren ist wenig erfolgreich, wenn die Benutzer die Wichtigkeit der Datensicherheit nicht verstehen oder mit dem Schadsoftwareschutz nicht umgehen können. Die Organisationen sollen ermöglichen, dass ihre Beschäftigten an Schulungen teilnehmen oder durch andere Quellen über das Thema informiert werden, damit ihr Kenntnisstand darüber aktuell bleibt.

4.3.4 Handhabung von technischen Schwachstellen

Die Schwachstellen sind die ursprünglichen Quellen für die Informationssicherheitsrisiken. Eine potenzielle Bedrohung, zum Beispiel durch eine Malware-Attacke, kann erst nach der Erkennung einer Schwachstelle erfolgen. Das

bedeutet: Es muss eine Schwachstelle vorhanden gewesen sein, damit die Malware-Attacke durchgeführt werden konnte.

Oft werden die Schwachstellen mit der Schadsoftware verwechselt. Deshalb denken viele Unternehmen, dass die Einführung von Schadsoftware-Erkennungsprogrammen wie Antivirenprogrammen für die Bekämpfung von Schwachstellen ausreichend sei.

Die Schwachstellen umfassen nicht nur technische, sondern auch organisatorische Fehler. Zu den typischen Schwachstellen gehören Fehler in der Anwendungssoftware oder in Systemkonfigurationen und in fehlenden Software-Updates. Die Schwachstellen liegen also nicht bei der Schadsoftware, sondern bei den Fehlern in der Handhabung.

Auf Basis der Schwachstellen vorkommende Angriffe bedeuten eine große Gefahr für die Organisationen. Aus diesem Grund ist es sehr wichtig, die Lücken oder Fehler in den Informationssystemen zu beseitigen, bevor man sich mit deren Ursachen und Bedrohungen beschäftigt. (www.security-insider.de, 2018)

Alle verfügbaren Assets der Organisation mit ihren zugehörigen Informationen sollen inventarisiert sein, bevor man mit dem eigentlichen Prozess für die Handhabung der Schwachstellen startet. Die Inventarisierung ist damit die wesentliche Quelle für die Feststellung der technischen Schwachstellen, indem sie die nötigen Daten zu Software-Anbietern, Software-Versionsnummer und zuständigen Personen liefert.

Der Prozess „Handhabung von technischen Schwachstellen“ wird durchgeführt, um die Schwachstellen und ihre Auswirkungen zu früh wie möglich erkennen und die Schwachstellenrisiken zu behandeln.

Schwachstellen erkennen/überwachen

Für die Erkennung der Schwachstellen empfiehlt es sich, die Schwachstellen-Erkennungsprogramme zu verwenden. Diese dienen zur Feststellung der Softwarefehler, durch die eine Sicherheitslücke entstehen kann.

Risiken bewerten

Die Risikobewertung bezüglich einer Schwachstelle ist ein wichtiger Vorgang, wodurch die Schwachstellen priorisiert und entsprechende Gegenmaßnahmen umgesetzt werden können. Die Fragestellung lautet dabei: Welche Risiken können die Schwachstellen hervorrufen?

Gegenmaßnahmen definieren

Um die Auswirkungen zu vermeiden oder zu reduzieren, welche Schwachstellen verursachen können, sind die Gegenmaßnahmen zu definieren. Für die Gegenmaßnahmen können die Verwendung der Patches, Abschaltung der Dienste bzw. Funktionen, Anpassung der Zugriffssteuerung als Beispiele dienen.

Je nach Verfügbarkeit können entweder Patches oder Alternativmaßnahmen für die Schwachstellenbehandlung angewendet werden.

Patches suchen

Zur Behandlung einer gemeldeten Schwachstelle wird in den meisten Fällen ein Patch vom Anbieter der betroffenen Software zur Verfügung gestellt. Die Patches sind von einer vertrauenswürdigen Webseite herunterzuladen.

Patches testen/überprüfen

Die Aufgabe der Organisation, welche die lückenhafte Software anwendet, ist es dabei, den fertigen Patch gründlich zu überprüfen.

Der Patch-Anbieter steht oft unter Zeitdruck und versucht, so schnell wie möglich einen Patch fertigzustellen, nachdem eine Schwachstelle in einer von ihm entwickelten Software bekannt geworden ist. Daher kann es vorkommen, dass der Patch selber fehlerhaft ist. Durch das Testen des Patches können seine Nebeneffekte erkannt werden.

Risiken bewerten

Zusätzlich soll eine Risikobeurteilung durchgeführt werden, bevor der Patch installiert wird. Dabei untersucht der Prozessverantwortlicher, ob die Installation oder Durchführung des Patches irgendeine Auswirkung mitbringen kann. Die durch die Schwachstellen auslösende Risiken werden gegenüber den Risiken der Installation von Patches verglichen. Die zentralen Fragen, die mit der Durchführung der Risikobewertung beantwortet werden sollen, im Folgenden beschrieben.

- Welche Risiken können durch die Verwendung des Patches entstanden werden?
- Sind die Risiken des Patches geringer als die Risiken der Schwachstelle?

Alternativmaßnahmen bestimmen

Alternativmaßnahmen sind durchzuführen, falls kein Patch zur Verfügung steht oder aufgrund seiner hohen Risiken nicht verwendet werden kann.

Gegenmaßnahmen melden

Die durchzuführenden Gegenmaßnahmen sollen zur Genehmigung vorgelegt werden, bevor sie umgesetzt werden.

Gegenmaßnahmen überprüfen

Die Gegenmaßnahmen werden hinsichtlich der Anforderungen von Organisation und Informationssicherheit überprüft.

Gegenmaßnahmen genehmigen

Falls die Gegenmaßnahmen die Anforderungen erfüllen, dann erfolgt eine Genehmigung zu ihrer Durchführung

Gegenmaßnahmen ablehnen

Im anderen Fall werden die Gegenmaßnahmen abgelehnt.

Gegenmaßnahmen durchführen

Wenn eine Schwachstelle bereits bekannt ist, soll ein bestimmter Zeitraum festgelegt werden, um darauf schnellstmöglich zu reagieren. Eine schnelle Reaktion verhindert die Ausnutzung der entdeckten Schwachstelle seitens des Angreifers.

Wirksamkeit bewerten

Mit der Umsetzung der Gegenmaßnahmen zu Schwachstellenbehandlung ist der Prozess Handhabung von Schwachstellen noch nicht beendet. Zunächst werden die durchgeführten Gegenmaßnahmen bezüglich ihrer Wirksamkeit überprüft.

Verfahren protokollieren

Zuletzt sind alle Prozessaktivitäten in einem Audit-Protokoll zu dokumentieren.

Im weiteren Verlauf dieses Abschnittes folgen das Prozessmodell und die Prozessbeschreibung. (DIN, ISO/IEC 27002, 2015, S. 65-66)

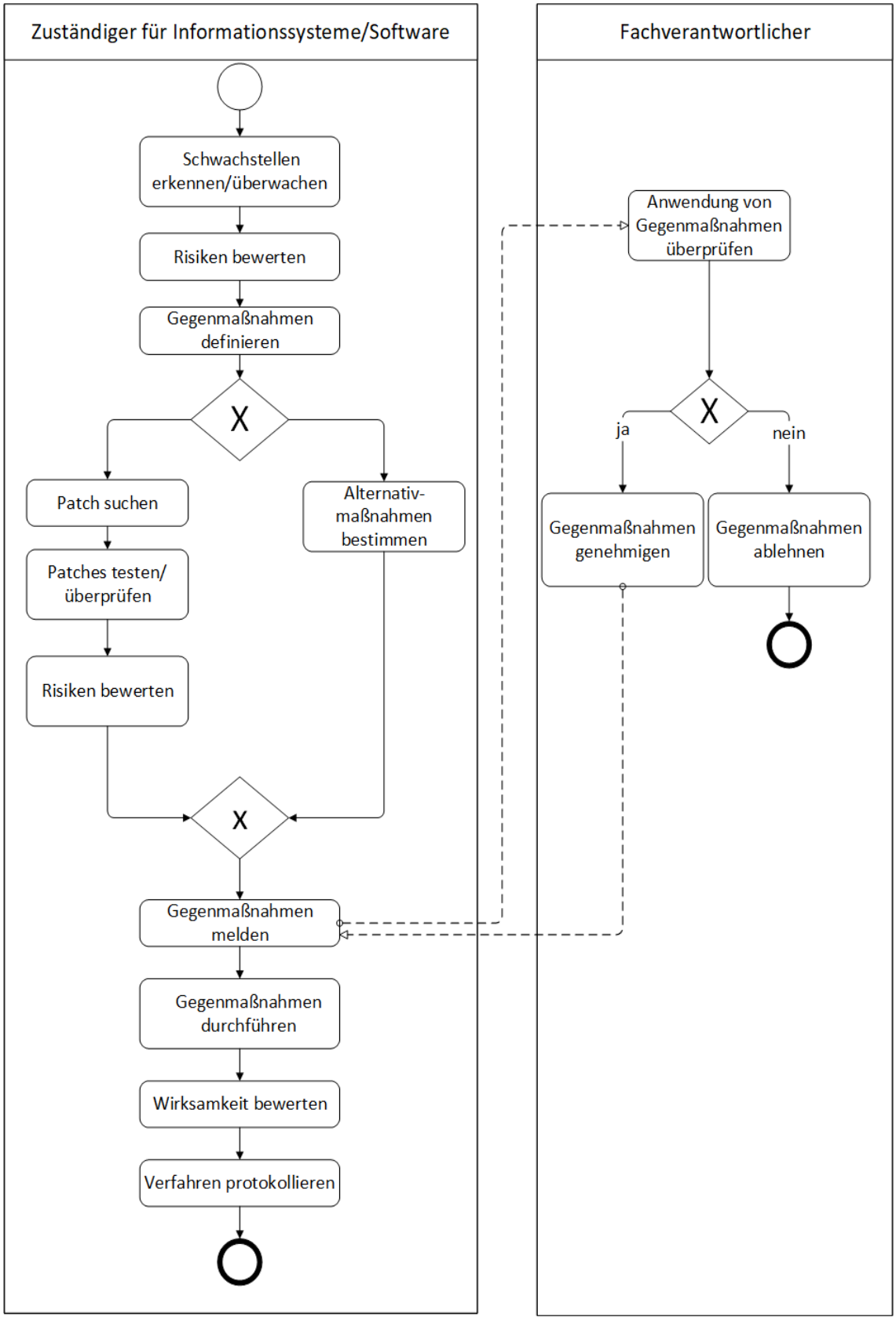

Abbildung 17: Prozessmodel der Handhabung von technischen Schwachstellen

Quelle Firuza Muhamadova.

Tabelle 8: Prozessbeschreibung der Handhabung von technischen Schwachstellen

Prozessname: Handhabung von technischen Schwachstellen	
Zweck: „Die Ausnutzung technischer Schwachstellen ist verhindert“	
Verantwortlicher: Zuständiger für Informationssysteme/Software	**Mitwirkende Personen:** Fachverantwortlicher, Softwareanbieter
Input: Fehler in Software oder Systemeinrichtungen	
Output: Dokumentierte Vorgehensweise zu Schwachstellenbehandlung, behandelte Schwachstellen	
Anforderungen: Die Informationen über einen bekannten Schwachstellen sollen rechtzeitig eingeholt werden, um die möglichen Auswirkungen der Schwachstellen bewerten und entsprechende Gegenmaßnahmen zur deren Handhabung umsetzen zu können.	
Mitwirkende Dokumente: Inventarliste von Assets; Audit-Protokolle	
Schnittstellen des Prozesses: Änderungssteuerung, Handhabung von Informationssicherheitsvorfällen, Risikomanagement	

Quelle: Firuza Muhamadova

4.4 Handhabung von Informationssicherheitsvorfällen

Die Beschäftigung mit Informationssystemen und -technologien verlangt eine hohe Affinität zu dem Tätigkeitsbereich und ein hohes Bewusstsein über Sicherheitsverfahren. Mit solchen Fähigkeiten beweisen die Personen, die täglich mit den Informationen oder deren Systemen arbeiten, ihre Qualifizierung für diesen Bereich. Ein qualifizierter Beschäftigter kann zum Beispiel sofort eine Phishing-Mail erkennen. Außerdem weiß er genau, wie er in diesem Fall reagieren soll.

Je nach sicherheitsspezifischer Kompetenz eines Mitarbeiters für Informationen kann eine unbewusste Aktivität seinerseits ganze Organisationen stilllegen.

Daher beschäftigt sich der Standard ISO/IEC 27002 mit der Beschreibung der Wichtigkeit von richtigen Reaktionen, welche von den Beschäftigten und Auftragnehmern einer Organisation erfolgen sollen. Demnach sollen die Beschäftigten in der Lage sein, die Informationssicherheitsereignisse und -vorfälle zu erkennen und sie schnellstmöglich dem zuständigen Team zu melden. In den meisten Fällen wird es ein Expertenteam geben, das sich um die Analyse und Behandlung von solchen Vorfällen kümmert, das sogenannte Computer Security Incident Response Team (CSIRT).

4.4.1 Diskussion der wichtigen Begrifflichkeiten

Bevor die einzelnen Aktivitäten der Handhabung von Informationssicherheitsvorfällen und die dabei an die Beschäftigten gesetzten Bedingungen erläutert werden, erfolgt hier zuerst eine Diskussion über die Begrifflichkeiten Informationssicherheitsvorfall und -ereignis.

Laut ISO/IEC 27001 sind Informationssicherheitsvorfall und Informationssicherheitsereignis unterschiedlich definiert, wohingegen sie in anderen Quellen synonym verwendet werden.

Der Informationssicherheitsvorfall bezeichnet nach ISO-Standard eine Situation, in der unbekannte und ungewollte Ereignisse auftreten und diese die Integrität, Verfügbarkeit und Vertraulichkeit der Informationen oder Systeme gefährden. Dieser Vorfall ist unmittelbar mit finanziellem Schaden für die Organisation verbunden.

Das Informationssicherheitsereignis beschreibt dabei das Auftreten sowohl eines bereits bekannten als auch eines unbekannten Ereignisses. Als die möglichen Auslöser zählen dafür Nichteinhaltung oder Verstöße gegen Richtlinien und Unwirksamkeit der vorgenommenen Maßnahmen. Im Folgenden werden die möglichen Sicherheitsereignisse aufgezählt.

- Erscheinung der bekannten Computerviren
  Den Zuständigen ist die Art und Funktion der aufgetauchten Viren bekannt. Dementsprechend wurden bereits die Sicherheitsmaßnahmen definiert. Die Gegenmaßnahmen können durchgeführt werden, bevor die Viren das betroffene System oder Netzwerk schädigen.
- Erkannte Verletzung der Zutritts- oder Zugriffsregeln
  Angenommen, dass sich ein unbefugter Benutzer für den Zugang zu einem bestimmten System interessiert. Um sein Ziel zu erreichen, versucht der Benutzer das Passwort für das System herauszufinden. Die übliche Methode ist dabei die Eingabe der möglichen Zeichen aus der Tastatur. Die vordefinierten Maßnahmen aktivieren bei mehrmaligen Versuchen mit falschen Passwörtern eine Benutzerkontosperrung.
- Nichteinhaltung der Richtlinien
  Die beabsichtigte oder unbeabsichtigte Nichteinhaltung der Richtlinien wird erkannt und schnell beseitigt, bevor sich negative Folgen zeigen.

Die obigen Erklärungen der wichtigen ISO-Begrifflichkeiten lassen sich wie folgt zusammenfassen: Ein Informationssicherheitsvorfall kann wegen seiner Unbekanntheit einem Unternehmen Schaden bereiten, während ein Informationssicherheitsereignis oft bekannt ist und dessen Schäden sich durch den Einsatz von relevanten Maßnahmen beseitigen lassen.

4.4.2 Der Prozess für die Handhabung von Informationssicherheitsvorfällen

Der Prozess „Handhabung von Informationssicherheitsvorfällen“ befasst sich mit dem Umgang und der Beseitigung von Sicherheitsvorfällen.

Informationssicherheitsvorfälle identifizieren

Der Prozess wird mit der Identifizierung von Informationssicherheitsvorfällen gestartet.

Meldung der Informationssicherheitsereignisse

Bei der Identifizierung von Informationssicherheitsvorfällen spielt die sofortige Meldung der Informationssicherheitsereignisse von den Beschäftigten eine entscheidende Rolle. Denn die Informationssicherheitsereignisse zählen als eine wichtige Quelle für die Vorfälle. Wenn die Ereignisse nicht rechtzeitig gemeldet und Gegenmaßnahmen nicht getroffen werden, können diese finanzielle Verluste verursachen. Daher ist jeder Beschäftigte verpflichtet, bei der Erkennung der Informationssicherheitsereignisse diese sofort dem Zuständigen zu melden.

Die ISO/IEC 27002 empfiehlt, die Rollen und Verantwortlichkeiten für die Handhabung von Informationssicherheitsvorfällen festzulegen. Demnach ist ein Servicedesk für den einzelnen identifizierten Vorfall verantwortlich. Für die Bewertung der Vorfälle wird die Hilfe des Expertenteams CSIRT benötigen.

Risiko beurteilen

Als Nächstes werden die gemeldeten Informationssicherheitsereignisse hinsichtlich ihrer Auswirkung überprüft, welche Risiken dadurch entstehen können. Entsprechend deren Risikolevel sollen diese Vorfälle klassifiziert werden, und zwar mit einer Klassifizierung zwischen „sehr hoch“, „hoch“, „mittel“ und „niedrig“.

Die Reaktion auf die Vorfälle planen

Nach der Klassifizierung von Sicherheitsvorfällen erfolgt die Planung und Vorbereitung der Reaktion. In diesem Vorgang werden die benötigten Aktivitäten für die Beseitigung der Vorfälle geplant und zuletzt die geplanten Aktivitäten durchgeführt.

Informationssicherheitsvorfälle behandeln

Zu den möglichen Reaktionsformen gehört die Eskalation oder die kontrollierte Wiederherstellung.

Erkenntnisse protokollieren

Als Letztes sollen die Erkenntnisse, welche aus der Lösung dieser Vorfälle gewonnen wurden, dokumentiert werden. Die Dokumentation dient der Verhinderung von etwaigen künftigen Informationssicherheitsvorfällen. (DIN, ISO/IEC 27002, 2015, S. 116-119)

Eine graphische Prozessdarstellung ermöglich die folgende auf BPMN basierende Abbildung.

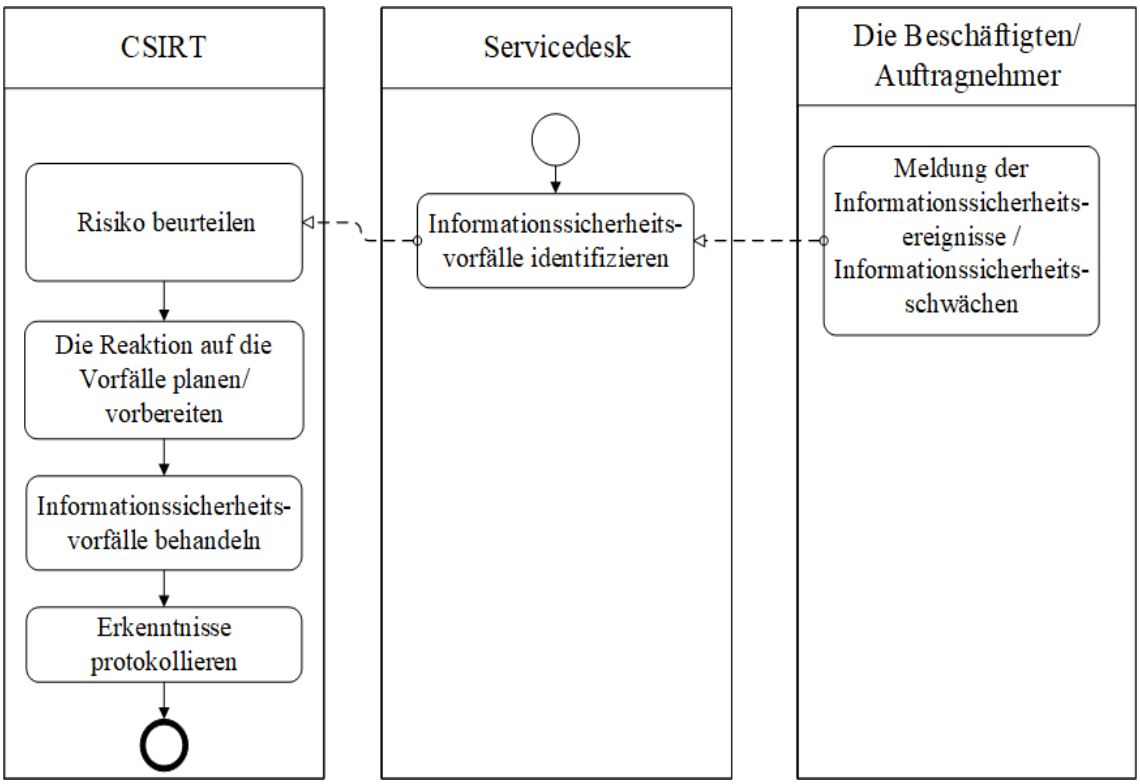

Abbildung 18: Prozessmodell der Handhabung von Informationssicherheitsvorfällen

Quelle: Firuza Muhamadova

Die weiteren Prozessdetails werden durch die Prozessbeschreibungstabelle ermittelt.

Tabelle 9: Prozessbeschreibung der Handhabung von Informationssicherheitsvorfällen

Prozessname: Handhabung von Informationssicherheitsvorfällen	
Zweck: Mit der Umsetzung des Prozesses wird sichergestellt, dass die Informationssicherheitsvorfälle erkannt und behandelt wird.	
Verantwortlicher: Servicedesk	**Mitwirkende Personen:** Beschäftige/Auftragnehmer, CSIRT Team

Input: Gemeldete Informationssicherheitserreignisse/Informationssicherheitsschwächen
Output: Dokumentiertes Verfahren für die Handhabung von Informationssicherheitsvorfällen, behandelte Informationssicherheitsvorfälle
Anforderungen: Die Ziele der Handhabung von Informationssicherheitsvorfällen sollen mit dem Organisationsleiter abgesprochen werden.
Mitwirkende Dokumente: Informationssicherheitsrichtlinien
Schnittstellen des Prozesses: Datensicherung, Risikomanagement

Quelle: Firuza Muhamadova

4.5 Risikomanagement

Dieses Kapitel befasst sich mit der Definition und der regelgemäßen Einführung von Risikomanagement. Das Risikomanagement ist ein wesentlicher Teil des Unternehmensmanagements, welches kontinuierlich durchgeführt werden soll.

Wann wird Risikomanagement verwendet und welche Faktoren spielen für seine Einführung eine Rolle? Wirft man einen Blick hinter die Kulissen, wird die Notwendigkeit des Risikomanagements für eine Organisation sofort klar. Als Erstes müssen hierzu die Begriffe „Risiko“ und „Risikomanagement“ erklärt werden.

Unter dem Risiko im Informationssicherheitsumfeld ist eine Kombination aus der Eintrittswahrscheinlichkeit und Auswirkung einer denkbaren Bedrohung zu verstehen.

Die hier bereits ausgedrückte Komplexität erfordert es, die einzelnen Komponenten eines Risikos genauer zu untersuchen. Eine Bedrohung ist ein unerwünschtes Ereignis, welches einer Organisation Schaden zufügen kann. Zu den typischen Bedrohungsquellen gehören die Natur, Menschen, durch sie verursachte Fehler und technische Fehler. Folgende Tabelle zeigt Beispiele für die Bedrohungen mit deren Auswirkungen.

Tabelle 10: Beispiele für Unternehmensbedrohungen und deren Auswirkungen

Bedrohungen	Auswirkungen
Zu hohe Temperaturen am Standort des Servers	Ausfall des Servers
Inkompetente Mitarbeiter	Nichteinhaltung von Richtlinien
Fehlfunktion in Software	Schadsoftwareangriffe

Quelle: Firuza Muhamadova

Für den Eintritt einer Bedrohung spielen die vorhandenen Schwachstellen eine entscheidende Rolle. Erst nach deren Ausnutzung kann eine Bedrohung seine negativen Folgen zeigen. Zum Beispiel kann die Bedrohung „Diebstahl von Informationen oder Dokumenten“ dann erfolgen, wenn der Speicherplatz, auf dem sich Dokumente und Informationen befinden, nicht geschützt ist. Der nicht geschützte Speicherort ist dabei eine Schwachstelle, welche von der Bedrohung ausgenutzt werden kann.

Das Risikomanagement bezeichnet die koordinierten Aktivitäten zur Steuerung und Kontrolle einer Organisation unter Berücksichtigung von Risiken.

Die unkoordinierte Durchführung von Veränderungen bei einem Unternehmen ohne ein Risikomanagement berücksichtigt keine Risiken. Zum Beispiel möchte der Leiter einer Firma seine Daten in eine Cloud übertragen, weil es günstiger ist, ohne etwas über die möglichen Transferrisiken zu wissen. Risikomanagement sorgt also als eine Art von Management für die harmonisierte Gestaltung der Änderungen zu den bestehenden Organisationsregelungen und beachtet dabei die möglichen Risiken. (Klipper, 2015, S. 44 ff.)

Die Notwendigkeit des Risikomanagements ist wie folgt im Standard ISO/IEC 27005 definiert: „Eine systematische Vorgehensweise für Risikomanagement im Bereich Informationssicherheit ist erforderlich, um die organisatorischen Bedürfnisse hinsichtlich der Anforderungen von Informationssicherheit zu definieren und das ISMS effektiv zu gestalten.“

Der Prozess „Risikomanagement“ gibt die einzelnen Vorgänge des Risikomanagements an und die folgende Abbildung zeigt, welche Aktivitäten des Risikomanagements in welcher Phase der PDCA-Methodik durchzuführen sind.

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

Abbildung 19: Die Ausrichtung des ISMS- und Informationssicherheits-Risikomanagementprozesses
Quelle: ISO/IEC 27005, 2011, S. 9.

Zu den wichtigsten Schritten für die Durchführung des Risikomanagements zählen:

Risikomanagementkontext festlegen

Der Risikomanagementprozess startet mit der Festlegung des Kontextes. Dabei werden die Anwendungsbereiche, Grenzen, Rollen und Verantwortlichkeiten sowie Basiskriterien für das Risikomanagement definiert.

Umfang/Grenzen definieren

Dieser Vorgang beschäftigt sich mit der Festlegung, wann der Risikomanagementprozess durchgeführt und welche Risiken mit der Prozessumsetzung behandelt werden soll.

Umfang/Grenzen bestätigen

Den festgelegten Umfang und die Grenzen des Risikomanagements sollen vom Fachverantwortlicher bestätigt werden.

Basiskriterien definieren

Die Basiskriterien umfassen die Risikobewertungs-, Auswirkungs- und Risikoakzeptanzkriterien.

Die Risikobewertungskriterien stellen die Kritikalität des Assets fest. Bei Berücksichtigung der Informationssicherheitsschutzziele wie Vertraulichkeit und Integrität wird eine Skala zur Einstufung der Risiken entwickelt. Dabei fragt sich, welche Risiken auf welcher Stufe einer Skala eingeordnet werden sollen.

Zum Beispiel kann der Ausfall eines Servers als ein hohes Risiko eingestuft werden, wohingegen die Nichteinhaltung der Richtlinien ein relativ niedriges Risiko darstellt.

Risikoauswirkungskriterien basieren auf den Risikobewertungskriterien, ergänzen diese auch. Die Auswirkungskriterien stellen den Grad der Schäden oder Kosten fest, welche der Risikoeintritt verursachen kann.

Die Risikoakzeptanzkriterien hängen von Strategie und Zielen der Organisation ab. Deshalb ist es sinnvoll, dass jede Organisation ihre individuelle Skala für die Einstufung der Risikoakzeptanz definiert. Im Allgemeinen sollen die Risikoakzeptanzkriterien festlegen, wann ein Risiko akzeptierbar ist.

Risiko bewerten

Dieser Vorgang wird wie die Festlegung des Kontextes in der Planungsphase der PDCA-Methodik durchgeführt. Die Risikobewertung gliedert sich in Risikoidentifizierung, Risikoanalyse und Risikobewertung.

Risiko identifizieren

Die Identifizierung eines Risikos erfolgt wiederum durch mehrere Schritte. Hier werden alle Assets identifiziert, welche die Organisation besitzt. Je nach Art und Struktur des einzelnen Assets werden die Bedrohungen und deren Auswirkungen, welche das Asset betreffen können, und die Asset-Schwachstellen identifiziert. Zusätzlich ist in diesem Vorgang festzustellen, welche Maßnahmen bereits vorhanden sind, die beim Eintritt der bekannten Risiken eingesetzt werden können.

Risiko analysieren

Die Risikoanalyse beschäftigt sich hauptsächlich mit Schätzungen. Die Auswirkungen und die Eintrittswahrscheinlichkeit von identifizierten Bedrohungen werden geschätzt und dem entsprechenden Risiko-Level zugeordnet. Mithilfe dieser Klassifizierung kann entschieden werden, welche Risiken zuerst behandelt werden sollen.

Risiko bewerten/priorisieren

Dabei werden die Prioritäten für die Behandlung der Risiken gesetzt.

Bevor man mit dem nächsten Vorgang beginnt, ist festzustellen, ob die Ergebnisse der Risikobewertung ausreichend sind. Der Risikomanagementprozess kann mit dem Vorgang der Risikobehandlung fortgesetzt werden, falls die Ergebnisse ausreichend sind. Wenn dies nicht der Fall ist, dann ist die Risikoidentifizierung noch einmal durchzuführen, bis die Ergebnisse den Erwartungen entsprechen.

Zusätzlich soll überprüft werden, ob die vorhandenen Standardmaßnahmen für die Risikobehandlung ausreichend sind. Es ist erforderlich, die Risikobehandlungs-

alternativen auszusuchen, wenn die Standardmaßnahmen für die Risikobehandlung nicht genügen.

Risikobehandlungsalternative auswählen

Risikobehandlungsalternativen sorgen dafür, die Eintrittswahrscheinlichkeit und Auswirkung eines möglichen Risikos zu vermindern oder zu verhindern.

Die ISO/IEC 27005 hat eine Reihe von Möglichkeiten für die Risikobehandlung festgelegt. Dementsprechend kann ein Risiko durch Vermeidung, Modifizierung, Übernahme oder Teilen behandelt werden. Auf Basis der Resultate der Risikobewertung werden eine oder mehrere passende Alternativen für die Risikobehandlung ausgewählt.

Risiken modifizieren

Durchgeführte Maßnahmen tragen zur Modifizierung des Risikolevels bei. Mit der Risikoübernahme entscheidet man sich, die Schäden eines Risikos zu akzeptieren, da in manchen Fällen die Risikobehandlung mehr Kosten verursachen kann als der eigentliche Risikoschaden.

Risiken vermeiden

Bei den hoch eingestuften Risiken sollen diejenigen Aktivitäten vermieden werden, welche das Risiko auslösen.

Risiken teilen

Das Teilen von Risiken bezeichnet die Verlagerung von Risiken in externe Bereiche oder andere Filialen der Organisation. Es könnte dabei allerdings eine zusätzliche Risikobehandlung benötigt werden, weil das Teilen der Risiken auch oft neue Risiken verursachen kann.

Nach der Auswahl und Durchführung der geeigneten Alternativen der Risikobehandlung ist zu überprüfen, ob die Risikobehandlung die entsprechenden Ergebnisse geliefert hat. Der Vorgang der Risikobehandlung muss so lange wiederholt werden, bis deren Ergebnisse ausreichend sind. Im besten Fall wird der Prozess nun mit der Risikoakzeptanz fortgesetzt.

Risiko akzeptieren

Es ist dabei zu beachten, dass die Begrifflichkeiten Risikoübernahme und Risikoakzeptanz unterschiedliche Bedeutungen innerhalb der Informationssicherheit haben. Die Risikoakzeptanz folgt nach der Risikobehandlung und akzeptiert die restlichen Risiken, welche trotz der durchgeführten Risikobehandlung verblieben sind.

Im Gegensatz dazu geht es bei der Risikoübernahme um eine Möglichkeit der Risikobehandlung.

Restrisiko bestätigen

Die zu akzeptierenden Risiken sollen mit dem Organisationleiter kommuniziert werden. Dafür werden alle verbleibenden Risiken in einer Liste zusammengefasst und ihm vorgelegt. Erst nach der Zustimmung des Organisationsleiters können die Restrisiken akzeptiert werden.

Risiko überwachen/überprüfen

Die Überwachung und Überprüfung der Risiken und ihrer Faktoren wird durchgeführt, um die möglichen Änderungsbedarfe möglichst früh zu entdecken. Der Standard ISO/IEC 27005 gibt vor, den Risikomanagementprozess kontinuierlich zu überwachen. Die Frage ist dabei, ob die durchgeführten Bewertungen und Behandlungen wirksam sind. Darüber hinaus ist zu überprüfen, ob die Prozessverbesserung nötig ist.

Risikomanagement verbessern/aktualisieren

Bei Bedarf wird der Risikomanagementprozess optimiert. Das Endergebnis des Prozesses ist das Erreichen eines aktuellen Risikomanagements, welches für die Geschäftsziele einer Organisation geeignet ist. Für den Erfolg des Risikomanagements ist die ständige Kommunikation zwischen dem Manager und dem IT-Sicherheitsbeauftragten sehr wichtig. Jeder Prozessschritt und die jeweiligen Ergebnisse sollen kommuniziert werden.

Im Weiteren sind das Prozessmodell und die Prozessbeschreibung des Risikomanagements dargestellt. (DIN, ISO/IEC 27005, 2011, S. 5 ff.) (Klipper, 2015, S. 59-94)

Tabelle 11: Prozessbeschreibung des Risikomanagements

Prozessname: Risikomanagement
Zweck: Die Festlegung einer systematischen Risikomanagementvorgehensweise im Bereich Informationssicherheit, um die organisatorischen Bedürfnisse bezüglich der Anforderungen von Informationssicherheit zu identifizieren und ein effektives ISMS zu gestalten. Dabei soll sichergestellt werden, dass das Informationssicherheitsrisikomanagement seine beabsichtigten Ziele erreichen kann und die unerwünschten Auswirkungen verhindert oder verringert. Das Informationssicherheitsrisikomanagement soll zur fortlaufenden Verbesserung des ISMS beitragen.

Verantwortlicher:	**Mitwirkende Personen:**
IT-Sicherheitsbeauftragter	Führungskräfte/Manager, Mitarbeiter, Fachverantwortlicher, Datenschutzbeauftragter
Input: Vorzunehmende Änderungen, Projekte und Sicherheitsvorfälle	
Output: Transparente Risikosituation, behandelte Risiko, akzeptierte Restrisiko	
Anforderungen: Die entwickelte Risikomanagementvorgehensweise soll für die Organisationsumgebungen geeignet sein. Das Risikomanagement soll ein wesentlicher Teil von Informationssicherheitsmanagement sein und sowohl in der Implementierungs- als auch in der Umsetzungsphase angewendet werden. Das Informationssicherheitsrisikomanagement soll ein kontinuierlicher Prozess in einer Organisation sein.	
Mitwirkende Dokumente: Organisationsrichtlinien, inventarisierte Asset-Liste, Liste der Standardmaßnahmen	
Schnittstellen des Prozesses: Änderungssteuerung, Handhabung von Informationssicherheitsvorfällen, Handhabung von technischen Schwachstellen	

Quelle: Firuza Muhamadova

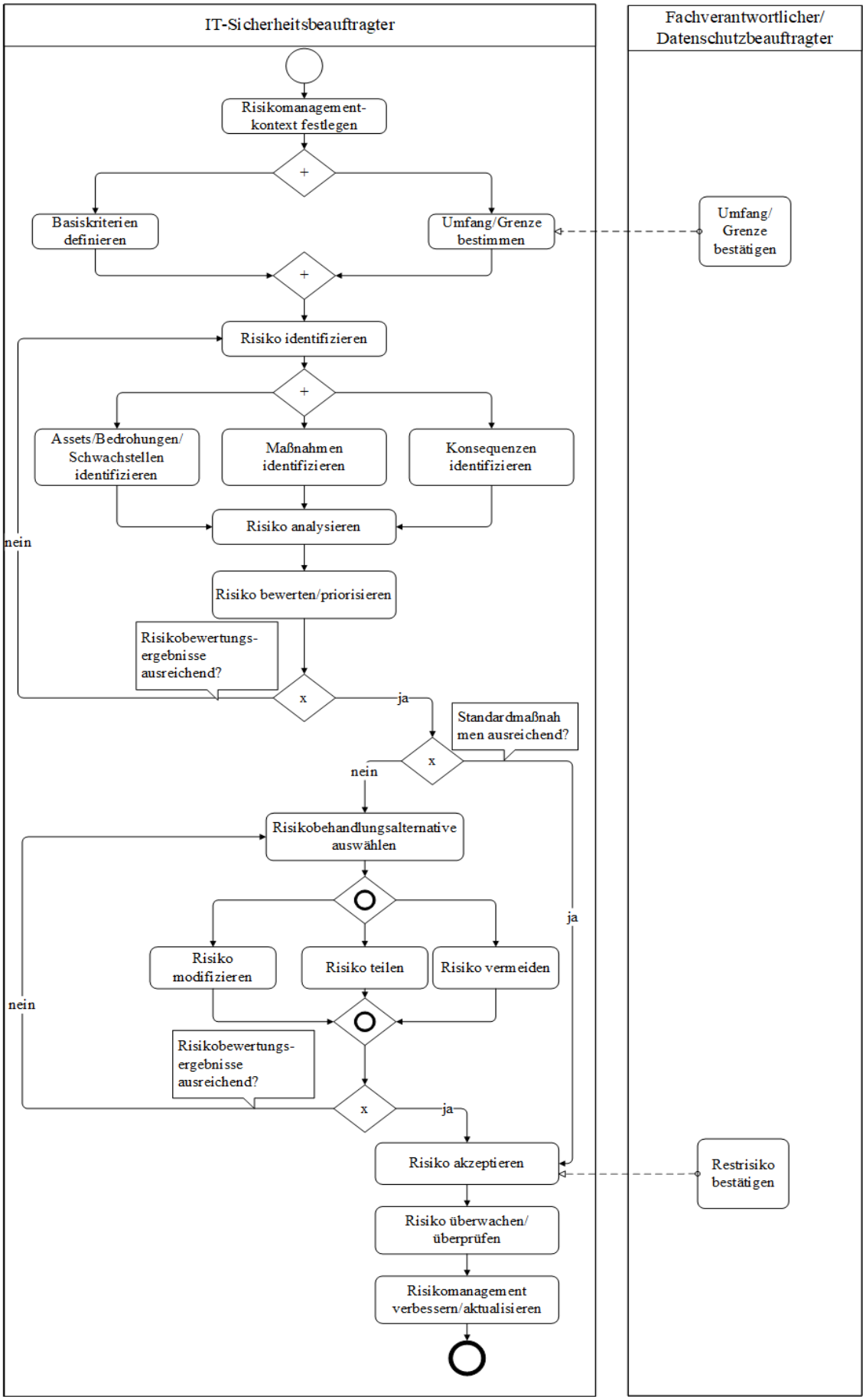

Abbildung 20: Prozessmodell des Risikomanagements

Quelle: Firuza Muhamadova.

5. Exemplarische Anwendung des Benutzerkennungsverwaltungsprozesses im Hochschulumfeld

Dieses Kapitel beschäftigt sich mit der Frage, wie der Prozess Benutzerkennungsverwaltung an der Hochschule Augsburg durchgeführt wird. Um dies herauszufinden, war eine Kontaktaufnahme mit der zuständigen Person, die den Prozess Benutzerkennung verwaltet, wichtig.

Die Prozessdetails wurden nach dem Gespräch mit Herrn Tkotz deutlich erkennbar. Herr Tkotz arbeitet im Rechenzentrum der Hochschule Augsburg und sorgt u. a. für die sorgfältige Durchführung des Benutzerkennungsverwaltungsprozesses.

Nach Herr Tkotzs Angaben werden folgende Aktivitäten innerhalb des Benutzerkennungsverwaltungsprozesses an der Hochschule ausgeführt.

Benutzerantrag starten

Für die Benutzerkennungserstellung ist die aktive Interaktion seitens Benutzer, welcher die Kennung später für seinen Zugang in die Systeme und Informationen verwenden wird, erforderlich. Das bedeutet, die Benutzerkennung wird teilweise von ihrem künftigen Nutzer angelegt. Alle Benutzer lassen sich an der Hochschule in vier Gruppen gliedern. Darunter fallen die Studierende, Lehrende, Angestellte und Gäste. Je nach der Benutzerart kann die Benutzerkennungserstellung etwas unterschiedlich laufen.

Persönliche Daten eintragen

Alle Benutzer sind aufgefordert, ihre persönlichen Daten wie Nachname, Vorname und Adresse für die Benutzerkennung einzutragen.

Matrikelnummer/Masterkennwort eintragen

Die Studierenden sollen ihre Matrikelnummer und Masterpasswort eintragen, um eine Benutzerkennung sofort freischalten zu können.

Freischaltung beantragen

Gäste, Lehrende und Angestellte sollen für die Freischaltung ihrer Benutzerkennung einen Antrag stellen.

Antrag überprüfen

Die Entscheidung für oder gegen die Freischaltung der Benutzerkennung liegt beim Administrator. Dabei stützt er sich auf die Ermittlungen der Personalabteilung oder des Studentenamts.

Personalfall anlegen/Student immatrikulieren

In diesem Vorgang legt die Personalabteilung bzw. das Studentenamt den Personalfall bzw. den Studenten an. Das Vorhandensein der Unterlagen wie Arbeitsvertrag oder Immatrikulationsbescheinigung dienen als ein Nachweis, dass die Studierende oder Arbeitnehmer an die Hochschule neu aufgenommen sind und somit berechtigt sind, eine Kennung zu beantragen.

Autorisation vornehmen

Wenn die Benutzerkennung noch nicht existiert, kann sie vom Administrator angelegt und werden.

Antrag ablehnen

Der Freischaltungsantrag der Benutzerkennung wird abgelehnt, wenn dafür keine Grundlage seitens der Personalabteilung oder des Studentenamts besteht.

Benutzerkennung freischalten

Im anderen Fall wird die Benutzerkennung freigeschaltet.

Existente Mitglieder melden

Die Personalabteilung bzw. Studentenamt übermittelt eine Liste der existierenden Hochschulmitglieder aus ihrem Bereich als Grundlage für die Autorisation zur Freischaltung der Benutzerkennung.

Liste aktualisieren

Die bereits vorhandenen Benutzerkennungen werden täglich hinsichtlich der Veränderung an der Beschäftigung oder an dem Studentenstatus überprüft. In beiden Fällen: Exmatrikulieren der Studierende und Kündigung der Beschäftigte ist der Benutzerkennungsstatus anzupassen.

Alle Benutzerkennungen, deren Status positiv beibehalten werden soll, werden dem Administratorgemeldet.

Existente Mitglieder überprüfen

In diesem Vorgang werden alle gemeldeten Benutzerkennungen gegenüber den bereits vorhandenen Benutzerkennungen überprüft.

Ungültige Kennung kennzeichnen

Mit der Meldung der Benutzerkennungen kann deren Gültigkeitsdauer verlängert werden. Die Abweichungen davon ergeben die zu löschenden Kennungen.

Löschen der Benutzerkennung informieren

Jede Benutzerkennung besitzt eine Gültigkeitsdauer. Die Kennung der Studierenden haben eine Gültigkeitszeitraum von sechs Monaten, was einem Semester entspricht. Der User wird darüber informiert, bevor seine Kennung endgültig gelöscht wird.

Benutzerkennung löschen

Mit dem Löschen der Benutzerkennung wird der Benutzerkennungsverwaltungsprozess beendet. (Tkotz, 2018)

Wie bekannt aus früheren Abschnitten der Arbeit folgen in diesem Kapitel auch das Prozessmodell und eine Prozessbeschreibungstabelle zu dem Benutzerkennungs-verwaltungsprozess.

Mithilfe des Prozessmodells werden die bereits beschriebenen Vorgänge graphisch dargestellt. Die Prozessbeschreibungstabelle beinhaltet die weiteren Prozessdetails, die beachtet werden sollen.

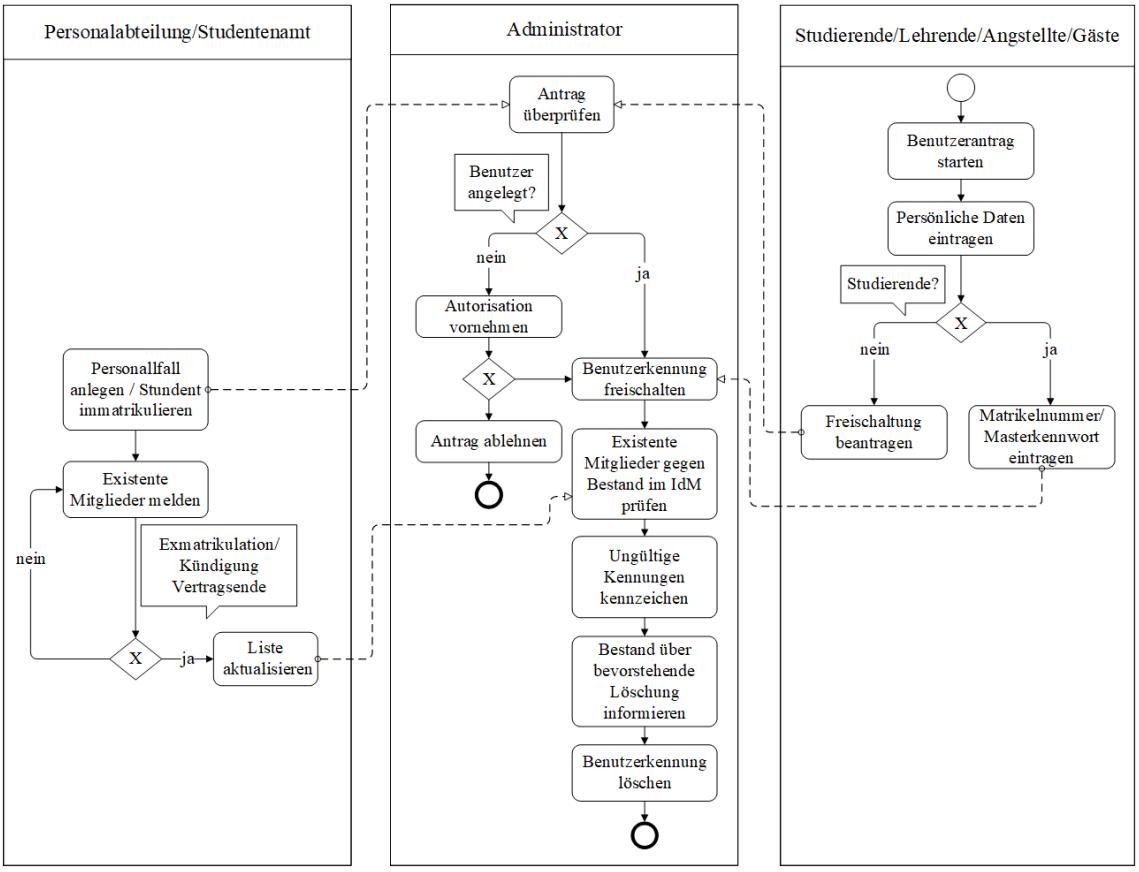

Abbildung 21: Prozessmodell der Benutzerkennungsverwaltung

Quelle: Firuza Muhamadova

Tabelle 12: Prozessbeschreibung der Benutzerkennungsverwaltung

Prozessname: Benutzerkennungsverwaltung	
Zweck: Mit der Umsetzung des Prozesses sollen die Benutzerkennungen vor ihrer Freischaltung überprüft werden. Die Benutzerkennungen sind nach dem Austritt einer Beschäftigter oder nach der Exmatrikulation einer Studierenden möglichst schnell zu melden und zu deaktivieren.	
Verantwortlicher: Administrator	**Mitwirkende Personen:** Personalabteilung, Studentenamt, Studierende, Angestellte, Lehrende, Gäste
Input: Benutzerkennungserstellung	
Output: Angelegte/freigegebene/gelöschte Benutzerkennungen	
Anforderungen: Die Benutzerkennungen, deren Benutzer aktiv an der Hochschule sind, sollen täglich gemeldet werden. Im kritischen Fällen sind die Benutzerkennungen sofort zu löschen.	
Mitwirkende Dokumente: Immatrikulationsbescheinigung der Studierende, Arbeitsvertrag, Benutzerkennungsliste	

Quelle: Firuza Muhamadova

6. Zusammenfassung

Im Fokus der Arbeit steht die Gestaltung der Prozesse, die für den Betrieb eines Informationssicherheitssystems erforderlich sind. Dafür waren als theoretische Grundlagen Einblicke in Prozessmanagement und Prozessmodellierung nötig.

Die nächste Herausforderung bestand darin, die relevanten Prozesse im Bereich der Informationssicherheit zu definieren. Zu diesem Zweck wurden die dazu geeigneten ISO/IEC-Standards ausgewählt, welche ein Muster für die Einrichtung und Umsetzung eines Informationssicherheitsmanagementsystems zur Verfügung stellen. Dieses muss angewendet werden. Als Ergebnis wurden dabei die Definitionen zu den folgenden Prozessen und Unterprozessen entwickelt, welche mindestens für den Aufbau eines ISMS erforderlich sind.

- Personalsicherheit
- Benutzerzugangsverwaltung
  Registrierung und Deregistrierung von Benutzern
  Zuteilung und Entziehung von Benutzerzugangsrechten
  Verwaltung privilegierter Zugangsrechte
  Verwaltung geheimer Authentisierungsinformationen
- Betriebssicherheit
  Datensicherung
  Änderungssteuerung
  Handhabung von technischen Schwachstellen
- Handhabung von Informationssicherheitsvorfällen
- Risikomanagement

Die aus den ISO/IEC-Vorgaben abgeleiteten Prozesse und Unterprozesse wurden anschließend in der Prozessdokumentation erfasst, in der zuerst die jeweilige Aufgabe mit den zugehörigen Vorgängen eines bestimmten (Unter) Prozesses beschrieben wird. Danach wurden die (Unter) Prozesse mithilfe der BPMN-Werkzeuge zur Prozessmodellierung visualisiert. Jedem Prozess ist eine zusätzliche Prozessbeschreibungstabelle beigefügt, in der die wesentlichen Prozessinformationen zusammengefasst sind.

Schließlich wurde untersucht, wie der Benutzerkennungsverwaltungsprozess an der Hochschule Augsburg durchgeführt wird. Anhand eines Interviews mit dem Prozessverantwortlichen wurden die durchzuführenden Vorgänge innerhalb des

Prozesses definiert und dokumentiert. Auch hierzu wurden ein Modell und eine Tabelle erstellt.

Mit der Registrierung und Deregistrierung von Benutzern bietet die ISO/IEC27002 eine Möglichkeit zum Vergleichen an. Dabei können die aus dem Standard abgebildeten Prozesse der Registrierung und Deregistrierung von Benutzern mit dem an der Hochschule Augsburg angewendeten Prozess für die Benutzerkennungsverwaltung verglichen werden.

Aus diesem Vergleich wird es deutlich, dass die Prozesse der Registrierung und Deregistrierung von Benutzern die grundlegenden Vorgänge für die Benutzerkennungsverwaltung darstellen, wohingegen der Prozess an der Hochschule noch speziellere Vorgänge umfasst.

Das Ziel der ISO/IEC-Standards besteht auch darin, allgemeine Vorgaben für die Einrichtung und Durchführung der ISMS zu machen, damit diese für jede Organisation geeignet sind, unabhängig von ihrer Art und Größe. Je nach Art und Ziel können die Organisation aufbauend auf den ISO/IEC-Vorgaben ihre organisationsspezifischen Vorgaben oder Richtlinien für ihr ISMS festlegen.

Aus dem Interview mit Herrn Tkotz ist klar geworden, dass die Durchführung der informationssicherheitsrelevanten Prozesse an der Hochschule auf Basis der gesammelten Erfahrungen erfolgt. Das für die Prozessdurchführung im Laufe der Jahre aufgebaute Know-how ist einem neu hinzukommenden Mitarbeiter weiterzuvermitteln. Dies kann mithilfe der Prozessdokumentation gelöst werden.

Die Ergebnisse aus dem Prozessvergleich lassen zusammenfassend erkennen, dass die in der vorliegenden Arbeit dokumentierten Prozesse für die Erstellung der Prozessdokumentation als Grundlage für die Informationssicherheitsprozesse dienen können. Der Prozessverantwortliche kann die aus den ISO/IEC-Standards abgeleiteten Prozesse mit den organisationspezifischen Prozessaktivitäten erweitern und somit organisationeigene Prozesse definieren bzw. dokumentieren.

Mit der zunehmenden Digitalisierung, dem Internet der Dinge und der Industrie 4.0 wird ein fehlerfrei laufendes ISMS immer wichtiger werden. Forschungen dazu sollten daher weiter vorangetrieben werden.

Literaturverzeichnis

DIN. (2011). *ISO/IEC 27005.* Schweiz.

DIN. (2014). *ISO/IEC 27001.* Berlin: Beuth Verlag GmbH.

DIN. (2015). *ISO/IEC 27002.* Berlin: Beuth Verlag GmbH.

DIN. (2016). *ISO/IEC 27004.* Schweiz.

DIN. (2017). *ISO/IEC 27003.* Schweiz.

DIN. (2018). *ISO/IEC 27000.* Schweiz.

Füermann, T. (2014). *Prozessmanagement.* München: Carl Hanser Verlag.

Heinrich Kersten, J. R.-W. (2013). *IT Sicherheitsmanagement nach ISO 27001 und Grundschutz.* Wiesbaden: Springer Vieweg Verlag.

Jochen Göpfert, H. L. (2013). *Geschäftsprozessmodellierung mit BPMN 2.0.* München: Oldenbourg Wissenschaftsverlag GmbH.

Jörg Becker, M. K. (2012). *Prozessmanagement.* Berlin: Springer Verlag.

Klipper, S. (2015). *Information Security Risk Management.* Wiesbaden: Springer Vieweg Verlag.

Michael Brenner, N. G. (2017). *Praxisbuch ISO/IEC 27001.* München: Carl Hanser Verlag.

Sowa, A. (2017). *Management der Informationssicherheit.* Wiesbaden: Springer Vieweg Verlag.

Tkotz, P. (11. April 2018). Angstellte im Rechenzentrum. (F. Muhamadova, Interviewer)

www.bitkom.org/. (25. Februar 2018). Von https://www.bitkom.org/Presse/Presseinformation/Die-zehn-groessten-Gefahren-im-Internet.html abgerufen

www.bsi.bund.de. (17. Februar 2018). Von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html abgerufen

www.security-insider.de. (20. März 2018). Von https://www.security-insider.de/lueckenschluss-in-der-it-sicherheit-a-500143/ abgerufen

www.techrepublic.com. (8. März 2018). Von https://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/ abgerufen

www.verizonenterprise.com. (15. März 2018). Von https://www.verizonenterprise.com/verizon-insights-lab/dbir/ abgerufen