IT-Risikomanagement

Bachelor-Thesis
zur Erlangung des akademischen Grades B.Sc.

Thomas Ehlers
2058055

Hochschule für Angewandte Wissenschaften Hamburg
Fakultät Design, Medien und Information
Department Medientechnik

Erstprüfer: Prof. Dr. Nils Martini
Zweitprüfer: Prof. Dr. Andreas Plaß

Hamburg, 3. 2. 2016

Inhalt

Zusammenfassung

Die folgende Arbeit soll einen Überblick über das Thema IT-Risikomanagement bieten. Hierfür wird die Entwicklung des Risikomanagements, bis zum heutigen IT-Risikomanagement beschrieben.

Weiterhin wird der Begriff des Risikos genauer untersucht und nach welchen Betrachtungspunkten ein IT-Risikomanagement als solches bewertet. Dabei werden monetäre Fragen berücksichtigt, wie die Kosten eines Risikos bei Eintritt oder die Kosten für die Beseitigung/Behebung des Problems. Ferner wird auf die Wahrscheinlichkeit eines Risikoereignisses eingegangen.

Das IT-Risikomanagement kennt verschiedene Methoden, um Risiken zu bewerten. Einige dieser Methoden werden erläutert, auch wenn diese Arbeit nur einen kleinen Einblick in die Vielzahl der Methoden bieten kann. Darüber hinaus wird eine ISO-Norm beschrieben, die ein IT-Risikomanagement beinhaltet.

Abschließend wird eine Umfrage analysiert, die zum Ziel hatte zu erfahren, wie verbreitet ein IT-Risikomanagement in Unternehmen in der heutigen Zeit ist.

Abstract

This thesis is a survey of the theme IT-Risk-Management. It will show the evolution of Risk Management to the IT-Risk-Management of today.

For that it will define the word risk and show, how the IT-Risk-Management is considering it. It considers monetary question, like how high the expenses will be, if a risk takes place. In addition to that it will take a look at how high the expenses are to reduce the effect of a risk. Beside that it will illustrate, how the probability of an event will be handled.

There are different methods to rate a risk in the IT-Risk-Management. Some oft this methods will be described, although this thesis can just show a small insight into this subject, since there are a multitude of different methods. Beyond that an ISO Standard, which is handling IT-Risk-Management, will be shown.

Concluding this thesis it will analyse a survey, which purpose was to determine, how common an IT-Risk-Management in companies nowadays is.

1 Grundlagen

1.1 Risiko als Chance

Das IT-Risikomanagement ist eine Unterart des Risikomanagements in Unternehmen. Auf Seite 8, Abbildung 1 kann man verschiedene Unterarten sehen, die unter einen gemeinsamen Oberpunkt, dem Risikomanagement im Unternehmen (Enterprise Risk Management) stehen.

Das Wort Risiko ist eher negativ behaftet und wird auch im Duden eher negativ beschrieben: „möglicher negativer Ausgang bei einer Unternehmung, mit dem Nachteile, Verlust, Schäden verbunden sind; mit einem Vorhaben, Unternehmen o. Ä. verbundenes Wagnis“ (Dudenverlag, 2016)

Hierbei wird oftmals übersehen, dass ein Risiko auch eine Chance sein kann. Im Falle eines Unternehmens kann ein Risiko am Ende zum Beispiel auch einen Gewinn bedeuten. So ist ein Investment im Aktienmarkt immer mit einem Risiko verbunden. Das Risiko kann sich dann aber positiv, wie auch negativ auswirken.

Auch vor Jahrhunderten wurde ein Risiko schon als Chance gesehen, das folgende Kapitel befasst sich mit dieser Entwicklung.

1.2 Entwicklung des Risikomanagements

Risikomanagement in Unternehmen wird schon immer betrieben. Selbst im Mittelalter musste ein Händler sich überlegen, ob sich z.B. eine monatelange Reise lohnen wird. Preise konnten sinken oder fallen während er unterwegs war. Oder die ganze Ware konnte durch Diebe oder Wettereinflüsse verloren gehen. Zu dieser Zeit nutzten die Händler allerdings nur ihren eigenen Sachverstand, um dieses Problem zu lösen. So waren es meistens der zu erwartende Gewinn und die Risikobereitschaft, die am stärksten zu der Entscheidung beigetragen haben.

Die Entscheidungsprozesse haben sich im Laufe der Zeit fortwährend weiterentwickelt. Heutzutage stehen Unternehmen mathematische Formeln zur Verfügung, mit denen Wahrscheinlichkeiten errechnet werden, um sicherere Entscheidungen treffen zu können. Mit diesem Hilfsmittel kann ein Unternehmen besser einschätzen, ob sich ein Risiko lohnt oder es lieber gemieden werden sollte.

Diese Methoden können nicht verhindern, dass falsche Entscheidungen getroffen werden. Sie bieten zumindest eine Hilfestellung, um die Wahrscheinlichkeit schlechter Entscheidungen zu senken.

Das ausführende Organ bleibt dennoch der Mensch, der seine Entscheidungen oftmals emotional trifft. Dies könnte dazu führen, dass die Entscheidungsträger sämtliche Analysen ignorieren.

Außerdem sind diese Methoden ja auch lediglich Prognosen, die nach bestem Wissen angefertigt werden. Dieses Wissen kann Lücken enthalten, oder auch einfach nicht so eintreten, wie es erwartet wird. Dazu kann es bei Wahrscheinlichkeiten auch passieren, dass anstatt der 99% Chance, die 1% Chance eintritt. Somit ist das Risikomanagement nur ein weiteres Hilfsmittel um Entscheidungen zu treffen. Ob und wie stark es genutzt wird oder eben nicht, ist auch immer ein menschlicher Faktor. Dennoch kann es ein wichtiges Werkzeug bei der Entscheidungsfindung sein. Wichtig hierbei ist, auf die Analysen vertrauen zu können. Also kompetente Mitarbeiter zu haben, die ein möglichst genaues Bild liefern können.

Das Risikomanagement beschränkt sich natürlich nicht nur auf monetäre Fragen. Es soll auch allgemeine Risiken im Unternehmen abschätzen. Vermeidung von Fehlern durch Angestellte oder gesetzliche Verpflichtungen sind weitere Beispiele, die hier Beachtung finden.

So soll möglichst bei jedem Prozess des Unternehmens das Risiko auf negative Auswirkungen minimiert werden.

Kleinere Unternehmen haben oft nicht die Möglichkeit, alles genau einschätzen und errechnen zu können. So werden dort oft keine großen Analysen getätigt, sondern vielmehr alles durchdacht und dann nach bestmöglichem Wissen gehandelt.

Demnach wird ein kleiner Malerbetrieb, mit vier Mitarbeitern, keine großen Analysen mit Wahrscheinlichkeitsrechnungen über die Zukunft nutzen, wenn er einen neuen Mitarbeiter einstellt. Stattdessen werden vielleicht die Auftragslage und der Umsatz bzw. Gewinn gegenüber gestellt, um eine Entscheidung zu treffen. Für kleinere Betriebe ist ein kontinuierliches Risikomanagement aber auch aufgrund der Kosten kaum möglich. Und das was genutzt wird, reicht für kleinere Entscheidung aus.

Ein Beispiel für Unternehmensgruppen, die stark auf ein gutes Risikomanagement setzen, sind Versicherungen. Versicherungen leben von einem guten Risikomanagement. Indem sie

das Risiko möglichst genau errechnen, können sie ermitteln welchen Preis sie für eine Versicherung verlangen müssen. Fehler in diesen Analysen kosten das Unternehmen Geld.

Das IT-Risikomanagement hingegen ist für alle großen Unternehmen eine Hilfestellung, auch wenn es vielleicht nicht so leicht ersichtlich ist wie bei den Versicherungen. Im folgenden Kapitel wird darauf eingegangen.

1.3 IT-Risikomanagement

In dem schon lange vorhandenen Gebiet des Risikomanagements ist das IT-Risikomanagement eine neuere Disziplin, die erst in den 90er Jahren anfing, sich richtig zu entwickeln. Auch vorher haben sich Unternehmen bereits über bestimmte Risiken Gedanken gemacht. Aber zu einem eigenständigen Gebiet im Risikomanagement hat es sich erst nach und nach entwickelt. Die Relevanz nahm dann im Laufe der letzten Jahrzehnte immer mehr zu.

Ein Grund hierfür ist, dass die Bedeutsamkeit des Internets immer größer wurde, gleichzeitig aber auch die Risiken, die mit ihm einhergehen wuchsen.

Gleiches gilt für Daten, die in Unternehmen gespeichert werden. Für viele Unternehmen kann ein Verlust selbiger zu großen Problemen führen. Je nach Unternehmen auch bis hin zur starken Gefährdung dessen gesamten Fortbestandes.

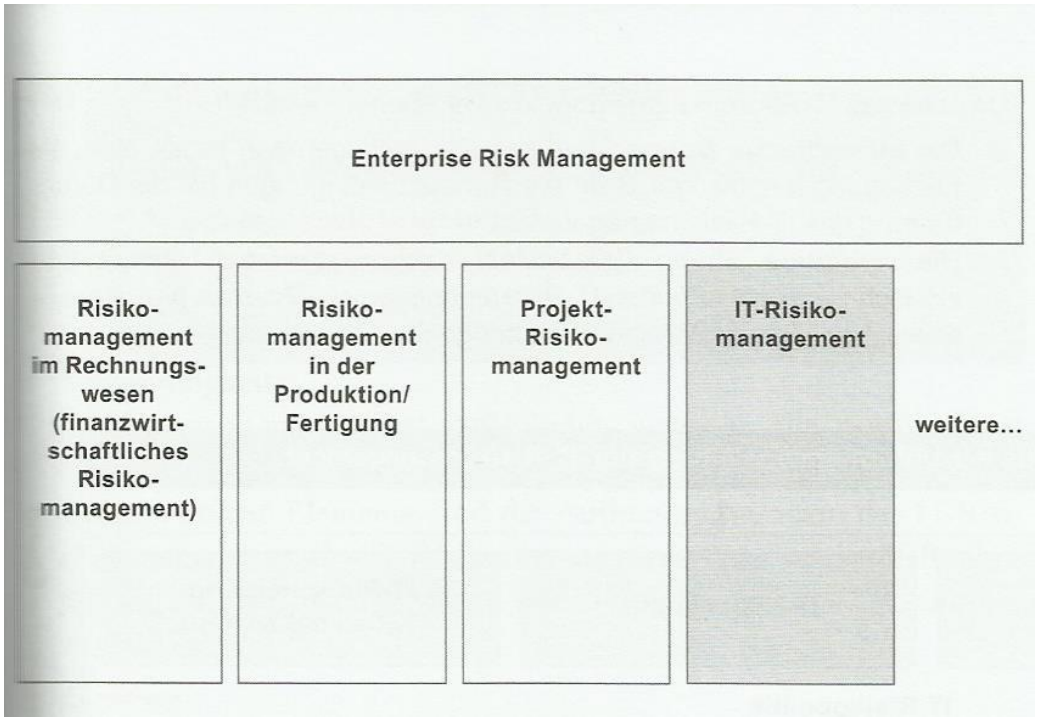

Abbildung 1 Enterprise Risk Management und bereichsbezogenes Risikomanagement

Resultierend aus der Wichtigkeit des Internets (Zugriff auf Firmennetzwerke auch von außen), der elektronisch gespeicherten Daten und vielfältigen anderen Gründen hat sich das IT-Risikomanagement, auf welches im nächsten Kapitel genauer eingegangen wird, zu einer wichtigen Unterdisziplin im Risikomanagement vieler Unternehmen entwickelt.

2 IT-Risikomanagement

2.1 Risikobegriff

2.1.1 Ursachenbezogene Sicht

Laut Knoll gibt es zwei verschiedene Sichtweisen auf ein Risiko.

„Die ursachenbezogene Sicht geht von einem initialen Zustand und einem oder mehreren gleichzeitig oder (kurz) aufeinander folgenden Ereignissen aus. Der initiale Zustand sowie Art, Häufigkeit und Zeitpunkt der Ereignisse stellen die Ursachen für das Risiko dar. Sie können unternehmensintern oder unternehmensextern begründet sein.“ (Knoll, 2014, S. 10)

Hier wird, wie der Name sagt, die Ursache in den Vordergrund gestellt. Es wird die ursprüngliche Entscheidung in den Mittelpunkt gestellt. Nach dieser Entscheidung können Risiken entstehen oder ausgelöst werden, die zum Zeitpunkt der Entscheidung so nicht ersichtlich waren.

Der ursachenbezogenen Sicht steht die wirkungsbezogene gegenüber, die im Folgenden erläutert wird.

2.1.2 Wirkungsbezogene Sicht

Wie der Name sagt, wird hier vor allem auf die Auswirkung der Risiken geschaut. Diese können das Unternehmen selber betreffen, aber auch Lieferanten oder Kunden.

„Für das Verständnis der wirkungsbezogenen Sicht sind Art, Umfang, Zeitpunkt und Dauer der Auswirkung entscheidend.“ (Knoll, 2014, S. 10)

Ob ursachenbezogen oder wirkungsbezogen, sie werden auf konkrete Situationen angewendet. Das folgende Kapitel enthält einige Beispiele, auf die beide Sichtweisen angewendet werden können.

2.2 Beispiele für Aufgaben des IT-Risikomanagements

Die Aufgaben eines IT-Managements sind vielschichtig. Im Folgenden werden einige dieser Aufgaben genannt.

Die augenscheinlichste Aufgabe ist das Erkennen von Gefahren, wie Angriffen aus dem Internet oder Netzwerk. Diese sollen genau analysiert werden, um herauszufinden wogegen man

vorgehen muss und welche Mittel man hierfür einsetzen kann. Auch die Frage der Kosten wird hier mit eingebunden und dem Ertrag entgegen gesetzt.

Hierbei ist das IT-Risikomanagement selber aber nicht unbedingt die Instanz, die dann die Maßnahmen umsetzt, sondern eher das Organ, welches diese Maßnahmen dem Management des Unternehmens vorschlägt und beschließen lässt. Dies kann allerdings von einzelnen Unternehmen abhängig sein. So können, gerade in kleineren Unternehmen, auch eine oder mehrere Personen sowohl für die Analyse zuständig sein, als auch nach der Bewilligung für die praktische Umsetzung.

Neben Angriffen aus dem Netzwerk gibt es auch noch andere Risiken, die im Auge behalten werden müssen. So muss die Hardware sicher sein, dass Datenverluste möglichst nicht auftreten. Dies kann von Datensicherung, bis zu Hochverfügbarkeitsnetzwerken reichen.

Eine weitere Aufgabe stellt die Sensibilisierung der Mitarbeiter für Sicherheit im Umgang mit IT-Systemen dar. Wenn einzelne Mitarbeiter Warnhinweise ignorieren oder aber nicht wissen, dass sie sich unsicher verhalten, kann es zu großen Problemen führen. Zwar können die Probleme durch Sicherheitsmaßnahmen aufgefangen werden, einfacher ist es aber, sie durch gute Aufklärung gar nicht erst entstehen zu lassen. Dadurch kann man eventuell einige Probleme so weit verhindern, dass sie nicht vorkommen, oder die Wahrscheinlichkeit des Vorkommens reduzieren. Eine gewissenhafte Aufklärung der Mitarbeiter führt somit zu einer Kosteneinsparung im Bereich der Gegenmaßnahmen.

Rechtliche Fragen dürfen dabei nicht außer Acht gelassen werden. Werden alle Gesetze eingehalten, wie zum Beispiel der Datenschutz? Was für Gesetzesänderungen gibt es oder kommen künftig auf das Unternehmen zu? Nicht zuletzt, welche Kosten können diese Änderungen verursachen, sei es durch Anschaffung neuer Hardware, oder ein benötigter Anstieg an Arbeitsstunden oder anderen Anforderungen?

Wenn diese Fragen konstant im Auge behalten werden, kann ein Unternehmen im Voraus planen, wie es zum Beispiel eine neue Gesetzesanforderung einhalten kann. Es lassen sich dann die benötigten Maßnahmen zur Einhaltung der Gesetze auch zeitlich planen, so dass die Firma nicht Gefahr läuft, bei Einführung des Gesetzes bei eventuellen Änderungen die Termine nicht einzuhalten und deshalb eventuell Strafen zahlen zu müssen oder Aufträge zu verlieren.

Um diese Beispiele oder auch andere besser kategorisieren zu können gibt es Schutzziele, die im folgenden Kapitel erklärt werden.

2.3 Schutzziele

Nach Knoll (Knoll, 2014, S. 18 f.), sind beim Eintritt eines IT-Risikos ein oder mehrere Schutzziele verletzt. Nach ihm gibt es hier vier wesentliche Schutzziele zu beachten.

1. **Vertraulichkeit**

   Vertraulichkeit bedeutet im Zusammenhang mit der IT, dass nicht berechtigte Parteien Zugriff auf nicht öffentliche Daten des Unternehmens nehmen konnten oder können. Ein kurzer Zugriff, der entdeckt und abgebrochen wurde reicht aus.

   Beim Eindringen können nicht nur interne Daten des eigenen Unternehmens betroffen sein, sondern auch Daten über Dritte, die das Unternehmen gespeichert hat. Dazu gehören Nutzerdaten oder auch Daten über andere Unternehmen wie Zulieferer und Kundendaten.

   Beispiele hierfür sind das Ausspähen von Kundendaten oder das Abhören von Kommunikation.

   Eine Möglichkeit Vertraulichkeit herzustellen, ist zum Beispiel die Verschlüsselung der Daten.

2. **Integrität**

   Die Integrität ist ein Maß um sagen zu können, ob Daten, Anwendungen oder auch das Informationssystem unverändert sind oder nicht. Das bedeutet, dass gesichert sein muss, dass keine unberechtigten Parteien diese verändert haben könnten. Es ist schon möglich die Integrität durch eine unsachgemäße Modifikation an einem Informationssystem zu verletzen.

   Falls die Integrität verletzt sein könnte, gilt sie so lange als verletzt, bis eindeutig das Gegenteil erwiesen werden kann.

   Ist die Integrität nicht gesichert, kann dies bei wichtigen Daten zu wesentlichen Problemen führen. So können falsche Finanzdaten, die kontrolliert wurden, auch rechtliche Fragen auslösen. Abseits von rechtlichen Themen, kann es auch intern zu großen Schwierigkeiten führen, wenn die Integrität nicht gewahrt ist und eventuell mit falschen Daten gearbeitet wird.

   Auch Dritte können durch eine Verletzung der Integrität betroffen sein. So können be-

troffene Daten und Anwendungen an Dritte weitergegeben werden und auch dort zu Problemen führen.

„Die Integrität kann beispielsweise durch ein Identitätsmanagement, Zugangs- und Berechtigungssystem, fachliche wie technische Abstimmungen der Datenbestände oder ein geordnetes Change-Management-Verfahren von Anwendungen sichergestellt werden.“ (Knoll, 2014, S. 19)

Echtheit: Die Echtheit und die Integrität sind stark miteinander verwoben. Mit ihr kann man bestätigen, dass Daten nicht verändert wurden.

Dies ist zum Beispiel mit Prüfsummen möglich.

3. **Verfügbarkeit**

   Die Verfügbarkeit stellt sicher, dass ein Informationssystem, möglichst immer voll erreichbar ist. Auch kurze Momente ohne Zugang zu dem System oder nur Teilen des Systems führen zu einer Einschränkung der Verfügbarkeit. Betroffen können hier die eigenen Mitarbeiter sein. Aber auch Dritte wie Kunden, die selber auf das System zugreifen wollen (z.B. einen Online-Versandhandel) oder durch Mitarbeiter nicht mehr bedient werden können, sind betroffen.

   Um die Verfügbarkeit zu gewährleisten, ist Redundanz wichtig. Redundanz bei der Hardware, aber auch bei der Software. Hochverfügbarkeitsnetzwerke sind hier eine Möglichkeit die Verfügbarkeit möglichst effizient zu bekommen. Sie liefern Redundanz in den meisten Systemen. Von der Datenspiegelung, bis zur kompletten Redundanz der gesamten Hardware.

4. **Zurechenbarkeit**

   Die Zurechenbarkeit soll garantieren, dass sich miteinander austauschende Parteien sicher sein können, dass sie die sind, für die sie sich ausgeben.

   Es soll verhindert werden, dass die Identität eines Dritten angenommen werden kann, ohne dass dies der anderen Partei auffällt.

   Wenn die Zurechenbarkeit nicht gewährleistet sein sollte, kann es zu großen Schäden führen. So können Online-Banking-Identitäten, wenn sie nicht zurechenbar sind, gesperrt werden. Oder wenn die Zurechenbarkeit nicht garantiert ist, könnte die Identität gefälscht werden um auf ein Konto zuzugreifen.

   Um die Zurechenbarkeit zu garantieren, können Signaturen eingesetzt werden.

Diese Schutzziele können von verschiedenen Personen verletzt werden. Diese müssen nicht mit Kalkül handeln, sondern können fahrlässig handeln oder ein Problem wie einen Bug in einem Programm durch Zufall entdecken.

Wenn eines oder mehrere dieser Schutzziele gebrochen werden, ist die Motivation der auslösenden Person zweitrangig. Zuerst muss auf das Problem reagiert werden, um einen eventuellen Schaden möglichst klein zu halten.

In der Nachbetrachtung wird es dann interessant herauszufinden, woher das Problem kam. Haben Personen mit Kalkül gehandelt, muss man die Sicherheitslücke schließen, die die Angreifer genutzt haben, um weitere Angriffe auf dieselbe Art zu unterbinden. Ist das Problem durch Fahrlässigkeit aufgetreten, muss untersucht werden ob das Problem durch Aufklärung gelöst werden kann. Soll heißen, dass Mitarbeiter dahingehend geschult werden, dass sie nicht mehr fahrlässig handeln. Oder ob es möglich ist das Problem so zu lösen, dass es nicht mehr durch Fahrlässigkeit ausgelöst werden kann. Wenn dies nicht möglich ist, bleibt nur der erste Punkt, die Aufmerksamkeit der Mitarbeiter zu erhöhen.

Gibt es ein Problem, das beim normalen Benutzen des Systems durch Nutzer auftreten kann, sollten die Mitarbeiter, die dieses System nutzen, über dieses Problem aufgeklärt werden. Dies soll verhindern, dass das Problem erneut auftritt, während man an einer Lösung arbeitet, die das Problem ausschaltet.

Für detaillierte Beispiele aus der Wirtschaft siehe Kapitel 6 Beispiele aus der Wirtschaft Seite 31.

Welches der Schutzziele auch verletzt wird, wichtig ist für ein Unternehmen, welche Kosten bei einer solchen Verletzung auf es zukommen. Wie solche analysiert werden zeigt das folgende Kapitel.

2.4 Monetäre Schäden

Ein wichtiger Punkt bei der Betrachtung von IT-Risiken ist die Ermittlung wie hoch der Schaden beim Eintritt eines Risikos ist.

Diese Betrachtung versucht klar erkennbare Kosten genauso zu berücksichtigen, wie schwer erkennbare Kosten.

Als Beispiel hierfür kann man sich ein Online-Versandunternehmen vorstellen, das durch den Ausfall eines Servers seinen Kunden für eine Stunde nicht zu Verfügung steht. Die Kosten für eine Reparatur lassen sich gut einschätzen. Auch die Kosten, die durch nicht getätigte Käufe innerhalb dieser Stunde entstehen, kann man noch gut schätzen. Hierfür betrachtet das Unter-

nehmen seine Daten um festzustellen, wieviel innerhalb dieser Stunde im Schnitt umgesetzt wird. Hier kann auch die Zeit mit eingerechnet werden. So wird ein Ausfall mitten in der Nacht weniger Kosten verursachen als einer der am Nachmittag eintritt.

Größere Probleme bereitet es einzuschätzen, wie groß der Schaden durch den eventuellen Reputationsverlust ist. Dieser kann durch verschiedene Faktoren beeinflusst werden. So wird ein etabliertes Unternehmen vielleicht keinen großen Verlust erleiden. Es hat seine zufriedenen Kunden, die ein solches Problem verzeihen würden, sofern es nicht häufig auftritt. Ein neues Unternehmen, das erst seit kurzem existiert, kann durch einen solchen Vorfall wiederum zu einem sehr schlechten Ruf gelangen und damit einen sehr hohen monetären Schaden davontragen. Der Faktor wie lange ein Unternehmen existiert, soll hier nur ein Beispiel sein. Die Faktoren um so etwas wie einen Reputationsverlust zu ermitteln sind zahlreich und von Unternehmen zu Unternehmen, von Branche zu Branche, unterschiedlich und können teilweise auch mit Glück oder Unglück zu tun haben. Wie das Beispiel der Uhrzeit des Problemeintritts schon zeigt.

Das sind Gründe, warum die monetären Kosten eines Reputationsverlusts schlecht zu beziffern sind. Dazu kommen auch Prozesse in Unternehmen, die schlecht monetär zu bewerten sind.

„Viele Fertigungsunternehmen sind nicht in der Lage, den Gesamtschaden bei einem Ausfall zentraler ERP- und PPS-Systeme und einem daraus resultierenden Produktionsstillstand *exakt* zu ermitteln. Ursache sind fehlende Grunddaten, komplexe oder undokumentierte Prozesse, die Vielzahl von betroffenen Personen, zu detaillierte Kosten- und Verrechnungsstrukturen und veraltete Verzeichnisse genutzter Maschinen und deren Steuerungen.“ (Knoll, 2014, S. 21 f.)

Das Problem, das ein nicht genau errechenbarer monetärer Schaden mit sich bringt ist, dass es schwerer wird zu entscheiden, ob ein Risiko hinnehmbar ist oder nicht.

Neben der Analyse der Kosten ist vor allem die Wahrscheinlichkeit eines Risikos zu beachten. Dies erklärt das nächste Kapitel.

2.5 Wahrscheinlichkeit von Risiken

2.5.1 Allgemein

Wenn man Risiken bewertet kann man nie genau sagen wann, oder ob das Risiko eintritt. Man kann nur versuchen, eine möglichst genaue Wahrscheinlichkeit dieser Ereignisse festzulegen, um sie einschätzen zu können. Ein Problem ist hier, dass Einschätzungen immer von Menschen vorgenommen werden, die auch subjektiv handeln. Sei es bei Teileinschätzungen des Risikos oder beim gesamten Risiko. So kann es passieren, dass zwei verschiedene Menschen zu sehr unterschiedlichen Ergebnissen kommen, oder zumindest zu unterschiedlichen Ergebnissen. Wenn dieser Wert nicht zu weit auseinander liegt kann es sogar helfen, ein Risiko besser einzuschätzen. So kann man versuchen einen Mittelwert zu finden oder aber einen Bereich angeben, der zeigt wie hoch die Wahrscheinlichkeit ist. Angenommen mehrere Mitarbeiter sollen ein Risiko bewerten, die einzelnen Personen können Werte zwischen 30% und 40% berechnen. Man hat verschiedene Möglichkeiten mit diesen Werten umzugehen. Es könnte der Mittelwert der einzelnen Punkte errechnet werden, um dann diesen als Risikowahrscheinlichkeit anzugeben. Alternativ kann man aber auch sagen, dass das Risiko zwischen 30% und 40% liegt, oder ein Gebiet um die meisten Einschätzungen wählen.

Das Problem ist die Wahrscheinlichkeiten gut errechnen zu können. Denn hierfür müssen Daten zur Verfügung stehen, die man dann zum Errechnen nutzen kann. Da im eigenen Unternehmen allerdings meistens nicht schon alle Risiken aufgetreten sind, muss man sich hier oft auf externe Daten verlassen. Diese müssen dann auf die eigene Firma angewendet werden. Auch hier sind oft Anpassungen nötig, da ein Risiko nicht immer von einer Firma zur nächsten eins zu eins übertragbar ist.

Bei Hardware gibt es oftmals Angaben der Hersteller über die Wahrscheinlichkeit eines Ausfalls. Festplatten, Netzteile und alle anderen Komponenten im gesamten Informationssystem können so hinsichtlich ihrer theoretischen Lebensdauer betrachtet werden. Dies ist vor allem an kritischen Punkten des Systems wichtig. Diese Wahrscheinlichkeiten können schon beim Aufbau eines Systems helfen, um hier möglichst geringe Ausfallwahrscheinlichkeiten zu gewährleisten. Bei längerem Einsatz von bestimmter Hardware können dann mit den gesammelten Daten auch eigene Statistiken zu Grunde gelegt werden. Zwar können auch eigene Statistiken nicht korrekt sein, aber zumindest werden sie mit der Motivation generiert, dem Unternehmen zu helfen und nicht um ein Produkt anzubieten.

Das Problem mit externen Daten ist, sie können selbst zu einem Risiko werden. Falls man sie nicht verifizieren kann, könnten sie sich als falsch herausstellen. Entweder weil sie nicht genau gemessen wurden, oder weil sie für das eigene Unternehmen nicht übertragbar waren. Falsche Werte in diesem Bereich können die gesamte Einschätzung eines Risikos verfälschen. So könnte das Risiko deutlich höher oder tiefer sein als errechnet und damit ganz andere Maßnahmen benötigen, als getroffen wurden.

Es folgen zwei Beispiele, für ein besseres Verständnis zu diesem Thema.

2.5.2 Beispiele Eintrittswahrscheinlichkeit

1. Ein System hat zur Redundanz zwei Router parallel in Betrieb. Wenn einer ausfällt, kann der andere die Last übernehmen. Die beiden Router sind von verschiedenen Herstellern. Der eine hat eine Ausfallwahrscheinlichkeit von 0,2%, der andere eine von 0,1%. Das Gesamtrisiko errechnet sich durch die Multiplikation der beiden einzelnen Ausfallwahrscheinlichkeiten. In diesem Fall rechnet man 0,2%×0,1% und kommt so auf ein Ergebnis von 0,02%. Die Wahrscheinlichkeit für einen kompletten Ausfall des gesamten Systems sinkt so also von 0,2% auf 0,02%.

   Die Aufstellung des zweiten Routers kann schon eine Entscheidung des IT-Risikomanagements gewesen sein, um das Risiko mit nur einem Router stark zu senken. So wurde die Wahrscheinlichkeit von 0,1%, wenn der bessere Router aufgestellt war, auf 0,02% gesenkt.
2. Für das zweite Beispiel wird angenommen, dass das System statt zwei parallelen Routern, zwei hintereinander in Reihe gesetzte Router besitzt. Die Ausfallwahrscheinlichkeit der beiden einzelnen Router ist der gleiche Wert wie im vorherigen Beispiel. In diesem Fall wird die Wahrscheinlichkeit eines Ausfalls mit 1-[(1-0,002)×(1-0,001)], also 0,2998% errechnet. Dass die Wahrscheinlichkeit insgesamt steigt ist logisch, da der Ausfall auch nur einer Komponente zum Ausfall des Systems führen würde. Ein funktionierender Router würde nicht genügen.

Wenn die monetären Schäden und die Wahrscheinlichkeit bekannt oder geschätzt sind, kann man das Risiko analysieren. Darüber handelt das folgende Kapitel.

2.6 Risikoanalyse

Um ein Risiko nun zu bewerten, werden die Daten aus Kapitel 2.4 Monetäre Schäden und Kapitel 2.5 Wahrscheinlichkeit von Risiken zusammengeführt.

So wird der Blick nicht nur auf einen der beiden Faktoren gerichtet, sondern beide Faktoren gewertet. Die Gewichtung ist hier ein Faktor, der bei verschiedenen Unternehmen stark voneinander abweichen kann.

Manche Unternehmen sind bereit ein höheres Risiko einzugehen als andere. Das bedeutet, manche Unternehmen würden ein geringes Risiko, welches hohen Kosten produzieren würde, unbehandelt lassen, während andere Unternehmen schon geringe Risiken, mit wenig Kosten behandeln lassen (Siehe Abbildung 2).

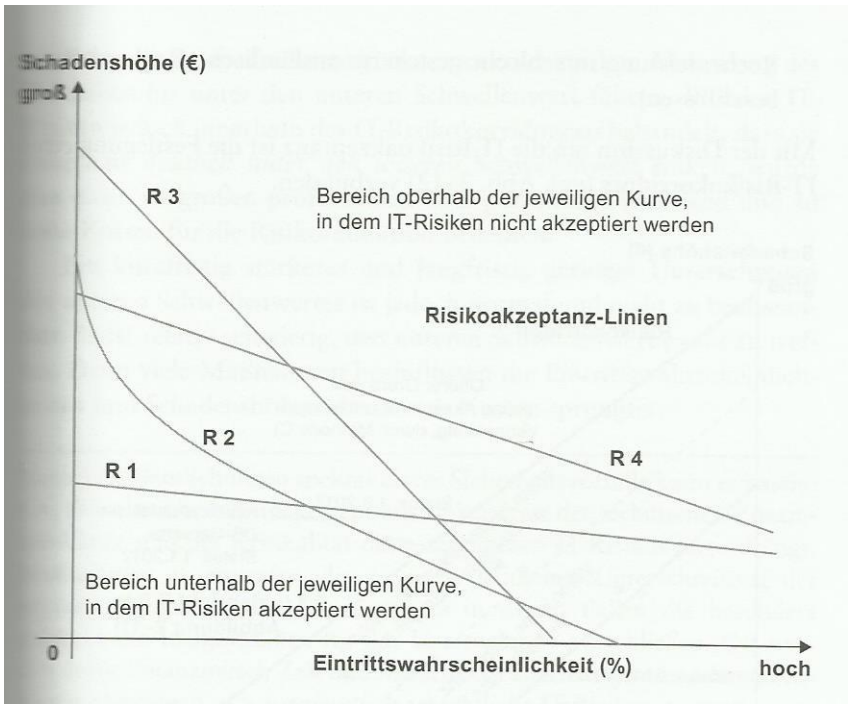

Abbildung 2 IT-Risikoakzeptanz, Schadenshöhe in Relation zur Eintrittswahrscheinlichkeit

„IT-Risikoakzeptanz (IT-Risikotoleranz) und IT-Risikotragfähigkeit

Die IT-Risikoakzeptanz gibt in Abhängigkeit von der IT-Risikoneigung und der IT-Risikotragfähigkeit an, bis zu welcher Höhe ein IT-Risiko akzeptiert werden kann.

Die IT-Risikotragfähigkeit wiederum ergibt sich aus den finanziellen Möglichkeiten unter Berücksichtigung der Interessen der Eigentümer eines Unternehmens.“ (Knoll, 2014, S. 46)

Auf Abbildung 2 kann man verschiedene exemplarische Denkweisen erkennen.

Die Risikoakzeptanzlinie R1 steht für ein eher risikoscheues Unternehmen. Schäden ab einer bestimmten, nicht sehr hohen Summe werden als nicht akzeptabel eingestuft. Allerdings nehmen sie dafür auch Risiken mit einer sehr hohen Wahrscheinlichkeit in Kauf, wenn die Schadenssumme nicht zu hoch ist. R4 ist eine etwas Risiko affinere Version von R1. Der Schaden darf höher sein als bei R1, bevor sie reagieren, dabei fällt die Gerade allerdings auch schneller ab. Ansonsten ähneln sich die beiden Kurven aber sehr.

Bei der Geraden R3 werden das Risiko und der Schaden stark zueinander in Relation gesetzt. Auch wenn die Schadenshöhe schon recht groß ist, werden Risiken mit geringer Wahrscheinlichkeit toleriert. Die Toleranz sinkt aber mit wachsender Wahrscheinlichkeit sehr rapide ab, so dass ab einer bestimmten Wahrscheinlichkeit kein einziges Risiko mehr hinnehmbar ist. Oder nur solche, die sehr geringe Kosten verursachen würden.

Die Risikoakzeptanzlinie R2 hingegen nimmt bei einer geringen Wahrscheinlichkeit noch eine hohe Schadenshöhe hin, fällt dann aber sehr schnell ab, wenn die Wahrscheinlichkeit steigt. Danach bleibt sie auf einen relativ konstanten Level, bis so gut wie kein Risiko mehr tragbar ist.

Ein dritter Faktor, der hier mit eingefügt wird ist, welche Kosten die Gegenmaßnahmen verursachen, die zur Verhinderung oder zur Senkung der Wahrscheinlichkeit des Eintritts eines Risikos nötig wären.

So kann ein Risiko verhindert werden. Es zu verhindern kostet aber eine bestimmte Summe für Personal und Hardware. Wenn diese Summe die Kosten übersteigt, die damit verhindert werden, ergibt es wirtschaftlich keinen Sinn.

Zum Beispiel ergibt es keinen Sinn, ein Risiko welches die Firma beim Eintreten 10.000 € kosten würde, mit Gegenmaßnahmen zu verhindern, die 50.000 € kosten. Natürlich können hier auch andere Faktoren eine Rolle spielen. So könnten die 50.000 € ein einmaliger Kostenpunkt sein und das Risiko kann häufig eintreten. Außerdem können bei den Kosten weiche Faktoren, wie Reputationsverlust, eventuell nicht mit eigerechnet werden, weil nicht bekannt. Auch dann kann überlegt werden, ob diese Kosten gerechtfertigt sind. Es kann auch möglich sein, das Risiko an eine Versicherung zu verlagern (Risikoverlagerung). Hier greifen aber dieselben Mechanismen wie zuvor, die Versicherungssumme muss sich für das Unternehmen rentieren.

Genaue Methoden zur Umsetzung der in diesem Kapitel besprochenen Themen, finden sich im nächsten Kapitel.

3 Methoden und Werkzeuge

Laut Knoll (Knoll, 2014, S. 14) kann man alle Werkzeuge und Methoden in ursachenorientiert und wirkungsorientiert aufteilen. Dazu kann man sie noch in quantitative Risikoanalyse oder qualitative Risikoanalyse kategorisieren. „Die Verfügbarkeit von Zeit und Budget und das Bedürfnis nach qualitativen oder quantitativen Aussagen zum Risiko und zu den Auswirkungen bestimmt, welche Methode(n) für das jeweilige Projekt angewendet wird/werden.“ (projektmanagement-definitionen.de, 2016)

Die qualitative Analyse wird im folgendem behandelt.

3.1 Qualitative Risikoanalyse

Nach der Webseite projektmanagement-definitionen.de (projektmanagement-definitionen.de, 2016), priorisiert die qualitative Analyse die Risiken für eine weiterführende Analyse oder eine Maßnahme.

Die qualitative Analyse analysiert für die weiterführende Analyse die Eintrittswahrscheinlichkeit und die Auswirkungen eines Risikos. Die Eintrittswahrscheinlichkeit und die Auswirkungen werden dann kombiniert. Auch werden andere Faktoren, wie Zeitrahmen, Kosten und Qualität erfasst.

Die qualitative Analyse gibt hier keine spezifischen Werte an, sondern bewertet die Kosten, Eintrittswahrscheinlichkeit oder das Risiko mit Aussagen wie leicht, mittel oder schwer.

Außerdem wird sie genutzt, um weitere Risiken zu identifizieren, auf die dann weitere Maßnahmen wie die quantitative Risikoanalyse angewendet werden können. Um diese geht es im folgenden Kapitel.

3.2 Quantitative Risikoanalyse

Die Webseite projektmanagement-definitionen.de (http://projektmanagement-definitionen.de, 2016), definiert eine quantitative Risikoanalyse wie folgt.

Die quantitative Analyse wird auf Risiken angewendet, die im Prozess der qualitativen Risikoanalyse identifiziert wurden. Die quantitative Risikoanalyse hilft, die Auswirkung dieser Risiken zu identifizierten und zu analysieren. Nach der Analyse des Risikos, wird dieses nu-

merisch eingestuft. Das bedeutet, dass im Gegensatz zur qualitativen Analyse das Risiko mit konkreten Werten angegeben wird. Wahrscheinlichkeiten so zum Beispiel mit Prozentzahlen oder Kosten in Euro.

Mit einer quantitativen Methode beschäftigt sich das nächste Kapitel.

3.3 Dreipunktschätzung

Laut Knoll (Knoll, 2014, S. 158) lässt sich die Dreipunktschätzung zu den quantitativen Analysen zählen. Sie kann sowohl für ursachenorientierte Analysen, als auch für wirkungsbezogene Analysen genutzt werden.

Die Dreipunktschätzung wird häufig verwendet, weil sie relativ einfach anzuwenden ist und dabei gute Werte liefern kann.

Dabei ist die Methode relativ simpel anzuwenden. Bei der Dreipunktschätzung werden möglichst viele Personen befragt. Diese Personen sollten gute Schätzungen über ein Risiko abgeben können. Dabei sollen die Befragten einzelnen Wert schätzen, sondern drei verschiedene Werte angeben. Der erste Wert soll versuchen eine realistische Schätzung abzugeben. Der zweite soll wiederum eine pessimistische Schätzung sein und der dritte eine optimistische Schätzung. Hierbei kann man sowohl die Eintrittswahrscheinlichkeit errechnen als auch die Schadenshöhe. Je nachdem was man errechnen will.

Die Rechnung an sich ist eine einfache Ermittlung des Durchschnittwertes. Mit dem Unterschied, dass der reale (real) Wert eine höhere Gewichtung (der Vierfachen) als die anderen beiden bekommt. Der pessimistische (pess) und der optimistische (opt) Wert werden hingegen mit derselben Gewichtung gerechnet (der Einfachen). Der Grund für die verschiedenen Gewichtungen ist, dass der reale Wert so einen höheren Stellenwert einnimmt. Da der reale Wert, der am stärksten zu erwartende ist, würde eine gleiche Gewichtung mit dem optimistischen und pessimistischen Wert zu einer zu starken Verschiebung in die pessimistische oder optimistische Richtung bedeuten.

$$x = (x_{pess} + 4x_{real} + x_{opt})/6$$

Da sich die befragten Personen nicht nur auf einen Wert festlegen müssen, sondern drei angeben, ist die Bereitschaft höher konkrete Werte anzugeben. Bei nur einem Wert, müssten Befragte den realen, pessimistischen und realen Wert als einen einzigen Wert angeben. Die

Hemmschwelle liegt hier niedriger, da ungern nur ein Wert geschätzt wird, der sich beim Eintreten des Risikos dann als zu pessimistisch oder optimistisch herausstellt. Von daher ist die Dreipunktschätzung auch für Schätzungen, bei unerfahrenen Befragten geeignet. Auch für schwer einschätzbare Risiken kann man so einen besseren Wert finden. (vgl. Knoll, 2014, S. 159; Jendryschik, 2009)

Nach dieser quantitativen Risikoanalyse folgt eine qualitative Risikoanalyse.

3.4 Post-mortem-Analyse

Für eine Post-mortem-Analyse benötigt man im IT-Risikomanagement einen abgeschlossenen Sachverhalt. Dieses Analyseverfahren ist ein qualitatives, ursachenorientiertes Verfahren. Im Gegensatz zu dem, was der Name suggeriert[1], muss der zu untersuchende Sachverhalt nicht negativ ausgegangen sein. Auch ein zur Zufriedenheit abgeschlossenes Projekt kann untersucht werden. Allgemein wird die Post-mortem-Analyse dazu genutzt, um die tatsächliche Reaktion bei Risikoeintritt zu untersuchen. Dabei ist es unerheblich, ob diese Reaktion Wirkung gezeigt hat oder nicht.

Ein großer Vorteil der Post-mortem-Analyse ist, dass sie frei gestaltbar ist. Es können Umfragen genutzt werden, Workshops oder auch weitere Möglichkeiten, die für sinnvoll erachtet werden. Da oftmals die für die Analyse notwendigen Daten bereits vorliegen, ist die Vorbereitung schnell abgeschlossen. Auch die für das Projekt zuständigen Mitglieder können leicht ermittelt und einbezogen werden. Diese Mitglieder können schnell lernen, welche Fehler begangen wurden und für das nächste Projekt nutzen.

Ein Nachteil ist hingegen, dass die Analyse relativ zeitaufwendig ist. Gerade bei Sachverhalten, die positiv geendet sind, kann es schwierig sein, die Zeit hierfür aufzubringen. Zudem kann es durch Zuweisung von Schuld bei negativen Sachverhalten zu Konflikten innerhalb des Teams kommen. Dazu kann es, gerade bei großen Unternehmen, schwierig sein, alle Beteiligten an dem Projekt an der Analyse zu beteiligen. Was positive Aspekte, wie Lerneffekte bei den Mitgliedern, konterkarieren kann (vgl. Knoll, 2014, S. 173; Wolf, 2010).

Ein gutes Beispiel für den Einsatz der Post-mortem-Analyse ist Schach. Beim Schach wird diese Analyse gerne nach Schachpartien von den beiden Kontrahenten eingesetzt. Sie besprechen einzelne Züge und spielen Situationen noch einmal durch. So können sie lernen, wo Feh-

[1] Post mortem bedeutet nach dem Tod

ler gemacht wurden, oder wo sie positive Züge getätigt haben. Hier erkennt man, dass die Analyse auch nach einem positiven Resultat genutzt werden kann. Der Sieger einer Schachpartie kann von einer Post-mortem-Analyse ebenfalls profitieren, da er noch einmal sieht, zu welchem Zeitpunkt eine Reaktion positiv war. Aber auch wo er eventuell Fehler, trotz des positiven Ergebnisses, begangen hat (vgl. chess24.com, 2016).

Im nächsten Kapitel wird ein wirkungsbezogenes Verfahren vorgestellt.

3.5 IT-Risikokennzahlen

IT-Risikokennzahlen sind eine wirkungsbezogene, qualitative und quantitavive Methode, zu der Einschätzung von Risiken.

„Eine IT-Risikokennzahl beschreibt ein IT-Risiko einschließlich möglicher Ursachen und Auswirkungen oder die Wirkung von Maßnahmen. Sie kann die tatsächliche oder angestrebte IT-Risikolage darstellen.

Qualitative IT-Risikokennzahlen beschreiben Sachverhalte verbal und subjektiv, etwa durch Begriffe wie „hoch“, „stark“ oder „angemessen“.

Quantitative IT-Risikokennzahlen beschreiben Sachverhalte über mathematischen Beziehungen und nachprüfbare Messvorschriften.“ (Knoll, 2014, S. 164)

Beispiele:

- die Anzahl eingehender Spam-Mails in Relation zu den insgesamt empfangenen E-Mails. Bezogen auf einen Zeitraum, zum Beispiel pro Tag, pro Monat oder pro Jahr.
- Temperatur- und Spannungswerte in Serverschränken
- die Datenmenge, die pro Tag oder Monat über einen bestimmten Router läuft (auch möglich mit Tag oder Nacht)
- datenschutzrelevante Anwendungen im Vergleich zu den nicht datenschutzrelevanten Anwendungen
- die Anzahl der Angriffe von außen auf einen bestimmten Teil des Systems (z.B. die Netzwerkaußengrenze)
- wie viele Fehler sind in einem Quellcode enthalten. Relation zwischen Anzahl der Zeilen mit Fehlern, in einem frei wählbaren Abschnitt von Zeilen

Kennzahlen werden je nach Anforderungen oder im Rhythmus der normalen Berichterstattung über die IT-Risikolage aktualisiert. (Knoll, 2014, S. 164)

Eine ermittelbare Kennzahl ist die Risikoprioritätszahl (RPZ). Mit Hilfe dieser Kennzahl kann ermittelt werden, wie hoch das IT-Risiko ist. Um sie zu ermitteln benötigt man drei verschiedene Werte.

1. Die Entdeckungswahrscheinlichkeit eines Fehlers (E)
2. Die Wahrscheinlichkeit, dass der Fehler auftritt (W)
3. Der Schweregrad des resultierenden Schadens (S)

Allen drei Punkten wird ein Wert zwischen 1 und 10 zugewiesen. Mit 1 als geringe Wahrscheinlichkeit oder Schaden, bis 10 als hohe Wahrscheinlichkeit oder Schaden. Für den Schweregrad kann die Einschätzung von 1 bis 10 über die Einschätzungen von nicht existent bis katastrophal ermittelt werden. Bei den beiden Wahrscheinlichkeitswerten kann man alle zehn Prozent den Wert um eins erhöhen. So hätte eine Wahrscheinlichkeit von 0% bis 10% den Wert 1 (extrem gering) und die Wahrscheinlichkeit von 91% bis 100% einen Wert von 10 (fast sicheres Eintreten). Um hieraus die RPZ zu ermitteln, werden die drei Kennzahlen miteinander multipliziert.

$$RPZ = E * W * S$$

Damit kann der RPZ einen Wert zwischen 1 und 1000 annehmen. Bei dem RPZ 1 ist das IT-Risiko sehr gering. Bei einem RPZ 1000 ist das Risiko äußerst kritisch. (Prof. Dr. Johner, 2015)

Um zum Beispiel die Eintrittswahrscheinlichkeit einer nicht Verfügbarkeit von Daten oder nicht Verfügbarkeit eines Internet-Shops zu senken, könnte ein Hochverfügbarkeitsnetzwerk helfen. Im folgenden Kapitel soll nun eine solche praktische Maßnahme, ein Risiko zu senken, erläutert werden.

4 Praktische Maßnahmen zur Senkung von Risiken

4.1 Hochverfügbarkeitsnetzwerke

Hochverfügbarkeit ist ein Begriff, der in der IT beschreibt, dass ein System zu hohen Prozentzahlen zur Verfügung steht. Nach der Havard Research Group (HRG) muss dies zu 99,999% möglich sein. Das bedeutet, in einem Jahr darf das System wenig mehr als fünf Minuten ausfallen. Hierbei ist es unerheblich, ob diese fünf Minuten bei einem Fehlerfall auftreten, oder über das Jahr verteilt bei mehreren Fällen mit einer geringeren Ausfallzeit pro Fall. Bei mehreren Fällen darf die Summe der Ausfallzeiten die fünf Minuten nicht überschreiten.

Um eine so hohe Verfügbarkeit zu erreichen, ist Redundanz wichtig. Es sollten möglichst alle Komponenten eines Systems redundant sein, damit im Falle eines Fehlers eine andere Komponente übernehmen kann. Besonders wichtig ist es hierbei, keinen Single Point of Failure zuzulassen. Ein solcher Punkt in einem System würde bei einem Fehler das gesamte System zum Erliegen bringen. (vgl. www.itwissen.info/, 2016)

Abbildung 3 zeigt die Darstellung eines Hochverfügbarkeitsnetzwerkes. Diese Darstellung ist allerdings nicht repräsentativ. Hochverfügbarkeitsnetzwerke können in verschiedenen Formen aufgebaut werden. Hierbei wird die Anforderung des aufbauenden Unternehmens berücksichtigt.

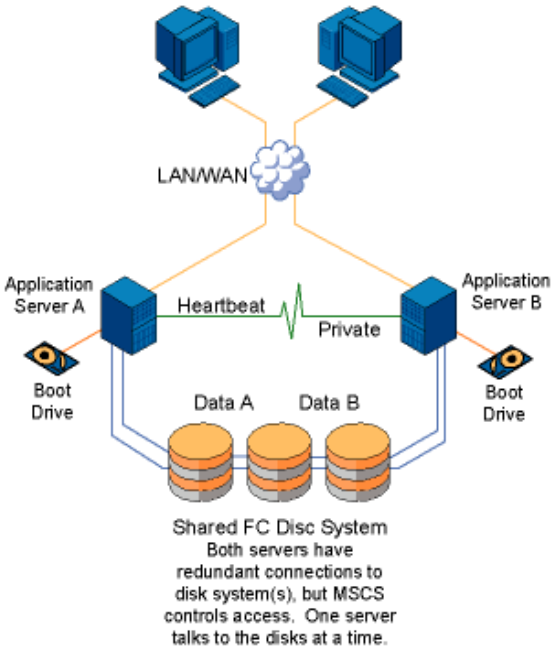

Abbildung 3 Darstellung eines Hochverfügbarkeitsnetzwerkes

Auf der Abbildung kann man erkennen, dass die Computer der Endbenutzer über ein LAN oder WLAN mit den Servern kommunizieren können. Welche Route für den Zugriff auf die Daten genutzt wird, ist für den Endbenutzer nicht zu erkennen und unbedeutend. Der Benutzer braucht nur den Zugang zu den Daten.

Interessant wird es, wenn in einem der Server ein Fehler vorliegt. Wenn statt der zwei Server nur einer zur Verfügung stehen würde, würde dadurch das gesamte System ausfallen. Der Benutzer hätte keine Möglichkeit mehr, auf die Daten zuzugreifen. Durch die Redundanz des Serversystems kann dieses Problem aber umgangen werden. Im günstigsten Fall merkt der Benutzer beim Zugriff auf das System nicht, dass einer der Server ausgefallen ist. Im schlechtesten Fall muss die Anfrage erneut gestartet werden, um die Anfrage über den funktionierenden Server zu leiten.

Wichtig hierbei ist die Kommunikation der beiden Server untereinander. Wenn einer der beiden ausfällt, muss dem anderen um übernehmen zu können, mitgeteilt werden, dass der andere Server ein Problem hat. Ob dieses Problem die Hardware oder die Software betrifft, ist hierbei unerheblich. Hierfür ist ein sogenannter Cluster Manager zuständig. Der Cluster Manager ist eine Software, die alle Dienste überwacht um eingreifen zu können, wenn ein Problem auftritt. Selbst wenn eventuell nur ein einzelnes Programm auf einem Server ausgefallen ist, sollte dies sofort erkannt und eventuelle Last umgeleitet werden. (vgl. Loschwitz, 2011)

Beispiele für Open Source Cluster Manager oder Programmen, die die Funktionen zumindest teilweise übernehmen können sind:

1. pacemaker
2. OpenAIS
3. Heartbeat

Mit Hilfe eines Hochverfügbarkeitsnetzwerkes kann ein System eine hohe Verfügbarkeit bieten. Theoretisch ist es möglich das System so redundant zu gestalten, dass die Ausfallwahrscheinlichkeit Richtung Null geht. Das Problem hierbei ist, dass die Kosten dabei extrem hoch werden würden. Für eine solch extreme Verfügbarkeit bräuchte es redundante Systeme auf der ganzen Welt, um selbst nach Naturkatastrophen verfügbar zu sein.

Ein solches System wäre zwar sicher, zeigt aber auf, dass auch bei Hochverfügbarkeitsnetzwerken die Risikoanalyse Vorrang hat.

- Wie weit soll das Risiko abgesenkt werden?
- Welche Kosten entstehen, um das Risiko auf einen bestimmten erwünschten Wert abzusenken?
- Wie hoch wären die Kosten bei einem Störfall?
- Was ergibt Sinn, wenn man die vorherigen Punkte zusammenführt?

Dadurch sind solche Aufbauten, je nach Unternehmen, unterschiedlich. Die Anforderungen und die Kosten bestimmen was benötigt wird. Dies kann ein relativ einfaches System wie in Abbildung 3 bedeuten, aber auch mehrere solche Systeme an verschiedenen Standorten, um Effekte wie Stromausfall auszuschließen.

Falls es zu einem Störfall kommt, auch wenn dieser durch ein zweites System aufgefangen wird, benötigt es einen Wiederanlaufplan, der im folgenden Kapitel beschrieben wird.

4.2 Wiederanlaufpläne

Das BSI beschreibt einen Wiederanlaufplan wie folgt:

„Diese Dokumente beschreiben die Handlungsschritte für die **Wiederherstellung oder den Wiederanlauf wichtiger Ressourcen,** die Priorität, mit der diese Schritte erfolgen müssen sowie die zugehörigen Verantwortlichkeiten. Wiederanlaufpläne umspannen einen Zyklus beginnend mit der Fehlerbehebung und der Aufnahme des Notbetriebs, beispielsweise dem Anlauf eines Ausweichrechenzentrums, der Inbetriebnahme alternativer Produktionsanlagen oder der Einrichtung mobiler Arbeitsplätze, bis hin zur Rückführung in den Normalbetrieb.“ (BSI, www.bsi.bund.de, 2016)

Ein Wiederanlaufplan kann für einen einzelnen Server, aber auch für ein komplettes Rechenzentrum erstellt werden. In beiden Fällen ist es wichtig, einen Plan mit dem Ablauf des Wiederanlaufens oder der Wiederherstellung zur Verfügung zu haben.

Der Wiederanlaufplan kann für verschiedene Zwecke genutzt werden.

1. Wiederanlauf im Normalbetrieb
2. Wiederanlauf im Notfallbetrieb

Auch wenn der Wiederanlaufplan vor allem in Notfallsituationen genutzt wird, kann der Plan auch bei monatlichen Updates oder Kontrollabschaltungen genutzt werden. Hier werden dann einige Punkte, die im Wiederaufbauplan für den Notfall enthalten sind, ignoriert. Dies hat den Vorteil, dass zuständige Mitarbeiter mit dem Umgang der Wiederaufbaupläne geschult sind und so im Notfall eventuell besser reagieren können (vgl. Online Redaktion Docusnap, 2014), da einige der Handlungsweisen zum normalen Ablauf gehören. Wiederanlaufpläne sind auch ein Teil der ISO27001 Norm, diese wird im nächsten Kapitel erläutert.

5 ISO27001

ISO27001 ist der einzige internationale Standard, der die Anforderungen an ein Information Security Management System (ISMS) definiert. Unternehmen, die ein qualitativ hochwertiges Sicherheitsmanagement einhalten wollen und dies auch belegt haben wollen oder müssen, können sich nach ISO27001 zertifizieren lassen.

Die Norm ist in die Standards des Bundesamts für Sicherheit in der Informationstechnik eingebettet worden. Diese Standards sollen helfen, IT-Sicherheit zu gewährleisten. Das BSI empfiehlt hier drei IT-Grundschutz-Kataloge umzusetzen.

1. BSI Standard 100-1 Managementsysteme für Informationssicherheit
2. BSI Standard 100-2 IT-Grundschutz-Vorgehensweise
3. BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz

(vgl. BSI, 2016)

Wichtig ist die Zertifizierung, neben dem Erhöhen der eigenen Sicherheit, vor allem für die Umsetzung gesetzlicher Vorgaben, Anforderung durch Kunden, Aufsichtsbehörden oder auch Banken. Dazu kommt noch der Bereich der Haftung. Dieser verlangt häufig, dass die verkehrsübliche Sorgfaltspflicht eingehalten wird. Ein Zertifikat reicht hier unter normalen Umständen aus, um dies zu belegen. Weiterhin ist zu beachten, dass bei öffentlichen Ausschreibungen auch ein International gültiges Zertifikat benötigt werden kann. Da europäische Richtlinien ein nationales Zertifikat bei Ausschreibungen nicht zulassen, ist hier das internationale ISO27001 Zertifikat nötig. (vgl. Reiss & Sportelli, 2016)

Um sich zertifizieren zu lassen, wird ein Audit von externen Testern durchgeführt. Interne Tester sind nicht gestattet. Solche Audits werden beispielsweise durch zertifizierte Mitarbeiter des BSI durchgeführt. (vgl. BSI, 2016)

Kernpunkt der ISO27001 Zertifizierung ist, das Verständnis der Informationssicherheit als kontinuierlichen Prozess, der gelebt, geplant und überwacht wird. Dazu muss fortwährend an der Verbesserung und Aufrechterhaltung der Informationssicherheit gearbeitet werden. Dem zugrunde liegt das „Plan-Do-Check-Act-Modell“. (vgl. Reiss & Sportelli, 2016)

Das „Plan-Do-Check-Act-Modell“ ist ein Modell aus dem Management.

1. Plan: Plane eine Verbesserung für einen Punkt in der IT, wo Verbesserungspotential besteht. Dies kann auch bedeuten, funktionierende Systeme auf Verbesserungsmöglichkeiten zu überprüfen.
2. Do: Wenn eine Möglichkeit etwas zu verbessern gefunden und geplant wurde, führe diesen Plan aus. Es besteht auch die Möglichkeit den Plan auf kleinerer Ebene zu testen, sofern die bei der geplanten Veränderung möglich ist.
3. Check: Überprüfe die Umsetzung und analysiere die Ergebnisse. Entweder die aus dem Test oder aus der richtigen Anwendung. Abhängig wie Punkt zwei umgesetzt wurde.
4. Act: Überprüfe was aus Punkt drei zu lernen ist. Hat die neue Umsetzung keine Vorteile oder sogar Nachteile gebracht, verwerfe sie und starte wieder bei Punkt eins. Hat die neue Umsetzung positive Aspekte gehabt, starte größere Versuche, falls in Punkt zwei entschieden wurde zuerst kleinere Tests auszuführen, oder behalte die Änderung als neuen Standard bei. Auch in dem Fall, dass ein neuer Standard gesetzt wurde, fängt es wieder bei Punkt eins an.

(vgl. Tague, 2004, S. 390)

Grundsätzlich ist es wichtig nachzuweisen, dass ein solcher oder ähnlicher Prozess im Unternehmen umgesetzt wurde und gelebt wird. Hierfür ist es notwendig, dass eine Dokumentation der verschiedenen Umsetzungen und Maßnahmen erfolgt. (vgl. Reiss & Sportelli, 2016)

Auch eine Zertifizierung bietet keine hundertprozentige Sicherheit. Im folgenden Kapitel werden Beispiele von Problemfällen beschrieben.

6 Beispiele aus der Wirtschaft

Die Namen der Unternehmen wurden bei den Beispielen mit nicht öffentlich einsehbaren Problemen entfernt. Das erste Kapitel handelt von den Tochterfirmen der Firma Sony.

6.1 Hackerangriffe gegen Sony

Das Unternehmen Sony hatte mit seinen Tochterunternehmen schon häufig Probleme mit Hackerangriffen. So gab es 2011 einen Angriff auf das Sony Playstation Network, bei dem die Daten von mehreren Millionen Nutzer geklaut wurden. „Als Reaktion schaltete Sony die Plattform ab“. (Dr. Datenschutz, 2011)

Hier hatte Sony nicht nur die Kosten für die abgeschaltete Plattform und die Aufarbeitung der Probleme zu tragen, sondern auch die Kosten eines schwerer messbaren Reputationsverlusts.

Im Oktober 2014 gab es Berichte, dass es eine Sicherheitslücke auf der Website vom Playstation Network gibt. Hier soll es das Problem gegeben haben, „[…] durch eine SQL-Injection-Lücke Zugriff auf Kundendaten zu bekommen. Auf diese Berichte habe Sony aber nicht reagiert und die Sicherheitslücke nicht umgehend geschlossen.“ (Böck, 2014)

Bei diesem Fall entstanden keine direkten Kosten, aber gerade nach den Problemen 2011 hat es nicht geholfen, den Kunden Vertrauen einzuflößen und so zu einem weiteren Reputationsverlust geführt.

Im November 2014 hatte eine weitere Tochterfirma von Sony, die Sony Picture Entertainment, mit den Folgen eines Hackerangriffes zu kämpfen.

„So wurden interne Dokumente wie Gehälter, persönliche Mails oder auch noch unveröffentlichte Filme von den Hackern online gestellt.“ (Fuest, 2014)

Auch hier muss man neben den Kosten durch die veröffentlichten Filme, vor allem den Reputationsverlust beachten. In diesem Fall nicht nur durch die allgemeine Öffentlichkeit, sondern auch gegenüber Angestellten und Partnerunternehmen, die in internen Mails angegriffen wurden oder deren Gehalt öffentlich wurde.

Ein gutes IT-Risikomanagement hätte all diese Probleme im Idealfall komplett verhindern können. Ob ein Solches versagt hat, oder bei Sony zu dem Zeitpunkt überhaupt vorhanden war, ist von außen nicht zu sagen. Vielleicht war es auch vorhanden und die Kosten der Vorschläge des IT-Risikomanagements wurden als zu hoch angesehen oder die Risiken wurden falsch eingeschätzt.

Auch die Reaktion auf eine Sicherheitslücke deutet nicht auf ein gutes IT-Risikomanagement hin. Denn es ist unerheblich, ob ein Problem öffentlich bekannt wird, wie in diesem Fall, oder ausschließlich intern entdeckt wird, es muss von Unternehmensseite gehandelt werden.

Die beste Lösung wäre, das Problem sofort zu lösen. Dies ist aber nicht immer möglich. Der Fehler muss zuerst gefunden werden. Erst nach diesem Fund kann nach einer Lösung gesucht werden.

Wenn das Problem nicht öffentlich bekannt ist, kann entschieden werden das Problem möglichst schnell zu beheben, ohne das kritische System abzuschalten. In diesem Fall würde das Unternehmen ein Ausnutzen der Sicherheitslücke bis zu diesem Zeitpunkt in Kauf nehmen. Das Unternehmen muss hier einen Weg zwischen Kosten und Nutzen finden. Falls die Kosten beim Eintreten des Risikos hoch sind kann beschlossen werden, das System zu deaktivieren. Sind die Kosten niedrig kann versucht werden, die Sicherheitslücke ohne Deaktivierung zu lösen. Hierbei steht die Hoffnung, dass die Sicherheitslücke nicht ausgenutzt wird.

Wenn eine Sicherheitslücke allerdings öffentlich bekannt wird, sollte reagiert werden, um einen weiteren Reputationsverlust vorzubeugen. Hier hat man die Möglichkeit, das betroffene System mit der Sicherheitslücke vom Netz zu nehmen, oder offen zu kommunizieren, um möglichst schnell eine Lösung zu finden.

Eine Sicherheitslücke nicht zu kommunizieren und auch nicht vom Netz zu nehmen, steigert die Unsicherheit der Nutzer und führt so zu weiteren Reputationsverlusten. Es wird deutlich, dass es bei Sony zu viele große Vorfälle gab, um sie tolerieren zu können. Als weltweit agierendes Unternehmen sind fast jährlich auftretende schlechte Schlagzeilen in den Medien ein großes Problem für die Reputation und somit auch für den Umsatz.

In kleinerem Maßstab kann das folgende Beispiel zeigen, dass auch Mitarbeiter ein Problem im IT-Risikomanagement sein können.

6.2 Verbot von WhatsApp

Eine mittelständische Firma, die kein IT-Risikomanagement besitzt, hat seine Mitarbeiter angewiesen, den Instant-Messaging-Dienst WhatsApp nicht zu nutzen. Durch die nicht verschlüsselte Kommunikation (vgl. Trepesch, 2014) ist dieser Dienst dem Unternehmen zu gefährlich. Es wird befürchtet, dass interne Daten abgefangen werden könnten. Daten, mit denen dem Unternehmen Schaden zugefügt werden könnte.

Die Mitarbeiter empfinden dies allerdings als störend und benutzen den Dienst weiter, da es ihnen die Kommunikation mit Kollegen erleichtert. Außerdem hatte das Personal den Dienst schon vor dem internen Verbot genutzt und kann somit nicht nachvollziehen, warum sie wegen dieser Anweisung auf die Anwendung des Programms verzichten sollen. (persönliches Gespräch, 2016)

Ein gutes IT-Risikomanagement hätte hier nicht nur ein Verbot ausgesprochen, sondern versucht den Mitarbeitern durch Erklärungen deutlich zu machen, wo die Probleme beim Benutzen liegen.

Es hätte hierbei auch nicht nur eine Nachricht mit der Anweisung geschickt, sondern versucht das Problem durch verschiedene Ansätze deutlich zu machen. So könnte durch Schulungen versucht werden, das Problem zu erklären. Auch Aushänge oder Rundschreiben mit genauen Erklärungen können helfen.

Falls es sich abzeichnet, dass die Anweisung trotzdem missachtet wird, könnte auf Alternativen zurückgegriffen werden. So könnte man versuchen andere Instant-Messaging-Dienste zu finden, die das Problem, dass das Unternehmen mit WhatsApp hat, nicht besitzen.

Zum Beispiel könnte das Unternehmen seinen Mitarbeitern, eine Software wie Threema als Alternative anbieten. Da dieser Dienst seine Kommunikation verschlüsselt, wäre das Problem mit der unverschlüsselten Kommunikation gelöst.

Ein gutes IT-Risikomanagement könnte einen Umstieg auf eine geeignetere Lösung auch von vornherein vorschlagen. So würde gleichzeitig mit dem Verbot des alten Instant-Messaging-Diensts eine Alternative für die Mitarbeiter geschaffen. Da diese Alternative Geld kostet, müsste das Unternehmen entscheiden, ob es bereit ist Geld zu investieren.

Es muss hier allerdings berücksichtigt werden, dass eine Kommunikation der Mitarbeiter mit anderen Firmen eventuell nicht mehr so einfach möglich wäre, da der Kommunikations-

partner den gleichen Dienst bräuchte. Diese Einschränkung könnte zum weiteren Gebrauch des alten Dienstes führen.

Eine weitere Möglichkeit wäre, selber eine solche Software für das eigene Unternehmen zu schreiben oder in Auftrag zu geben. Hier könnten alle Anforderungen des Unternehmens berücksichtig werden und alle Sicherheitsaspekte somit gewährleistet werden. Die Frage ist, ob es dem Unternehmen wirklich hilft, einen solchen Dienst zu entwickeln, da die Kosten hierfür nicht unerheblich sind. Von der Programmierung bis zur benötigten Hardware und Wartung sind die Kosten ein nicht zu vernachlässigender Faktor.

Das Problem der Kommunikation mit Partnern außerhalb des eigenen Unternehmens bleibt allerdings auch hier, da die Mitarbeiter einer anderen Firma den eigenen Dienst nutzen müssten.

Dies sind alles Vorschläge, die ein IT-Risikomanagement den Entscheidungsträgern des Unternehmens bieten können. Gepaart mit Analysen, die aufzeigen welches Nutzungsverhalten die Mitarbeiter aufweisen. Welche Option die Entscheidungsträger dann wählen, ist eine Frage der Kosten und stellt für das Unternehmen ein finanzielles Abwägen der Kosten und Nutzen dar.

Für die mittelständische Firma in diesem Beispiel wäre eine eigene Software wohl deutlich zu kostenintensiv. Eine gute Kampagne, um zu erklären warum das Unternehmen die Nutzung von WhatsApp untersagt hat, wäre jedoch nicht mit großen Kosten verbunden. Auch der Aufwand auf eine Alternative umzusteigen, ist für das Unternehmen erschwinglich und könnten genutzt werden.

Am Ende sind es nicht nur die Kosten, die zu der Entscheidung führen, sondern auch der Nutzen für das Unternehmen. Wenn zum Beispiel am Anfang festgestellt wird, dass die Mitarbeiter aufgrund der Kommunikation mit anderen Firmen, weiterhin WhatsApp nutzen würden, mag eine alternative Software nicht sinnvoll erscheinen, geschweige denn eine eigene Software. Ist das der Fall, bleibt nur eine möglichst gute Aufklärung der Mitarbeiter, um das Problem zu lösen.

Neben den Mitarbeitern, kann auch das Management falsche Entscheidungen treffen, wie das folgende Kapitel aufzeigt.

6.3 Gesetzesänderung

Ein kleines Softwareunternehmen möchte/wollte SEPA-Überweisung für seine Software einführen.

Das bedeutet, das alte System mit Kontonummer und Bankleitzahl im Programm musste zu einem System mit der International Bank Account Number (IBAN) und dem Business Identifier Code (BIC), umgeändert werden.

Diese Anforderung war monatelang bekannt, die Umsetzung wurde aber zugunsten anderer, zu dem Zeitpunkt als wichtiger erachteten Problemen, immer wieder nach hinten versetzt. Wenige Tage vor dem verpflichtenden Termin der Gesetzesänderung, wurde die Anforderung für das Programm wieder entdeckt.

Nun musste dieses Problem gelöst werden. Durch ein nun enges Zeitfenster war das Unternehmen gezwungen das Programm überhastet zu überarbeiten. Am Ende dieses Vorganges war das Programm für die Gesetzesvorlagen umprogrammiert. Die Überarbeitung konnte aber nicht mit der üblichen Sorgfalt vorgenommen werden. So konnte die Qualität nicht gewährleistet werden, bevor es an die Kunden ausgeliefert wurde. Ein gutes IT-Risikomanagement hätte hier einen besseren Umgang mit der Gesetzesänderung erreichen können. Oder zumindest das Risiko eines schlechten Projetmanagement erkannt.

Zum Beispiel hätte das Risikomanagement von vornherein Zeitpläne erstellt, die eine Umsetzung und die Überprüfung des umgeschriebenen Programms einbezogen hätte. Zumindest hätte es auf das Fehlen eines Projektmanagement hingewiesen. Damit können nicht nur eventuelle Bugs beim Kunden verhindert werden, sondern auch eine vernünftige Programmierung gewährleistet sein. Dies unterbindet nicht nur Frustration beim Kunden und damit resultierende eventuelle Gewinneinbußen, sondern auch Unzufriedenheit bei den eigenen Mitarbeitern. Die Unzufriedenheit der Mitarbeiter ist nicht zu missachten, da Fehler in der Projektplanung und im Management nicht nur zu Frustration sondern auch zu Zeitdruck führen. Die Mitarbeiter können diesen Zeitdruck nicht nachvollziehen, da für die Umsetzung der benötigten Änderungen Monate Zeit waren. Dass diese Monate nicht genutzt wurden, kann somit auch psychische Schäden hinterlassen.

Unternehmen aus der freien Wirtschaft haben kein alleiniges Monopol auf schlechtes IT-Risikomanagement, wie das folgende Beispiel zeigen wird.

6.4 Hackerangriff auf den Bundestag

Mitte Mai 2015 wurde bekannt, dass das Netzwerk des Bundestages gehackt wurde. Nach Recherchen verschiedener Nachrichtenmedien (Süddeutsche Zeitung, 2015), erfolgte der Angriff laut Experten des Bundesamts für Sicherheit in der Informationstechnik (BSI) über eine E-Mail, die einen Link auf eine externe Seite enthielt. Nachdem Bundestagsabgeordnete diese Seite aufgerufen hatten, wurden die Computer dieser Personen mit der Schadsoftware der Hacker infiziert.

Sobald die Hacker durch diese Infizierung in das System eingedrungen waren, fingen die Angreifer bald auch Administratorkennwörter ab und konnten die volle Kontrolle über das Netzwerk erhalten. Die Angreifer sollen mehrere Gigabyte an Daten aus dem Netzwerk geladen haben. Diese Daten gingen an verschiedene Standorte und konnten nicht zurückverfolgt werden.

Auch nachdem der Angriff erkannt wurde, konnten die Angreifer noch über Tage weiter Daten aus dem Netzwerk entwenden. Das Herunterladen von Daten konnte erst durch das Abschalten des gesamten Systems für mehrere Tage gestoppt werden. Nach dem Herunterfahren des gesamten Systems soll sämtliche Schadsoftware entfernt worden sein. Nach dem Wiederhochfahren waren die E-Mails, die auf die Schadsoftware verlinken aber noch teilweise auf Computern zu finden. Dazu muss das gesamte IT-System ausgetauscht werden, was viel Zeit und Geld kosten wird.

Ein gutes IT-Risikomanagement hat hier eindeutig gefehlt, was man an Aussagen wie, „dass der Bundestag sich 2009, als die Entscheidung darüber anstand, nicht an das Netz der Bundesregierung angeschlossen hat. Dieses Netz wird vom BSI überwacht. Experten seien sich einig, dass der jüngste Angriff keinen Erfolg gehabt hätte, wenn die Regeln des BSI auch im Bundestag gegolten hätten.“ (Süddeutsche Zeitung, 2015) ersehen kann.

Ein IT-Risikomanagement scheint im Bundestag zu fehlen, auch wenn hier keine gesicherten Daten vorliegen. Die Größe dieses Angriffs, gepaart damit, dass das Netz der Bundesregierung deutlich besser abgesichert ist, deutet allerdings stark darauf hin, dass zumindest ein IT-Risikomanagement, sofern vorhanden, ignoriert wurde.

Regierungen arbeiten natürlich nicht so wie Unternehmen, von daher ist hier vielleicht ein normales IT-Risikomanagement nicht umsetzbar. Allerdings wäre etwas, das zumindest annähernd in die Richtung eines aus der freien Wirtschaft bekanntem IT-Risikomanagements

geht, auch hier ein positiver Faktor, um Probleme dieses Ausmaßes zu verhindern. Das BSI scheint, zumindest für das Netzwerk der Bundesregierung, nach diesen Berichten eine ähnliche Rolle einzunehmen.

Was ein gutes IT-Risikomanagement zu leisten im Stande ist, wird im folgenden Beispiel deutlich.

6.5 Chimera Ransomware

Bei dieser relativ neuen Angriffsart wird einem Unternehmen eine E-Mail mit einer angeblichen Bewerbung oder einem Auftragsangebot geschickt. Diese E-Mail enthält einen Link zu einer Datei, die über eine Dropbox-Adresse zu erreichen ist. Die Datei sieht zwar auf dem ersten Blick wie eine PDF- oder Word-Datei aus, ist aber ein ausführbares Programm. Beim Ausführen fängt dieses Programm an, die Festplatte und auch Netzlaufwerke zu verschlüsseln.

Wenn der Computer beim nächsten Mal gestartet wird, erhält man eine Nachricht auf dem Bildschirm, die dem Nutzer anweist eine bestimmte Summe auf ein Bitcoin-Konto zu überweisen, um wieder an die Daten zu gelangen. Teilweise auch um zu verhindern, dass hochgeladene Daten veröffentlicht werden. (vgl. Polizei, 2015)

Da die Daten mit dem Advanced Encryption Standard (AES) verschlüsselt werden, empfehlen teilweise sogar Behörden zu zahlen, falls wichtige Daten unwiderruflich abhandengekommen sind. Da die Verschlüsselung selbst nicht zu entschlüsseln ist. Das mittelständische IT-Unternehmen in diesem Beispiel besitzt allerdings ein IT-Risikomanagement. Die Datei wurde von einer Kraft aus dem Büro geöffnet. Da diese Person aber nur geringe Rechte im Netzwerk besaß, konnte die Schadsoftware nur begrenzten Schaden an Dateien dieser einen Kraft anrichten. Dazu kommen noch regelmäßige Backups, wodurch ein Großteil der Dateien wiederhergestellt werden konnten. Der Computer musste nur formatiert werden und die Firma selber hatte diesen Angriff damit überstanden. Als Reaktion wurden danach aber auch für einige Zeit viele Anhänge bei E-Mails gesperrt, damit sich so etwas trotzdem nicht so leicht wiederholen kann. Der Angriff wurde an das Management gemeldet, mit Folgen und Vorschlägen für die Zukunft, wie das Blocken bestimmter Anhänge.

Damit zeigt sich hier, wie ein vernünftiges IT-Risikomanagement große Schäden von vornherein verhindern kann. Und nach so einem Vorfall noch genauere Maßnahmen für die Zukunft einzusetzen gedenkt. (persönliches Gespräch, 2016)

Ob viele, gerade kleinere Unternehmen wie in diesem Beispiel, ein IT-Risikomanagement besitzen, soll die folgende Umfrage klären.

7 Umfrage

7.1 Fragestellung

Im Rahmen dieser Arbeit wurde an verschiedene Unternehmen eine Anfrage gesendet, telefonisch oder persönlich erfragt.

Den Kern der Anfrage, bildete folgende Fragestellung:

Die Hauptfrage ist, ob Sie ein Abteilung oder eine Person im Unternehmen haben, die sich mit dem Thema IT-Risikomanagement auseinander setzt.

Diese Person oder Abteilung sollte nicht nur für die Firewall zuständig sein, sondern sich auch Gedanken machen, welche Maßnahmen nötig sind und welche nicht. Hierzu werden meist Eintrittswahrscheinlichkeiten mit den Kosten beim Eintritt und den Kosten dies zu verhindern in Relation gesetzt.

Eine kurze Antwort ob, es so etwas bei Ihnen im Unternehmen gibt oder nicht, würde mir sehr weiterhelfen. Falls bei Ihnen ein externes Unternehmen für so etwas zuständig ist, würde mir auch das als Antwort helfen.

Falls Sie noch genauere Informationen geben könnten, würde ich mich natürlich freuen. So wären Ihre Erfahrungen mit IT-Risikomanagement, positive wie negative, eine große Hilfe. Die Größe Ihres Unternehmens würde mir für meine Daten auch helfen.

Diese Umfrage sollte versuchen zu ergründen, wie verbreitet ein IT-Risikomanagement heutzutage in verschiedenen Unternehmen ist. Vor allem, ob ein Unterschied zwischen großen und kleinen Unternehmen besteht. Zu diesem Zweck wurden Anfragen an ca. 50 Unternehmen geschickt. Diese 50 Unternehmen variieren nicht nur stark in der Größe, von international agierenden Großkonzernen, zu Betrieben mit weniger als fünf Angestellten, sondern auch von Privatwirtschaft zu öffentlichen Trägern. Von diesen 50 Unternehmen antworteten 20 direkt, oder gaben die Informationen über ihre jeweilige Webseite frei.

Diese 20 Unternehmen sind wiederum eine Mischung aus global agierenden Großkonzernen (7 Großkonzerne) und mittelständischen Unternehmen (13 mittelständischen Unternehmen). Auch die mittelständischen Unternehmen unter diesen 20, variieren in ihrer Größe. Es sind sehr kleine Unternehmen dabei, mit weniger als zehn Mitarbeitern, aber auch größere mit hunderten Mitarbeitern und einen Umsatz von teilweise mehr als 100 Millionen. Eine Auflistung der Antworten findet sich im nächsten Kapitel.

7.2 Ergebnisse

7.2.1 Komplette Liste der Unternehmen

In diesem Diagramm (Abbildung 4) sind alle Unternehmen die an der Umfrage teilgenommen haben Abgebildet.

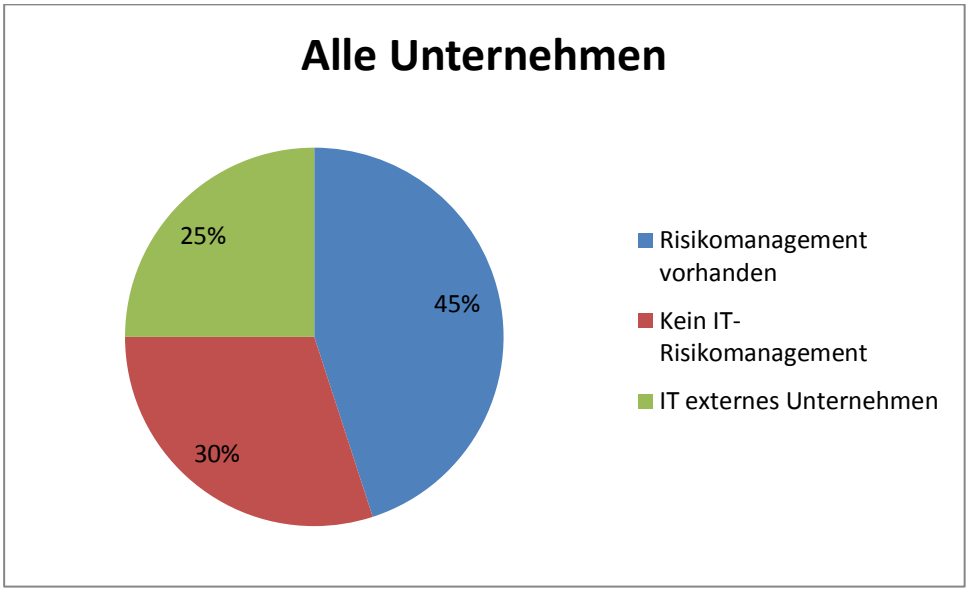

Abbildung 4 Unfrageergbnis alle Unternehmen

Wie man dem Tortendiagramm entnehmen kann, sind alle drei Möglichkeiten in Unternehmen vorhanden. Dies bedeutet, es gibt Unternehmen mit einem IT-Risikomanagement und einige Unternehmen ohne selbiges. Aber auch Unternehmen, die ihre IT an ein anderes Unternehmen ausgelagert haben.

Dazu kann man erkennen, dass ein IT-Risikomanagement bei weitem noch nicht in jedem Unternehmen zur Struktur gehört. Auch wenn es viele Unternehmen (45%) mit einem IT-Risikomanagement gibt.

Außerdem lässt sich erkennen, dass viele Unternehmen (25%), ihre IT an andere Unternehmen auslagern. Gleichzeitig besitzen diese Unternehmen kein IT-Risikomanagement, ansonsten hätte die Antwort bei der Umfrage anders gelautet. Sie vertrauen hier also stark auf ein anderes Unternehmen.

Wenn die Daten aus der Umfrage, mit allen Unternehmen, in verschiedene Kategorien aufgeteilt werden, wie die Größe der Unternehmen, ergibt sich ein anderes Bild. Im folgenden Kapitel wird dies mit mittelständischen Unternehmen gezeigt.

7.2.2 mittelständische Unternehmen

Dieses Tortendiagramm (Abbildung 5) enthält nur Unternehmen aus der Umfrage, die dem Mittelstand zugeordnet werden können, da nur diese als Daten für das Diagramm genutzt werden.

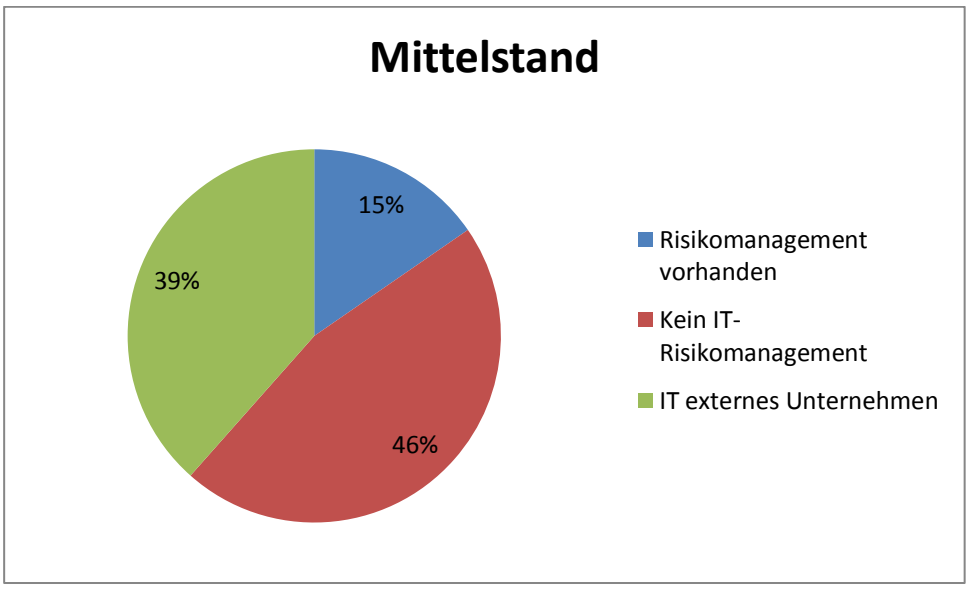

Abbildung 5 Umfrageergebnis Mittelstand

Durch diese Aufteilung der Daten sieht man hier einen deutlichen Unterschied zur ersten Auswertung.

Wo im ersten Diagramm noch die Mehrheit der Unternehmen ein IT-Risikomanagement besitzt, ist es bei mittelständischen Unternehmen der kleinste Wert (15%).

Dafür nimmt der Prozentsatz der Unternehmen mit einer ausgelagerten IT-Abteilung stark zu (39%). Dies deutet darauf hin, dass das IT-Risikomanagement in kleineren Unternehmen nicht praktiziert wird. Auch weil der größte Anteil (46%) hier, Unternehmen ohne IT-Risikomanagement ist.

Wie das gleiche Diagramm aussieht, wenn man die mittelständischen Unternehmen aus den Daten zieht, wird das folgende Kapitel aufzeigen.

7.2.3 Großkonzerne

Das letzte Diagramm (Abbildung 3) wiederum beinhaltet nur große, meist weltweit agierende Unternehmen mit tausenden Angestellten.

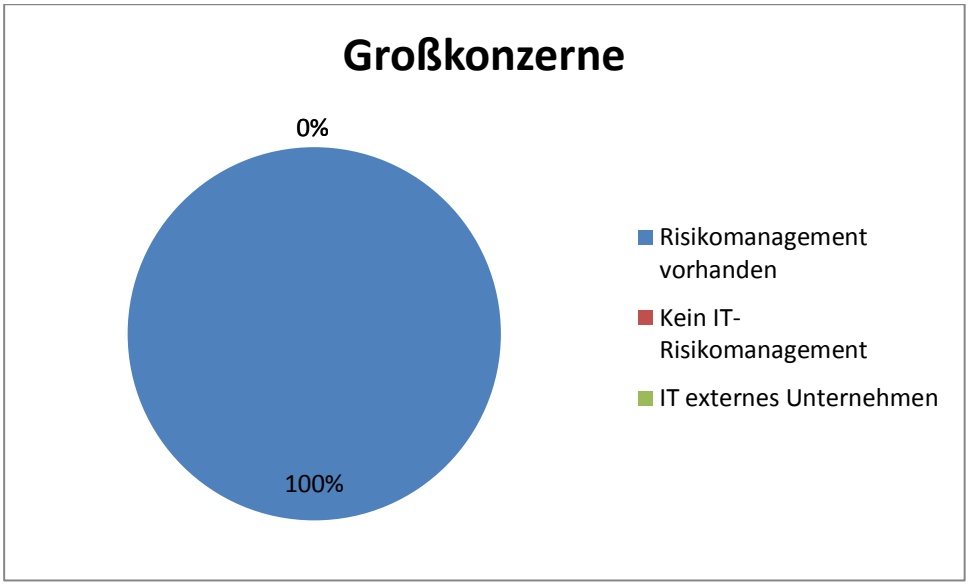

Abbildung 6 Umfrageergebnis Großkonzerne

Die Auswertung, in der nur Großkonzerne enthalten sind, zeigt ein einheitliches Bild. Hier erkennt man, dass Unternehmen ab einer bestimmten Größe ein IT-Risikomanagement besitzen.

Was genau mit diesen Daten anzufangen ist, soll das folgende Kapitel klären.

7.3 Analyse der Umfrage

7.3.1 Analyse aller Unternehmen (Abbildung 4)

Wenn man das Bild aller Unternehmen betrachtet kann man sehen, dass es sowohl Unternehmen gibt, die ein IT-Risikomanagement besitzen, als auch Unternehmen, die es nicht nutzen. Dazu gibt es noch Unternehmen, die ihre IT ausgelagert haben. Es muss allerdings festgehalten werden, dass dieses Diagramm durch die Auswahl der Unternehmen stark beeinflusst werden kann, wie die folgende Analyse der beiden andern Diagramme zeigt. Die Analyse aller Unternehmen zeigt noch keine großen Tendenzen auf. Im folgendem wird das mittelständische Unternehmen untersucht.

7.3.2 Analyse der mittelständischen Unternehmen (Abbildung 5)

Hier fällt der große Anteil an Firmen auf, die für ihre IT externe Unternehmen beauftragt haben. Dies zeigt auf, dass diese Firmen sich, selbst wenn ein gewisses IT-Risikomanagement vorhanden sein sollte, auf externe Quellen verlassen müssen.

Nach dem was zu erfahren war, ist es aber eher so, dass diese Unternehmen kein wirkliches Risikomanagement einbringen.

Sie haben eher die Aufgabe, eine gewisse Infrastruktur zur Verfügung zu stellen. Dies bedeutet ein Netzwerk aufzubauen und dieses soweit es geht abzusichern. Dazu kommen noch Punkte wie Datensicherungen und Hilfe bei allgemeinen IT-Fragen.

Die Nutzung externer Unternehmen als IT-Abteilung für Fragen des Alltags im Unternehmen ist nach dieser Umfrage zwar die Regel, soll aber nicht bedeuten, dass es nicht Unternehmen gibt, die auch durch externe Firmen ein leistungsfähiges IT-Risikomanagement zur Verfügung haben.

Weiterhin muss gesagt werden, dass die Hilfe bei Netzwerken und anderen IT-Problemen, für viele kleine Unternehmen auch ausreichend ist. Da hier auch die Kosten für eine Abteilung eine große Rolle spielen. Ob gerade sehr kleine Firmen überhaupt von einem eigenen IT-Risikomanagement groß profitieren könnten ist fraglich. Die Kosten können den Ertrag in einem solchen Fall leicht übersteigen.

Bei etwas größeren, mittelständischen Firmen ist die Frage der Kosten allerdings eine andere. Für solche Unternehmen ist ein IT-Risikomanagement zumindest eine Möglichkeit und kann positive Effekte im Unternehmen bewirken. Aufträge oder auch Kredite können zum Beispiel durch Einhaltung und Zertifizierung bestimmter Normen erleichtert werden.

Wie der Unterschied zwischen kleinen und großen mittelständischen Unternehmen ist, konnte bei dieser Umfrage nicht abschließend geklärt werden.

Wenn man allerdings bedenkt, „dass sich nur bei einem Drittel der mittelständischen Unternehmen der Geschäftsführer bzw. der Vorstand direkt mit Risikomanagement befassen“ (Löffler, Dr. Bömelburg, & Augsten, 2011), ist unwahrscheinlich, dass sich viele Unternehmen mit dieser Unterart des IT-Risikomanagement beschäftigen.

Das nächste Kapitel untersucht die Großkonzerne.

7.3.3 Analyse der Großkonzerne (Abbildung 6)

Während die Daten in Abbildung 1 noch eine gewisse Ausgeglichenheit zeigen, sieht man in Abbildung 2 und 3, dass dies doch stark von den Unternehmen und ihrer Größe abhängt.

Dass die wirklich großen Unternehmen ein IT-Risikomanagement besitzen ist leicht zu verstehen. Diese Unternehmen haben zum einen das Geld, um eine solche Abteilung zu bezahlen. Zum anderen besitzen sie auch eine Unternehmensstruktur, in der schon ein allgemeines Risikomanagement besteht. Dies erleichtert den Aufbau eines Risikomanagements für die IT.

Außerdem haben große Unternehmen auch eine große Zahl von Mitarbeitern, gepaart mit jeder Menge Außenstellen, oft weltweit. Wenn hier jeder Standort seine eigenen Regeln befolgen würde, vielleicht mal gut, mal weniger gut, wäre es für das Unternehmen zum einen ineffektiv und zum anderen auch bedrohlich, da auch Probleme an nur einem Standort Einfluss auf das gesamte Unternehmen haben können.

Daher kann das Risikomanagement regional verschieden sein. Das bedeutet, wenn man Standorte in verschiedenen Ländern besitzt, gibt es in jedem Land eine eigene Abteilung (dies hängt natürlich vom Unternehmen ab, oft auch von der Größe der jeweiligen Außenstelle). Diese Abteilungen können regionale Einflüsse, wie verschiedene Gesetze, behandeln. Diese regionalen Abteilungen unterstehen meist einer Abteilung, die das Risikomanagement der verschiedenen Standorte zusammenführt und auch allgemeine Richtlinien vorgibt, die regional unabhängig sind.

Nachdem mit den Großkonzernen die letzte Teilmenge untersucht wurde, folgt ein Fazit über die gesamte Umfrage.

7.4 Ergebnis der Umfrage

Das erste Diagramm (Abbildung 4) ist für eine kleine Umfrage wie diese nicht wirklich aussagekräftig. Durch den starken Unterschied vom Mittelstand zu Großkonzernen, ist eine Umfrage mit wenigen Unternehmen nicht zuverlässig genug, um eine gesamte Einschätzung vorzunehmen.

Interessant wird es, wenn man die mittelständischen Unternehmen von den Großkonzernen trennt.

Hier kann man, zumindest sehr gut Tendenzen erkennen. Großkonzerne haben mit einer sehr hohen Wahrscheinlichkeit ein IT-Risikomanagement. Bei mittelständischen Unternehmen ist dies eher noch unüblich. Und wenn es vorhanden ist, hat es zumindest in dieser Umfrage oft mit Gesetzesvorlagen zu tun, die für bestimmte Geschäftsprozesse nötig sind. Sei es für Aufträge oder Notwendigkeiten in bestimmten Branchen (persönliches Gespräch, 2016).

Während sich das Vorhandensein eines IT-Risikomanagement in Großkonzernen nicht mehr all zu leicht aufteilen lässt, ist dies bei mittelständischen Unternehmen noch gut möglich. Hier könnte man noch sehr kleine Unternehmen mit größeren vergleichen. Oder noch verschieden große Zwischenschritte setzen, nach Umsatz oder Anzahl der Mitarbeiter. Hierfür reichen in dieser Umfrage die Daten allerdings nicht aus.

Zu erwarten wäre allerdings, dass gerade sehr kleine Firmen kein IT-Risikomanagement besitzen. Viele kleine Firmen, mit weniger als fünf Angestellten, besitzen oft nicht einmal eine wirkliche IT. Je nach Art des Unternehmens nutzen hier viele nur einen oder vielleicht zwei Computer, nur für Rechnungen, E-Mails und die Verwaltung ihrer Termine.

Eine solche Auswertung würde also wahrscheinlich ein umgekehrtes Ergebnis zu dem von Großkonzernen zeigen.

Bei mittelgroßen bis großen mittelständischen Unternehmen wäre eine Analyse mit sehr vielen Datensätzen schon interessanter. Da diese beiden, je nach Geschäftsgebiet, auch von einem Risikomanagement profitieren können. Wenn man allerdings nach „Risikomanagement im Mittelstand“ (Löffler, Dr. Bömelburg, & Augsten, 2011, S. 6) geht, ist hier doch mit einem gewissen Anteil von Unternehmen zu rechnen, die ein IT-Risikomanagement besitzen. Wirklich hohe Prozentzahlen sind aber trotzdem nicht zu erwarten.

Im Folgenden wird das Ergebnis dieser Arbeit erläutert.

8 Ergebnisse

An der historischen Entwicklung des Risikomanagements kann man seine Relevanz erkennen. Auch wenn die Risikoanalyse am Anfang des Handelswesens noch rudimentär war, konnten Menschen, die ein Risiko gut einschätzten, schon immer einen Vorteil gegenüber Leuten erzielen, die dies nicht gut konnten.

Durch diese Relevanz wurde das Risikomanagement zu der wichtigen Instanz in Konzernen, die sie heute ist. Gerade in der modernen Zeit, mit der zunehmenden Bedeutung der IT in vielen Branchen, hat auch die Bedeutung des IT-Risikomanagements eine weitere Bedeutsamkeit erfahren.

Diese Arbeit erläutert hier einige wichtige Grundlagen, um Risiken besser bewerten zu können. Nicht zuletzt durch Vorstellung einiger Methoden, die für das Risikomanagement entwickelt wurden. Diese Methoden sollen helfen, ein Risiko besser einschätzen zu können. In der Praxis haben sich diese Methoden bewährt, auch wenn die meisten ihre eigenen Stärken und Schwächen haben. Aufgrund dieser Stärken und Schwächen kann man nicht von der einen, perfekten Methode sprechen. Jedes Unternehmen muss hier seine eigenen Präferenzen finden. Dies kann auch stark von den Erfordernissen zum jeweiligen Zeitpunkt der Analyse abhängen. Dabei kann zum Beispiel Zeitdruck oder auch das genaue Wissen um ein Risiko eine große Rolle spielen.

Sind die Risiken erkannt und zur Zufriedenheit bewertet, liegt es an den Entscheidungsträgern im Unternehmen zu entscheiden, was getan werden soll. Diese müssen entscheiden, ob ein Risiko hinnehmbar ist oder nicht. Wenn es hinnehmbar ist, wird das Risiko allerdings immer wieder überprüft um festzustellen, ob sich Änderungen ergeben haben. Diese Änderungen können alle Punkte betreffen, die Eintrittswahrscheinlichkeit oder aber auch die Kosten beim Eintritt eines Risikos, bzw. die Kosten um dieses Risiko zu senken. Wenn ein Risiko nicht hinnehmbar ist, müssen Wege erarbeitet werden, dieses Risiko in hinnehmbare Grenzen zu verschieben. Hierbei wird meistens versucht die Risikowahrscheinlichkeit zu senken, da es selten möglich ist die Kosten beim Eintreten eines Risikos zu beeinflussen.

Die Eintrittswahrscheinlichkeit eines Risikos zu senken ist allerdings vornehmlich eine Kostenfrage. Möglich ist es in den meisten Fällen, aber die Kosten müssen dem zu erleidenden Schaden entsprechen, bestenfalls unter den Kosten von einem Risikoeintritt liegen.

Unternehmen, die ein solches IT-Risikomanagement betreiben, können sich zertifizieren lassen. Zum Beispiel durch die Norm, die in dieser Arbeit vorgestellt wurde, die ISO27001. Eine Zertifizierung mit dieser Norm kann vielfältige Vorteile für das Unternehmen bringen. Von der erhöhten Erkennung von Risiken, über Vorteilen bei Aufträgen, die ein solches Zertifikat bedingen, bis zur Erleichterung beim Beantragen von Krediten.

Die Beispiele, vor allem die von Sony oder dem Bundestag zeigen, dass ein gutes Risikomanagement bei großen Firmen fundamental wertvoll sein kann. Da die internen Gründe für diese Fälle nicht öffentlich sind, kann nicht beurteilt werden, ob ein IT-Risikomanagement versagt hat oder ignoriert wurde. Aber es kann festgestellt werden, dass die Fälle aus diesen Beispielen nicht passieren sollten. Und da eine Vielzahl von Großkonzernen solch große Probleme nicht hatte, ist es wahrscheinlich, dass es möglich war diese Probleme zu verhindern.

Auch wenn die Umfrage durch wenige Teilnehmer nicht repräsentativ ist zeigt sie auf, dass in kleinen Unternehmen ein IT-Risikomanagement zumeist noch fehlt. Aufgrund der Kosten ist dies zwar verständlich, trotzdem wäre zumindest eine reduzierte Version auch für kleinere Unternehmen von Vorteil. Gerade auch weil viele der kleineren Unternehmen sich auf externe Vertreter für ihre IT verlassen. Wenn die externen Partner zumindest durch das Unternehmen kontrolliert werden würden, könnten die Unternehmen gezieltere Forderungen an ihre ausgelagerte IT stellen. Die meisten der sehr kleinen Unternehmen betrifft dies allerdings nicht. Sofern sie kein IT-Unternehmen sind, ist die Anforderung an die IT oft sehr gering. Auch kann durch die IT selten ein großer Schaden entstehen.

Abschließend muss gesagt werden, dass mutmaßlich das IT-Risikomanagement in vielen Unternehmen noch ausbaufähig ist. Es ist allerdings möglich, dass dies mit dem wahrscheinlich weiteren Anwachsen der Relevanz von IT-Systemen, automatisch passieren wird.

Anhang

E-Mail Umfrage

Sehr geehrte Damen und Herren,

mein Name ist Thomas Ehlers und ich studiere an der Hochschule für Angewandte Wissenschaften Hamburg Media Systems.

Ich arbeite gerade an meiner Bachelorarbeit zum Thema IT-Risikomanagement.

Für diese Arbeit führe ich eine Umfrage mit verschiedenen Unternehmen durch.

Die Hauptfrage ist, ob Sie ein Abteilung oder eine Person im Unternehmen haben, die sich mit dem Thema IT-Risikomanagement auseinander setzt.

Diese Person oder Abteilung sollte nicht nur für die Firewall zuständig zu sein, sondern sich auch Gedanken machen, welche Maßnahmen nötig sind und welche nicht. Hierzu werden meist Eintrittswahrscheinlichkeiten mit den Kosten beim Eintritt und den Kosten dies zu verhindern in Relation gesetzt.

Eine kurze Antwort ob, es so etwas bei Ihnen im Unternehmen gibt oder nicht, würde mir sehr weiterhelfen. Falls bei Ihnen ein externes Unternehmen für so etwas zuständig ist, würde mir auch das als Antwort helfen.

Falls Sie in Ihrem Unternehmen nicht der richtige Ansprechpartner sind, würde ich mich freuen, wenn Sie diese E-Mail an die zuständigen Personen weiter senden würden (vielleicht die IT-Abteilung). Wenn es in Ihrem Unternehmen keinen entsprechenden Ansprechpartner gibt, bitte ich um eine kurze Rückantwort.

Falls Sie noch genauere Informationen geben könnten, würde ich mich natürlich freuen. So wären Ihre Erfahrungen mit IT-Risikomanagement, positive wie negative, eine große Hilfe. Die Größe Ihres Unternehmens würde mir für meine Daten auch helfen.

Bei eventuellen Fragen stehe ich Ihnen natürlich zur Verfügung. Meine Telefonnummer und E-Mail-Adresse finden Sie am Ende dieser E-Mail.

Auch wenn ich nicht nach geheimen Daten frage möchte ich Ihnen versichern, dass Ihre Daten nicht weiter gegeben werden. Außerdem werden sich die Daten am Ende der Arbeit nur in Statistiken wiederfinden. Vielen Dank im Voraus für Ihre Unterstützung.

Abbildungsverzeichnis

Literaturverzeichnis

Böck, H. (30. 10 2014). *http://www.golem.de*. Abgerufen am 16. 1 2016 von http://www.golem.de/news/sql-injection-sicherheitsluecke-erlaubt-zugriff-auf-sony-kundendaten-1410-110199.html

BSI. (29. 1 2016). Abgerufen am 29. 1 2016 von https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html

BSI. (29. 1 2016). Abgerufen am 29. 1 2016 von https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html

BSI. (29. 1 2016). *www.bsi.bund.de*. Abgerufen am 29. 1 2016 von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/7_Notfaellebewaeltigen/nfm07_05.html

chess24.com. (25. 1 2016). *https://chess24.com/*. Abgerufen am 29. 1 2016 von https://chess24.com/de/lesen/glossar/analyse

Dr. Datenschutz. (27. 4 2011). *https://www.datenschutzbeauftragter-info.de*. Abgerufen am 16. 1 2016 von https://www.datenschutzbeauftragter-info.de/frisch-gehackt-its-not-a-trick-its-a-sony/

Dudenverlag. (20. 1 2016). *http://www.duden.de/rechtschreibung/Risiko*. Abgerufen am 19. 1 2016 von www.duden.de

Fuest, B. (12. 12 2014). *http://www.welt.de*. Abgerufen am 16. 1 2016 von http://www.welt.de/wirtschaft/article135283433/Sonys-verzweifelter-Gegenangriff-auf-die-Hacker.html

Gutmannsthal-Krizanits, H. (1994). *Risikomanagement von Anlageprojekten.* Wiesbaden: Springer Fachmedien.

http://projektmanagement-definitionen.de. (29. 1 2016). Abgerufen am 1. 29 2016 von http://projektmanagement-definitionen.de: http://projektmanagement-definitionen.de/glossar/quantitative-risikoanalyse/

Jendryschik, M. (8. 12 2009). *http://webkrauts.de*. Abgerufen am 28. 1 2016 von http://webkrauts.de/artikel/2009/hilfsmittel-fuer-aufwandsschaetzungen

Knoll, M. (2014). *Praxisorientiertes IT-Risikomanagement.* Heidelberg: dpunkt.verlag GmbH.

Löffler, H. F., Dr. Bömelburg, P., & Augsten, T. (2011). *Risikomanagement im Mittelstand.* S. 6: Funk RMCE, Rödl & Partner, Weissman & Cie.

Loschwitz, M. (1. 4 2011). *www.admin-magazin.de*. Abgerufen am 26. 1 2016 von http://www.admin-magazin.de/Das-Heft/2011/04/HA-Serie-Teil-1-Grundlagen-von-Pacemaker-und-Co

Online Redaktion Docusnap. (14. 5 2014). *www.docusnap.com*. Abgerufen am 27. 1 2016 von http://www.docusnap.com/it-dokumentation/grundlagen/wiederanlaufplane-ihrer-it-systeme

persönliches Gespräch. (2016).

Polizei. (12. 10 2015). *www.polizei-praevention.de*. Abgerufen am 25. 1 2016 von http://www.polizei-praevention.de/aktuelles/chimera-ransomware.html

Prof. Dr. Johner, C. (26. 6 2015). *https://www.johner-institut.de/*. Abgerufen am 29. 1 2016 von https://www.johner-institut.de/blog/iso-14971-risikomanagement/risikoprioritaetszahl-rpz/

projektmanagement-definitionen.de. (29. 1 2016). *http://projektmanagement-definitionen.de*. Abgerufen am 29. 1 2016 von http://projektmanagement-definitionen.de/glossar/qualitative-risikoanalyse/

Reiss, M., & Sportelli, M. (29. 1 2016). *www.security-insider.de*. Abgerufen am 29. 1 2016 von http://www.security-insider.de/iso-27001-international-anerkannte-isms-zertifizierung-a-334990/

Süddeutsche Zeitung. (14. 6 2015). *http://www.sueddeutsche.de*. Abgerufen am 19. 0 2016 von http://www.sueddeutsche.de: http://www.sueddeutsche.de/politik/hackerangriff-auf-den-bundestag-gesamtes-it-netz-des-bundestages-muss-ausgetauscht-werden-1.2519934

Tague, N. R. (2004). *The Quality Toolbox.* ASQ Quality Press.

Trepesch, S. (19. 6 2014). *http://www.giga.de*. Abgerufen am 25. 1 2016 von http://www.giga.de: http://www.giga.de/apps/threema/specials/messenger-test-threema-whatsapp-telegram-chadder-line-und-mehr-im-vergleich/page/2/?PageSpeed=noscript

Wolf, L. (17. 11 2010). *www.cdlib.org*. Abgerufen am 29. 1 2016 von http://www.cdlib.org/cdlinfo/2010/11/17/the-project-post-mortem-a-valuable-tool-for-continuous-improvement/

www.itwissen.info/. (27. 1 2016). */www.itwissen.info/*. Abgerufen am 27. 1 2016 von http://www.itwissen.info/definition/lexikon/Hochverfuegbarkeit-high-avaiability-HA.html

Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Bachelor-Thesis mit dem Titel:

„IT-Risikomanagement“

selbständig und nur mit den angegebenen Hilfsmitteln verfasst habe. Alle Passagen, die ich wörtlich aus der Literatur oder aus anderen Quellen wie z. B. Internetseiten übernommen habe, habe ich deutlich als Zitat mit Angabe der Quelle kenntlich gemacht.

(Unterschrift)