MASTERARBEIT

MASSNAHMEN ZUR VERMINDERUNG VON IT-SICHERHEITSBEDENKEN BEI EINEM ERP-SYSTEM IN DER CLOUD

ausgeführt am

Studiengang
Informationstechnologien und Wirtschaftsinformatik

Von: Stefan Lautner
Personenkennzeichen: 1610320021

Graz, am 14. Dezember 2017 .....

Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benutzt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

DANKSAGUNG

An dieser Stelle möchte ich mich herzlich bei Herrn DI (FH) Christian Schmid, MSc bedanken, der diese Arbeit betreut und mir jederzeit mit Rat und Tat zur Seite gestanden hat.

Des Weiteren bedanke ich mich bei allen Freunden, Kommilitonen und Lektoren, die stets offen für Fragen und mir eine große Hilfe bei der Fertigstellung dieser Arbeit waren.

Zum Schluss möchte ich mich noch bei meiner Freundin Sabrina bedanken, die mich immer unterstützt und ihr Wissen ihres abgeschlossenen Masterstudiums mit mir geteilt hat.

KURZFASSUNG

Die Cloud ist ein Thema, das Unternehmen durch die Digitalisierung mehr betrifft denn je. Während sie im Privatleben bereits Einzug in den Alltag gefunden hat, benötigen die Unternehmen noch etwas Zeit. Speziell in Bezug auf ERP-Systeme, die die sensibelsten Daten des Unternehmens beinhalten, verwehren sie sich diesem Trend. Dies liegt vor allem an der Sicherheit der Cloud. In dieser Arbeit wird darum untersucht, welche konkreten Sicherheitsbedenken die Unternehmen haben, wenn es darum geht, ihr ERP-System in der Cloud zu betreiben, und wie diese vermindert werden können. Zur Datenerhebung wurden Personen aus der IT interviewt, worauf anschließend eine Liste von Bedenken aus ihren Aussagen erstellt wurde. Die Priorisierung ergab, dass eine performante Internetverbindung und das Vertrauen in den Cloud-Anbieter die größten Bedenken im Bereich der IT-Sicherheit auslösen. Durch die technologischen Möglichkeiten in der Cloud können diese Bedenken jedoch vermindert werden, indem beispielsweise ein entsprechendes Verfügbarkeitsmodell gewählt oder eine private Verbindung zum Cloud-Anbieter aufgebaut wird. Dennoch ist es nicht möglich, alle Bedenken auszuräumen, da ab einem gewissen Punkt kein Einblick in und kein Einfluss mehr auf die Funktionalität der Cloud vorgenommen werden kann. Dies zeigt, dass vor allem Vertrauen die Basis für den sicheren Betrieb des ERP-Systems in der Cloud ist. Mit der vorliegenden Arbeit soll den Unternehmen gezeigt werden, dass sich ihre Bedenken leicht vermindern lassen.

ABSTRACT

The cloud is almost indispensable for enterprises seeking to digitise themselves. Although private citizens have embraced the cloud, enterprises have been slower to follow. ERP systems especially, which handle the most sensitive data in an enterprise, seek to keep their data in-house because of their scepticism of cloud security. This thesis investigates and tries to address the concerns of enterprises with regard to running their ERP system in the cloud. To this end, IT expert employees were interviewed to collate a list of concrete concerns regarding IT security for ERP systems in the cloud. This list shows that a high-performance Internet connection and the trust in the cloud provider are the biggest security concerns. However, these concerns can be mitigated by the technical capabilities of the cloud. An enterprise can, for example, select an appropriate availability model or set up a private connection to the cloud provider. Some concerns will inevitably remain, however, because the cloud provider cannot fully reveal how their technology works. Trust must be the basis for the secure operation of an ERP system in the cloud. This thesis shows that many concerns about the cloud can be properly addressed.

INHALTSVERZEICHNIS

1 EINLEITUNG

Bei aktuellen Trendumfragen in Unternehmen ist ein Thema dauerhaft präsent: die Cloud. Die Cloud erfüllt alle Voraussetzungen für die Digitalisierung, indem sie Skalierbarkeit, Agilität und Kapazität zur Verfügung stellt. Dennoch ist die Cloud ein noch immer heftig diskutiertes Thema, was sich vor allem darin zeigt, dass die Cloud einerseits für viele bereits zum Alltag gehört, sie aber andererseits auch auf komplette Ablehnung stößt. Trotz der unterschiedlichen Varianten der Cloud trennen sich Unternehmen ungern von der On-Premise-Installation ihrer Software (vgl. Abolhassan, 2017).

Diese Arbeit will versuchen, ERP-Systeme und deren Sicherheit in Bezug auf die Cloud näher zu betrachten. Dafür werden in diesem Kapitel die Ausgangsstellung und das Problem klar definiert, um nachfolgend die Forschungsfrage für diese Arbeit zu formulieren.

1.1 Ausgangsstellung

Vor ca. 20 Jahren, als die Gartner Group den Begriff ‚Enterprise Resource Planning' (ERP) in der Unternehmenswelt etablierte, hat nicht nur die Technologie im Hintergrund, sondern auch das tägliche Arbeiten einen Wandel erfahren. Heutzutage ist das Ziel ein effizienter, vernetzter und intensiver Informationsaustausch mit allen Stakeholdern des Unternehmens, angefangen bei den Kundinnen und Kunden über die Mitarbeiterinnen und Mitarbeiter bis hin zu den Lieferantinnen und Lieferanten. Durch das Internet und die weltweite Vernetzung ergeben sich auch in der Unternehmenswelt immer mehr Möglichkeiten und die Mobilität der Arbeit nimmt zu. Während Smartphones, Tablets und Co. bereits das tägliche Privatleben prägen, nehmen diese auch immer mehr Einfluss auf die Arbeitswelt. Dies geht so weit, dass Grenzen zwischen Privatem und Beruflichem zu verschwimmen drohen (vgl. Jung-Elsen, 2013).

Der Vorteil dieser Mobilität ist die Erfüllung des Wunsches nach aktuellsten Informationen auf Knopfdruck und einer benutzerfreundlichen Oberfläche. Während in den unterschiedlichsten Bereichen im Unternehmen, wie zum Beispiel in der gemeinsamen, vernetzten Zusammenarbeit oder dem Kundenbeziehungsmanagement, bereits Tools für die höchstmögliche Flexibilität und Mobilität im Einsatz sind, finden sich solche Anwendungen im ERP-Bereich nur selten. Dennoch müssen durch den Wandel im täglichen Arbeiten auch ERP-Systeme auf die neuen Anforderungen der Benutzerinnen und Benutzer reagieren. Mit Cloud-Computing steht nun eine Technologie zur Verfügung, mit der genau dieses Ziel erreicht werden kann (vgl. Jung-Elsen, 2013).

Nicht nur Jung-Elsen (2013) sieht im Cloud-Computing eine Technologie, die den Anforderungen der Benutzerinnen und Benutzer in Bezug auf ERP-Systeme gerecht werden kann. Auch Jain und Sharma (2016) zeigen die Auswirkungen auf das Unternehmen bei Verwendung von ERP-Systemen in der Cloud:

- Skalierbarkeit nach oben und unten
- Senkung der Kosten für die Wartung und Upgrades
- Reduzierung der Kosten für die IT-Infrastruktur
- Verbesserung der Flexibilität und Effizienz (vgl. Jain & Sharma, 2016)

Damit stellt das Cloud-Computing eine Plattform für ein flexibles, skalierbares und mobiles ERP-System bereit, das den Anforderungen gerecht werden kann. Mit der Hilfe von Cloud-Computing ist es möglich, Daten von überall in Echtzeit abzurufen, unabhängig vom Standort (vgl. Jung-Elsen, 2013).

1.2 Problemstellung

Laut Jung-Elsen (2013) werden ERP-Systeme, die die unterschiedlichsten Bereiche im Unternehmen in einem zentralen System vereinen, überwiegend als On-Premise-Lösung im eigenen Rechenzentrum oder Serverraum betrieben. Trotz Cloud-Computing schaffen es ERP-Systeme somit nicht, in den Unternehmen Fuß zu fassen. Speziell die IT-Abteilungen der Unternehmen sind von der neuen Technologie betroffen und stellen einen der Gründe dar, um dem Cloud-Computing Aufmerksamkeit zukommen zu lassen. Den Vorteilen des Cloud-Computing stehen dabei zahlreiche Hemmnisse gegenüber, die den Durchbruch bisher verhindert haben. Als Beispiel dafür dient laut Jung-Elsen (2013) unter anderem die Tatsache, dass sich Stakeholder bewusst sein müssen, dass unternehmensrelevante Daten das eigene Rechenzentrum oder den Serverraum verlassen und in die Cloud hineingehen.

Dieses Beispiel deckt sich mit den Ergebnissen der Studie von Bitkom Research im Auftrag von KPMG (2016), die in Abbildung 1-1 dargestellt wird. Ein Teil der Studie zeigt auf, welche Hindernisse beim Cloud-Computing aktuell vorhanden sind. Aus den Ergebnissen lässt sich ablesen, dass vor allem der Bereich Sicherheit als Hindernis und Hemmnis von Unternehmen identifiziert wurde. Dabei sticht besonders hervor, dass mehr als die Hälfte der Unternehmen angaben, dass sie Angst vor Zugriff auf sensible Unternehmensdaten haben, wenn Cloud-Computing im Einsatz ist. Die Studie liefert gleichzeitig eine Aussage darüber, wie viele Unternehmen bereits ein ERP-System in der Cloud im Einsatz haben: Der prozentuelle Anteil liegt bei 23 %. Das bedeutet, dass nur ca. jedes vierte Unternehmen sein ERP-System in der Cloud betreibt.

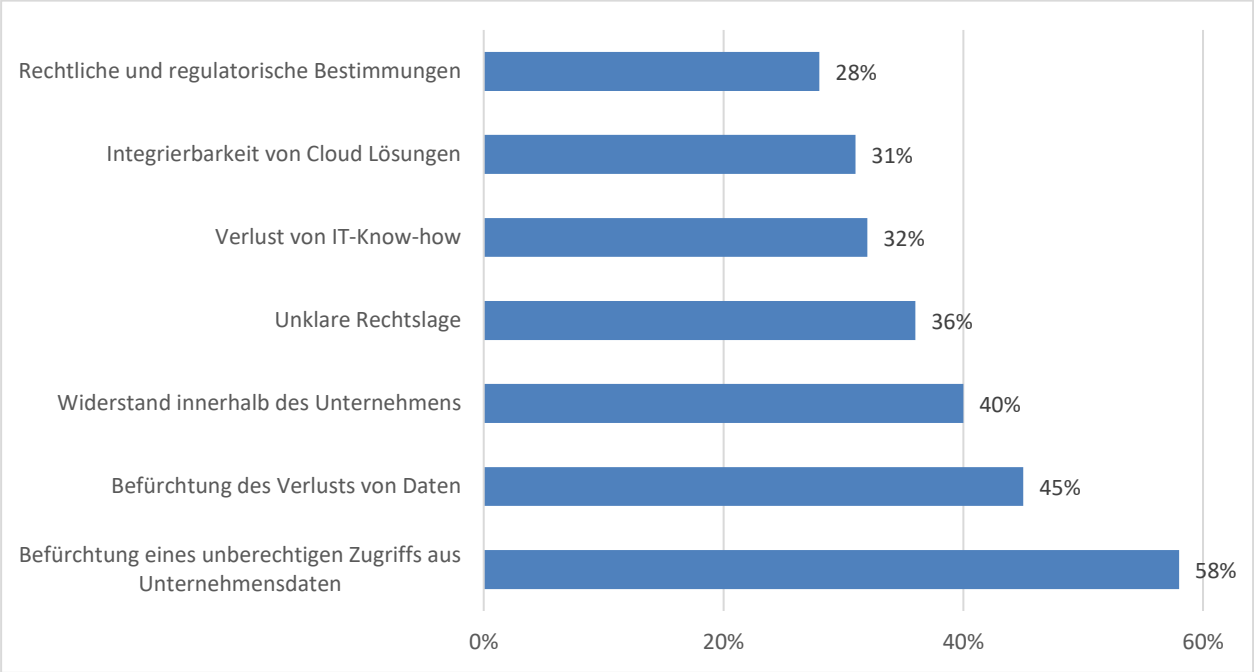


Abbildung 1-1 Bedenken gegenüber Cloud-Computing (Pols & Heidkamp, 2016)

Weitere Studien, wie zum Beispiel von Intel Corporation (2012), zeigen, dass die IT-Sicherheit eines der größten Hindernisse im Bereich des Cloud-Computings darstellt und beschäftigen sich zusätzlich mit der Frage, welche Bedenken es in diesem Bereich gibt. Die Studie von Intel Corporation (2012) bezieht sich jedoch nur auf das Cloud-Computing im Allgemeinen und verschweigt Hintergrundinformationen. Zum Beispiel konnte diese Studie zeigen, dass Access Control eines der größten Bedenken im Bereich der IT-Sicherheit bei Cloud-Computing darstellt, während die eigentlichen Bedenken dahinter nicht aufgeklärt wurden.

1.3 Fragestellung und Zielsetzung

Nach Klärung der Ausgangsstellung und des Problems, sollen in diesem Abschnitt die genaue Fragestellung und die Zielsetzung dieser Arbeit vorgestellt werden.

1.3.1 Forschungsfrage

ERP-Systeme in Verbindung mit Cloud-Computing weisen viele Vorteile auf, sind aber, wie bereits erwähnt, selten in Unternehmen vertreten. Da als Hauptgrund Sicherheitsbedenken angegeben werden, stellt sich die Frage, ob es nicht möglich ist, diese Bedenken bereits im Vorfeld zu vermindern. Um dies zu erreichen ist es nötig, entsprechende Maßnahmen durchzuführen, um die Bedenken hinsichtlich der Sicherheit zu vermindern. Daraus leitet sich folgende Forschungsfrage für die vorliegende Masterarbeit ab:

‚Welche Maßnahmen führen zu einer Verminderung der Bedenken im Bereich IT-Sicherheit bei der Einführung eines ERP-Systems in der Cloud?'

1.3.2 Hypothese

Neben der Forschungsfrage wird zu Beginn der Masterarbeit eine Hypothese erarbeitet. Die Prüfung dieser Hypothese leitet den weiteren Forschungsprozess an. Dabei ist es üblich, eine Nullhypothese H_0 und eine Alternativhypothese H_1 (komplementär zu H_0) aufzustellen. Das Ziel der Hypothesenprüfung ist die Verwerfung von H_0 (vgl. Raithel, 2006). Für diese Masterarbeit wurden folgende H_0 und H_1 aufgestellt:

H_0: Bei einem ERP-System in der Cloud gibt es keine Bedenken hinsichtlich der IT-Sicherheit.

H_1: Bei einem ERP-System in der Cloud gibt es Bedenken hinsichtlich der IT-Sicherheit.

1.3.3 Ziele

Im Zuge dieser Masterarbeit soll herausgefunden werden, welche Bedenken es im Bereich der IT-Sicherheit gibt, wenn ein ERP-System in der Cloud betrieben werden soll. Auf Basis dieser Ergebnisse sollen Möglichkeiten zur Verminderung dieser Bedenken gefunden werden, indem ausgewählte Bedenken näher betrachtet werden. Diese Arbeit soll aufzeigen, wie die kritischsten Bedenken vermindert werden können und welche Maßnahmen nötig sind, um die Nullhypothese verwerfen und eine Antwort auf die Forschungsfrage geben zu können. Wichtig hierbei ist zu erwähnen, dass nicht alle erforschten Bedenken auch wirklich sicherheitskritisch sind und deshalb untersucht werden müssen. Daher werden die Bedenken auf eine geeignete Art und Weise priorisiert.

1.3.4 Nichtziele

Bedenken bei der Einführung eines ERP-Systems in der Cloud beschränken sich nicht nur auf die IT-Sicherheit. Diese Arbeit setzt hierauf jedoch ihren Fokus und behandelt alle weiteren Bedenken, die im Laufe der Forschung auftreten, nicht. Des Weiteren ist es nicht Ziel der Arbeit, ein Referenzprojekt in der Praxis durchzuführen und die Technologie im Feld zu testen. Der Begriff IT-Sicherheit bezieht sich in dieser Arbeit nur auf die Cloud, nicht auf generelle Themen, wie zum Beispiel die Regelung von Zugriffsrechten innerhalb des ERP-Systems. Was genau unter IT-Sicherheit im Umfeld von ERP-Systemen in der Cloud zu verstehen ist, wird im theoretischen Teil der Arbeit näher erläutert.

Wie bereits erwähnt, ist es nicht Ziel der Arbeit, alle aufkommenden Bedenken zu betrachten. Stattdessen wird eine Priorisierung durchgeführt und nur die kritischsten Bedenken werden für die weitere Forschung verwendet. Das genaue Vorgehen und weitere Erklärungen können den entsprechenden Abschnitten der Arbeit entnommen werden.

1.4 Aufbau der Arbeit

Im ersten Kapitel dieser Arbeit wird ein Überblick über den Inhalt der Forschung gegeben und es erfolgt eine Vorstellung der Forschungsfrage und der Hypothese. Kapitel zwei bildet den theoretischen Teil dieser Arbeit und beschäftigt sich mit den Grundlagen zu den Themen ERP, Cloud-Computing und IT-Sicherheit. Die Themen werden nacheinander aufbereitet, wobei sie aufeinander aufbauen, sodass beispielsweise Cloud-Computing bereits im Kontext von ERP-Systemen betrachtet werden muss. Dieses Vorgehen erlaubt zusätzlich einen langsamen Aufbau der Zusammenhänge, was am Ende des theoretischen Teils einen umfassenden Überblick über die IT-Sicherheit im Bereich von ERP-Systemen in der Cloud sicherstellt. Im Anschluss an den theoretischen folgt der empirische Teil. Dafür wird in Kapitel drei zunächst der Forschungsprozess erläutert, bevor seine konkrete Ausgestaltung vorgestellt wird. Kapitel vier widmet sich dann der Auswertung der Daten, die in der Empirie erhoben wurden. Die Ergebnisse dieses Kapitels bilden die Basis für Kapitel fünf, in dem versucht werden soll, die IT-Sicherheitsbedenken gegenüber ERP-Systemen in der Cloud zu vermindern. Am Ende der Arbeit folgen noch die Kapitel sechs und sieben, in denen die Ergebnisse diskutiert und die gesamte Arbeit zusammengefasst werden soll.

2 THEORETISCHE GRUNDLAGEN

In diesem Kapitel werden die Begriffe aus der Forschungsfrage (ERP-System, Cloud-Computing und IT-Sicherheit) als Grundlage für das weitere Forschungsvorgehen erklärt. Dieses Kapitel soll Aufschluss darüber geben, wann von einem ERP-System in der Cloud gesprochen wird und welche Aspekte der IT-Sicherheit dabei von Relevanz sind.

2.1 ERP-Systeme

Dieser Abschnitt dient zum besseren Verständnis von ERP-Systemen, wobei die Abkürzung ERP für ‚Enterprise Resource Planning' steht. Wird der Begriff in die deutsche Sprache übersetzt, so bedeutet er ‚Unternehmensressourcenplanung' (vgl. Osterhage, 2014).

2.1.1 Definition

Hinter dem Begriff ‚Unternehmensressourcenplanung' steckt jedoch mehr als nur die Planung, denn ERP-Systeme beschäftigen sich vielmehr mit Unternehmensprozessen sowie der Steuerung und der Planung von Ressourcen (vgl. Osterhage, 2014). Laut Doedt (2013) sind Ressourcen in diesem Fall das Kapital, die Betriebsmittel und das Personal.

Osterhage (2014) identifiziert dabei die Betrachtung von ERP-Systemen als Synonym für eine Software zur Verwaltung von Ressourcen als Trugschluss. Ein ERP-System sei vielmehr ein organisatorisches Konzept, dem Unternehmensprozesse zugrunde liegen. Dieses Konzept bekommt in weiterer Folge Unterstützung durch eine gleichnamige Software, die es elektronisch abbildet. Daraus folgt, dass das Prinzip eines ERP-Systems nicht nur auf Unternehmen, sondern ganz allgemein auf Organisationen angewendet werden kann (vgl. Osterhage, 2014).

Der US-amerikanische Konzern Gartner, der sich selbst als weltweit führendes Unternehmen für Informationstechnologie und Forschung sieht, definiert ERP folgendermaßen (vgl. Gartner, 2017a):

> *„Enterprise resource planning (ERP) is defined as the ability to deliver an integrated suite of business applications. ERP tools share a common process and data model, covering broad and deep operational end-to-end processes, such as those found in finance, HR, distribution, manufacturing, service and the supply chain. ERP applications automate and support a range of administrative and operational business processes across multiple industries, including line of business, customer-facing, administrative and the asset management aspects of an enterprise." (Gartner, 2017b)*

Zusammengefasst lässt sich sagen, dass ERP-Systeme dazu dienen, die Unternehmensprozesse durch IT zu stützen und zu optimieren. Im Mittelpunkt steht dabei die Zentralisierung von Daten und Funktionen über alle Bereiche eines Unternehmens hinweg. Im weiteren Verlauf der Arbeit wird mit dem Begriff ERP-System somit auch die Software selbst gemeint.

2.1.2 Aufbau

Gartner (2017b) spricht bei der Definition von ERP-Systemen von einem gemeinsamen Datenmodell und Prozess. Als Backend kommt dabei meist eine relationale Datenbank zum Einsatz, die alle Daten des Unternehmens vereint. Im Gegensatz zu Lösungen ohne ERP-System liegt der Vorteil hierbei in der Zentralisierung der Daten. Dies ermöglicht einen einfachen Austausch der Daten zwischen den einzelnen Bereichen des Unternehmens. Des Weiteren werden durch die Zentralisierung Insellösungen verhindert, die untereinander kompatibel sein müssen, um miteinander kommunizieren zu können. Ein ERP-System vereint diese Insellösungen und ermöglicht beispielsweise dem Vertrieb, dass er Aussagen über den Lagerbestand von Artikeln treffen und gegebenenfalls den Produktionsprozess anstoßen kann (vgl. Doedt, 2013).

Laut Verma und Arora (2014) gibt es in ERP-Systemen anstatt der Insellösungen Module, die die unterschiedlichen Bereiche im Unternehmen abdecken sollen. Die zentralen Module, die auch von Doedt (2013) als diese definiert wurden, werden in Abbildung 2-1 dargestellt.

Abbildung 2-1 Module eines ERP-Systems (Verma & Arora, 2014)

Bei der Finanzbuchhaltung handelt es sich um eine unverzichtbare Komponente im Unternehmen, weshalb sie als eigenes Modul in das ERP-System integriert wird. Inhaltlich bearbeitet die Finanzbuchhaltung Themen wie zum Beispiel die Liquiditätsrechnung, Finanzpläne

oder den Cashflow (vgl. Osterhage, 2014). Den Kern des ERP-Systems bildet die Produktionsplanung und -steuerung. Diese hilft beim Planen und Steuern von Durchlaufzeiten, Terminen oder auch Betriebsmitteln der Produktion. Bei der Wertschöpfungskette handelt es sich grob beschrieben um die Prozesse des Einkaufs und Verkaufs, die auch unter dem Begriff ‚Supply Chain Management' (SCM) zusammengefasst werden. Diese Kette beginnt bei den Lieferantinnen und Lieferanten und endet bei den Kundinnen und Kunden. Ein insbesondere für den Vertrieb nützliches Modul ist das Kundenbeziehungsmanagement, auch ‚Customer Relationship Management' (CRM) genannt. Das Ziel des CRM-Moduls ist es, die Kundinnen und Kunden langfristig an das Unternehmen zu binden. Um dieses Ziel zu erreichen ist es notwendig, alle relevanten Informationen zu den Kundinnen und Kunden jederzeit abrufen zu können. Das fünfte Modul bildet die Mitarbeiterinnen- und Mitarbeiterverwaltung, das Unterstützung bei der Planung, Entwicklung und Verwaltung von Mitarbeiterinnen und Mitarbeitern bietet (vgl. Doedt, 2013).

Zwar gibt es für alle Module jeweils separate Systeme, ein ERP-System vereint jedoch die möglichen Insellösungen in einer Datenbank und sorgt damit für eine zentrale Datenbasis, die jedoch wiederum nur einen Teil des ERP-Systems darstellt (vgl. Doedt, 2013).

2.1.3 Systemarchitektur

In den 1980er-Jahren, als zunehmend grafische Oberflächen und datenbankbasierte Informationssysteme in Unternehmen genutzt wurden, wurde für diese eine sogenannte Schichtenarchitektur entwickelt. Das Informationssystem wurde dafür in drei Schichten aufgeteilt, wobei sich diese drei Standardschichten etabliert haben (vgl. Karagiannis & Rieger, 2006):

- Präsentationsschicht
- Anwendungsschicht
- Datenerhaltungsschicht (vgl. Karagiannis & Rieger, 2006)

Grundsätzlich wird bei dieser Aufteilung von einem Client-Server-Modell gesprochen, das auch im Bereich der ERP-Systeme genutzt wird. Es hat den Vorteil, dass eine einfachere Änderung von beispielsweise der Geschäftslogik in der Anwendungsschicht vorgenommen werden kann, da diese von den anderen beiden Schichten entkoppelt ist. Eines der ersten ERP-Systeme, das sich an diesem Modell orientierte, war das System R/3 von SAP im Jahre 1996. Dieses Modell hält sich bis heute und wird nicht nur von SAP eingesetzt, sondern stellt den Standard von heutigen ERP-Systemen dar. Als ein weiteres Beispiel kann Microsoft Dynamics NAV genannt werden, dessen Systemarchitektur in Abbildung 2-2, zur Verdeutlichung des Client-Server-Modells mit seinen Schichten, dargestellt ist. Anhand dieser Darstellung lässt sich erkennen, dass die bereits angesprochene Datenbank die unterste Schicht repräsentiert und somit alle Daten des ERP-Systems zentral in einer Datenbank verwaltet werden können (vgl. Karagiannis & Rieger, 2006).

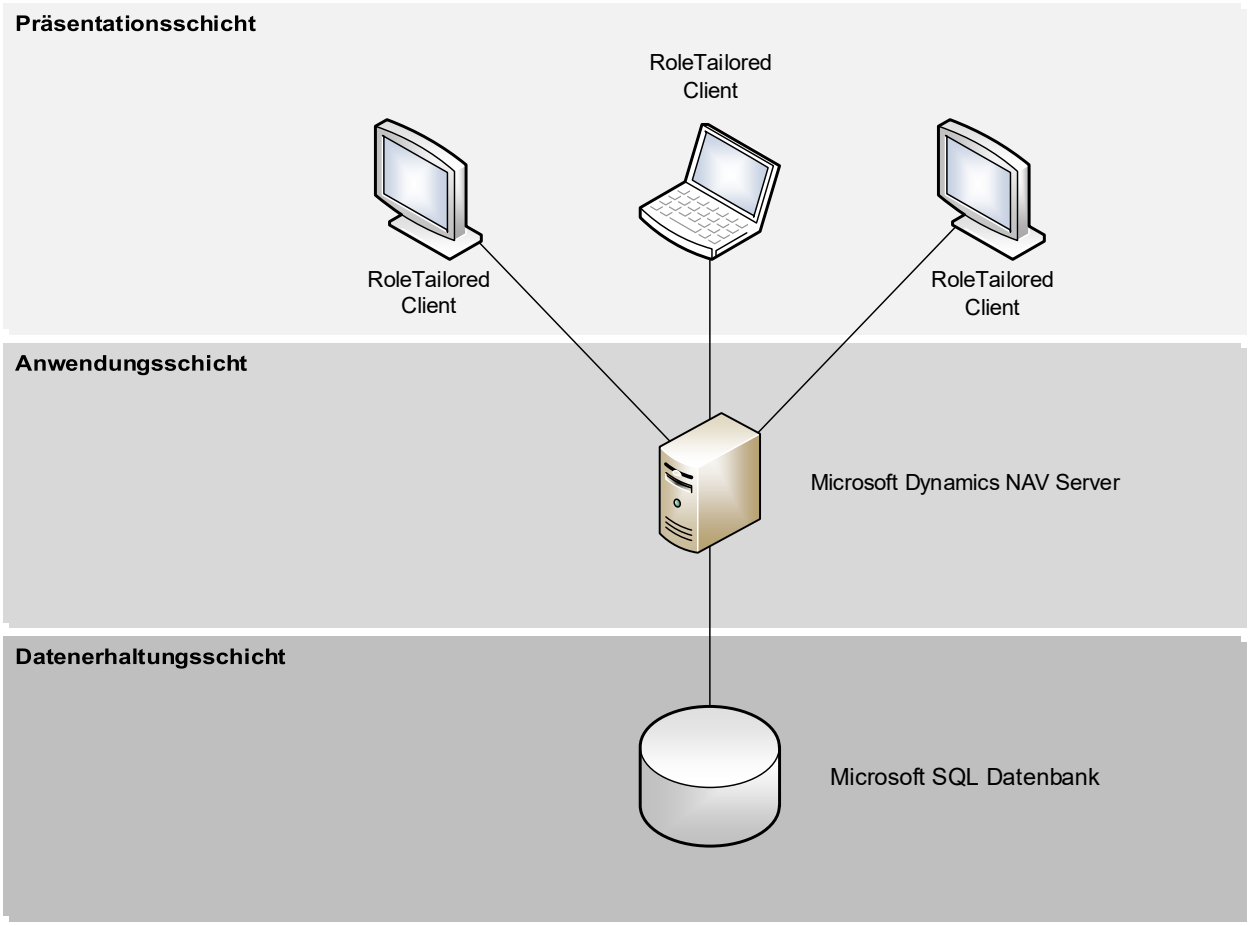


Abbildung 2-2 Client-Server-Modell von Microsoft Dynamics NAV (Karagiannis & Rieger, 2006)

Durch das vermehrte Aufkommen mobiler und zunehmend internetfähiger Geräte musste dieses Modell erweitert werden, sodass heutzutage mindestens eine weitere Schicht benötigt wird. Durch die unterschiedlichen Endgeräte ist es notwendig, die Daten in entsprechende Formate zu konvertieren, damit diese von den jeweiligen Endgeräten verarbeitet werden können. Da diese Änderung die Präsentationsschicht betrifft, wird hier eine Aufteilung in die Schichten Präsentationslogik und Präsentation vorgenommen. Dabei kümmert sich die Präsentationslogik um die Interpretation, Konvertierung und Bereitstellung der Daten, während die Schicht der Präsentation nur noch die Aufgabe der reinen Darstellung der Daten erfüllt, was die Plattformunabhängigkeit fördert (vgl. Karagiannis & Rieger, 2006).

Neben der Schichtenarchitektur rückten ab Anfang des 20. Jahrhunderts zunehmend die Anbieter von Web Services in den Fokus. Web Services stützen sich dabei auf das Konzept der serviceorientierten Architektur, auch als ‚Service Oriented Architecture' (SOA) bezeichnet (vgl. Karagiannis & Rieger, 2006):

> *„Mit dem SOA-Ansatz wird die starre Schichtenbildung [...], bei denen die Systemkomponenten fest an bestimmten Stellen verankert sind, aufgeweicht. Stattdessen gibt es ganz allgemeine Dienste (Services), die von Dienstanbietern (Service Providers) angeboten werden und von Verbrauchern (Service Consumers) genutzt werden können. Im Extremfall besteht die Architektur aus einer Sammlung von*

> *Dienstanbietern und Verbrauchern, die in einem Netzwerk zusammenwirken.“ (Karagiannis & Rieger, 2006)*

Web Services werden auf Basis der neuesten Webtechnologien betrieben und weisen neben loser Kopplung eine hohe innere Festigkeit auf. Auch ERP-Anbietern wurde dieser Wandel bewusst, was dazu führte, dass sie die ERP-Systeme an die SOA anpassten. Dieser Wandel hin zu Web Services bildet damit die Grundlage für die weitere Forschung (vgl. Karagiannis & Rieger, 2006).

Aus Gründen der Vollständigkeit sollen an dieser Stelle auch die Nachfolger der SOA, die Mikroservices, erwähnt werden. Mikroservices bauen ebenfalls auf dem Konzept der Webservices auf, verfolgen jedoch einen anderen Ansatz. Mikroservices modularisieren die Software, lassen diese aber als gänzlich eigenen Prozess laufen. Dies stellt gleichzeitig die Neuerung dar, die durch Mikroservices gegeben ist. Durch diesen Architekturansatz ist es den einzelnen Services möglich, sich auf eine einzige Aufgabe zu konzentrieren (vgl. Wolff, 2016).

Anders als bei Systemen, die sich im lokalen Netzwerk befinden, ermöglicht Cloud-Computing einen Zugriff auf Ressourcen von allen Orten der Welt, in denen ein Zugriff auf das Internet möglich ist (ausgenommen sind hier VPN-Verbindungen zum lokalen Netzwerk). Dies bringt jedoch auch mehrere Nachteile mit sich, wie zum Beispiel lange Antwortzeiten oder instabile Verbindungen (vgl. Baun, Kunze, Nimis & Tai, 2011). Daher empfiehlt sich eine „schwach gekoppelte, asynchrone und nachrichtenbasierte Kommunikation über Web Services“ (ebd.).

An dieser Stelle muss außerdem erwähnt werden, dass die konkreten Technologien, die im Hintergrund verwendet werden, vom jeweiligen Anbieter des ERP-Systems und der Version abhängen (vgl. Karagiannis & Rieger, 2006). Dieser Abschnitt soll damit lediglich der allgemeinen Aufarbeitung der Systemarchitektur in Bezug auf ERP-Systeme dienen.

2.1.4 Herausforderungen

Neben der Zentralisierung der Daten bieten ERP-Systeme noch weitere Vorteile, die auf Basis der Forschung von Rashid, Hossain und Patrick (2002) in Tabelle 2-1 dargestellt sind.

Vorteil	**Erreichung durch**
Zuverlässiger Informationszugang	Datenbankmanagementsystem, konsistente Daten, verbessertes Berichtswesen
Vermeidung von Datenredundanz	Module sind in der gleichen Datenbank vereint
Skalierbarkeit	Strukturierter und modularer Aufbau
Wartbarkeit	Wartung durch den Lieferanten des ERP-Systems

Tabelle 2-1 Vorteile von ERP-Systemen (Rashid et al., 2002)

Trotz der Vorteile von ERP-Systemen, stehen ihnen auch Herausforderungen gegenüber. Wird ein ERP-System nicht von der technischen Seite betrachtet, so wird deutlich, dass dessen Erfolg schlussendlich von den Benutzerinnen und Benutzern abhängt. Wie in Kapitel 1 bereits erwähnt, wünschen sich diese im Berufsumfeld zunehmend den Komfort, den sie aus dem Privatleben gewohnt sind. Dies führt dazu, dass ERP-Systeme, deren Clients in der Vergangenheit auf einem lokalen Rechner installiert wurden, einen Wandel durchlaufen. Die technischen Grundlagen dafür sind mit der Schichtenarchitektur und der SOA bereits gegeben (vgl. Osintsev, 2016).

Unternehmen werden jedoch mit noch weiteren Herausforderungen konfrontiert, die Osintsev (2016) folgendermaßen beschreibt:

> *„How to successfully select a software package is important but not the last problem that will appear on the thorny path toward getting the whole system (software and hardware, server, and users) working together and bringing any value back to the company. Another set of implementation issues is related to the technical part of the project. More than likely servers and workstations will need to be revised to accommodate the new system, and new and more modern ones may need to be ordered, purchased, and replaced. The internal network also has to be analyzed and modernized if required, and the speed and bandwidth of the existing Internet access should be taken into consideration along with possible technical concerns about the mobile devices being used.“ (Osintsev, 2016)*

Bisher wurden ERP-Systeme ‚On-Premise' betrieben, was bedeutet, dass die Server vom Unternehmen selbst gekauft, gewartet und skaliert werden mussten. Für Unternehmen fallen dadurch hohe Kosten für den Betrieb eines ERP-Systems an, weil zusätzlich fähiges Personal engagiert werden muss, um den Betrieb aufrechtzuerhalten. Nicht nur die Kosten, sondern der generelle Wandel der Technologie in den letzten Jahren machte es notwendig, dass sich ERP-Systeme an die neuen Technologien anpassen, um aktuelle Bedürfnisse erfüllen zu können. Mit dem Aufkommen des Cloud-Computings wird ERP-Systemen eine Möglichkeit geboten, die Anforderungen genau dieses Wandels zu bewältigen (vgl. Osintsev, 2016).

2.2 Cloud-Computing

Während ERP-Systeme viele Vorteile in sich vereinen, wie zum Beispiel Flexibilität, Integration zwischen den Abteilungen oder Management von Ressourcen, bergen sie auch mehrere Nachteile. Unter anderem können Probleme durch die Kosten und Schwierigkeiten bei der Einführung eines ERP-Systems entstehen. Diese Gründe sind unter anderem verantwortlich dafür, dass eine andere Lösung gefunden werden musste, die sich, bezogen auf die Systemarchitektur, vom Client-Server-Modell löst. Diese Lösung findet sich heutzutage im Cloud-Computing (vgl. Jain & Sharma, 2016).

Dieser Abschnitt dient zum besseren Verständnis des Begriffes Cloud-Computing und klärt, wie es als Basis für ein ERP-System genutzt werden kann. Dabei sollen neben einer allgemeinen

Einführung und Definition des Begriffes Cloud-Computing auch Abgrenzungen zu diesem Begriff getroffen werden.

2.2.1 Definition

Der Begriff Cloud-Computing gilt laut Bräuninger, Haucap, Stepping und Stühmeier (2012) als Schlagwort für den Wandel der Technikwelt der letzten Jahre. Dabei geht es hier weniger um eine technologische Revolution, als vielmehr um die Kombination von bestehenden Technologien und Methoden, die zu einem Gesamtkonzept vereint wurden. Dieser Wandel zeigt sich vor allem im Privatleben der Menschen. Anstatt Dokumente, Fotos und Musik lokal auf dem Rechner oder einer externen Festplatte zu speichern, werden die Daten in die sogenannte Cloud oder auch ‚Wolke' verschoben. Cloud-Computing ist jedoch auch auf Unternehmen anwendbar. Damit dient es dem klassischen Rechenzentrum als Konkurrenz und Alternative (vgl. Bräuninger et al., 2012). Für die Benutzer und insbesondere die IT-Abteilung ergeben sich durch dieses Konzept neue Möglichkeiten, die jedoch zu einem Paradigmenwechsel führen (vgl. Plass, Rehmann, Zimmermann, Janssen & Wibbing, 2013).

Bisher konnte die IT-Abteilung alle Systeme im unternehmenseigenen Rechenzentrum verwalten und hatte damit jederzeit die volle Kontrolle. Durch das Cloud-Computing ist es nun möglich, Teile der IT-Infrastruktur in die ‚Wolke' auszulagern. Diese Variante hat im Gegensatz zum Rechenzentrum den Nachteil, dass die IT-Abteilung keinen direkten und vollständigen Zugriff auf die IT-Infrastruktur und die Systeme mehr besitzt (vgl. Plass et al., 2013). Nach Plass et al. (2013) führt dieser Paradigmenwechsel mit all seinen Chancen und Risiken zu den immer gleichen Erwartungen unter Managern und Unternehmern:

- Einfache Skalierbarkeit
- IT zu günstigem Preis
- IT nach dem Motto „so einfach wie Strom aus der Steckdose" (Plass et al., 2013)
- Entfall von Wartungsfenstern
- 7/24 Verfügbarkeit (vgl. Plass et al., 2013)

Auch Mell und Grance (2011), die Autoren der Publication ‚The NIST Definition of Cloud Computing' für das National Institute of Standards and Technology (NIST), stellen das Cloud-Computing als ein sich entwickelndes Paradigma dar, das sie folgendermaßen definieren:

> *„Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models." (Mell & Grance, 2011)*

Diese Definition aus dem Jahre 2011 ist die am häufigsten zitierte Definition und spricht dabei von fünf essenziellen Charakteristiken, drei Service- und vier Bereitstellungsmodellen (vgl. Doedt, 2013). In den nachfolgenden Abschnitten sollen diese drei Bereiche näher betrachtet werden.

2.2.2 Charakteristiken

Nicht jeder Service, der im Internet verfügbar ist, fällt unter den Begriff Cloud-Computing. Zu diesem Zweck definieren Mell und Grance (2011) fünf essenzielle Charakteristiken, die erfüllt sein müssen, um von Cloud-Computing sprechen zu können:

- On-demand self-service (Selbstbedienung auf Abruf)
- Broad network access (breiter Netzwerkzugriff)
- Resource pooling (Bündelung von Ressourcen)
- Rapid elasticity (schnelle Elastizität)
- Measured service (messbare Dienste) (vgl. Mell & Grance, 2011)

Unter ‚on-demand self-service' wird beim Cloud-Computing die Möglichkeit verstanden, die Leistung, den Speicherplatz und die verwendete Software einfach und schnell zu verwalten. Dabei ist es möglich, während der Laufzeit in jede Richtung zu skalieren, ohne den Betrieb zu stören oder zu unterbrechen. Des Weiteren besteht der Vorteil darin, dass durch dieses Vorgehen keine Interaktion mit dem Anbieter des Service benötigt wird (vgl. Mell & Grance, 2011).

Die angebotenen Dienste des Cloud-Computings sollen per Definition von sogenannten Thin- und Thick-Clients verwendet werden können. Unter Thin- und Thick-Clients werden im Allgemeinen Mobiltelefone, Tablets, Laptops und PCs verstanden. Der Zugriff auf angebotene Dienste soll somit für diese Geräte einfach möglich sein. Dieses Charakteristikum wird als ‚broad network access' bezeichnet (vgl. Mell & Grance, 2011).

Für das ‚resource pooling' soll der Cloud-Computing-Anbieter mit der Hilfe eines Multi-Mandanten-Systems die Ressourcen gebündelt und je nach Bedarf an einen entsprechenden Rechner weitergeben können. Die Benutzerin oder der Benutzer empfängt dabei Ressourcen, ohne eine konkrete Auskunft über die Herkunft zu erhalten. Bei der Betrachtung einer höheren Abstraktionsschicht ist es sogar möglich, einer Benutzerin oder einem Benutzer zum Beispiel aufgrund des Landes, wo sie oder er arbeitet, Ressourcen zuzuteilen. Bei den hier angesprochenen Ressourcen kann es sich um Speicher, Netzwerkbandbreite oder auch Arbeitsspeicher handeln (vgl. Mell & Grance, 2011). Des Weiteren erwähnen Rountree und Castrillo (2014), dass das ‚resource pooling' auf dem Prinzip basiert, dass nicht alle Ressourcen gleichzeitig von allen Benutzerinnen und Benutzern verwendet werden. Stattdessen können Ressourcen, die momentan ungenutzt sind, einer anderen Benutzerin oder einem anderen Benutzer zugewiesen werden. Dies kann aus technischer Sicht zum Beispiel durch Virtualisierung ermöglicht werden.

Das vierte Charakteristikum der ‚rapid elasticity' beschäftigt sich mit der Elastizität von Cloud-Computing. Damit ist gemeint, dass es möglich ist, Ressourcen jederzeit zuzuweisen und auch

wieder wegzunehmen. Für die Benutzerin oder den Benutzer sieht es dabei so aus, als würde zu jedem Zeitpunkt die Menge an Ressourcen zur Verfügung stehen, die gerade benötigt wird (vgl. Mell & Grance, 2011). Dieses Charakteristikum wird mit einer Automatisierung und Orchestrierung erreicht. Benötigt eine Benutzerin oder ein Benutzer mehr Ressourcen, so wird beispielsweise ein Ereignis ausgelöst, das automatisch mehr Ressourcen für die aktuellen Tätigkeiten zur Verfügung stellt. Dies führt dazu, dass auch nur ein kurzer Bedarf an mehr Ressourcen schnell gedeckt werden kann (vgl. Rountree & Castrillo, 2014).

Aus den bisherigen Charakteristika lässt sich erkennen, dass Ressourcen wie zum Beispiel Speicherplatz, Arbeitsspeicher oder Prozessorleistung für den aktuellen Bedarf eingestellt werden können. Da Anbieter von Cloud-Computing diese Leistungen verrechnen, bedarf es einer genauen Aufstellung der verbrauchten Ressourcen. Um dies gewährleisten zu können, müssen die angebotenen Dienste messbar sein (‚measured service'). Diese Messbarkeit dient der größtmöglichen Transparenz, sodass der Ressourcenverbrauch überwacht, kontrolliert und gemessen werden kann (vgl. Mell & Grance, 2011).

2.2.3 Servicemodelle

Wie in den vorherigen Abschnitten beschrieben, bauen ERP-Systeme auf mehreren Schichten auf oder nutzen SOA, um auf Funktionalitäten zugreifen zu können. Das Cloud-Computing bietet für dieses Anwendungsgebiet verschiedene Servicemodelle. Da Cloud-Computing jedoch nur als Oberbegriff gelten kann, ist es notwendig, eine Differenzierung der sich dahinter verbergenden verschiedenen Begrifflichkeiten vorzunehmen (vgl. Plass et al., 2013).

In der Vergangenheit haben sich drei Modelle durchgesetzt, die in unterschiedliche Ebenen (Abbildung 2-3) untergegliedert werden (vgl. Mell & Grance, 2011):

- Software-as-a-Service (SaaS)
- Platform-as-a-Service (PaaS)
- Infrastructure-as-a-Service (IaaS) (vgl. Mell & Grance, 2011)

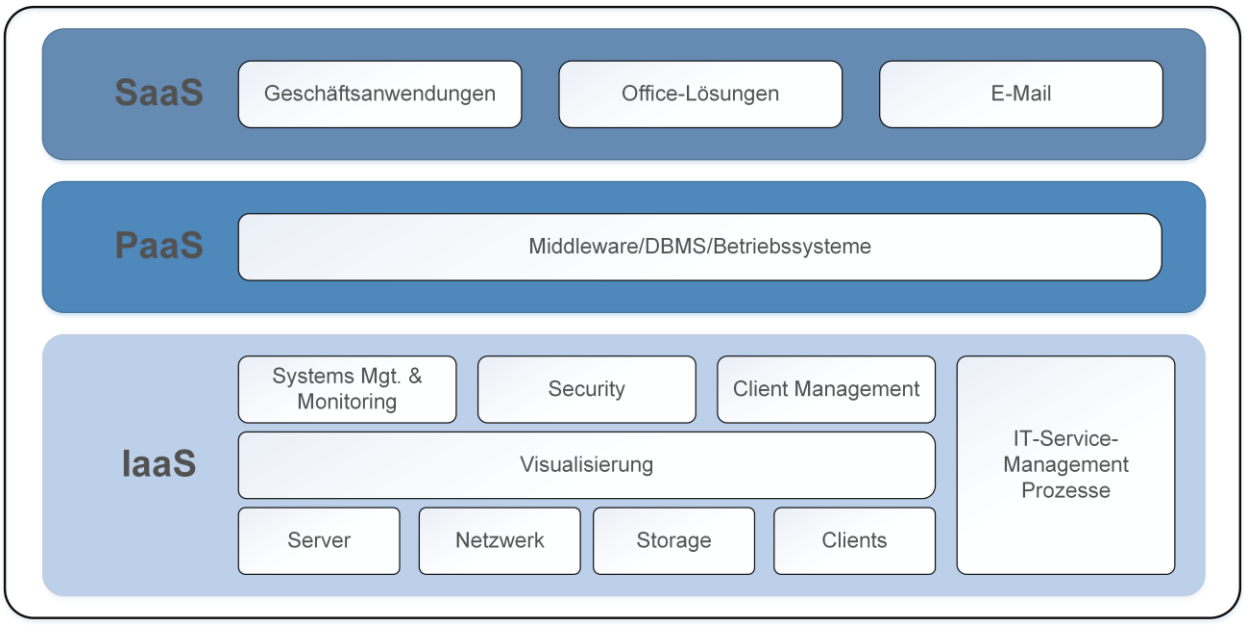


Abbildung 2-3 Ebenen im Cloud-Computing (Plass et al., 2013)

Die unterste Ebene bildet dabei Infrastructure-as-a-Service (IaaS), das als Oberbegriff für alle Leistungen im Bereich der IT-Infrastruktur verwendet wird. Ein Unternehmen bekommt dafür im einfachsten Fall Rechen- und Speicherleistung zur Verfügung gestellt. Der Vorteil gegenüber einem herkömmlichen und unternehmenseigenen Rechenzentrum ergibt sich daraus, dass sich das Unternehmen nicht selbst um die Wartung oder Inbetriebnahme kümmern muss. Neben Rechen- und Speicherleistung stellen IaaS-Lieferanten auch noch andere Leistungen, wie zum Beispiel das Systemmanagement und Monitoring-Services zur Verfügung. Die Praxis zeigt, dass vor allem mittelständische Unternehmen über zu kleine IT-Abteilungen mit zu wenig Know-how verfügen, als dass diese sich professionell und adäquat um dieses Bereiche zu kümmern könnten (vgl. Plass et al., 2013). IaaS hat zusätzlich den Vorteil, dass das Unternehmen nur für die Leistung zahlt, die es wirklich in Anspruch nimmt. Im Vergleich zu einem herkömmlichen Rechenzentrum fallen für nicht benutzte Server oder Speicher keine Kosten kann. Um die IaaS-Leistungen anbieten zu können, wird im Hintergrund mit Virtualisierung und Automatisierung gearbeitet (vgl. Ostermann, Prodan & Fahringer, 2010). Hier lassen sich bereits die Charakteristika (gebündelte Ressourcen) des Cloud-Computings in der Praxis erkennen.

Die mittlere Ebene Platform-as-a-Service (PaaS) dient der Bereitstellung einer Entwicklungsplattform für Anwendungsentwicklerinnen und -entwickler, Softwarearchitektinnen und -architekten sowie Anwendungsintegratorinnen und -integratoren. Diese Möglichkeit gilt als einfach und kostengünstig (vgl. Ostermann et al., 2010). Mit PaaS entfallen Verwaltungsaufgaben wie die Wartung und Erstellung solcher Plattformen und die Nutzergruppen können sich vermehrt den eigentlichen Aufgaben widmen, anstatt „wie bisher allzu viel Zeit mit den aus Entwickler-Sicht lästigen Verwaltungsaufgaben zu vergeuden“ (Plass et al., 2013). Typischerweise bieten PaaS-Lieferanten Services wie zum Beispiel Datenbankmanagementsysteme, Entwicklungsplattformen oder Versionsverwaltungen an. Wie alle Cloud-Services sind diese ebenfalls in beide Richtungen skalierbar und können jederzeit an die Bedürfnisse der Benutzerinnen und Benutzer angepasst werden (vgl. Plass et al., 2013).

Anders als bei IaaS und PaaS werden dem Unternehmen auf der obersten Ebene, Software-as-a-Service (SaaS), komplette Services zur Verfügung gestellt. SaaS gilt dabei als der populärste Vertreter im Bereich Cloud-Computing und bietet dem Unternehmen unter anderem Applikationen zum Speichern von Dateien, Werkzeuge für gemeinsames Arbeiten oder auch ERP-Systeme. Der Unterschied zu traditionellen Internetseiten und Applikationen liegt darin, dass SaaS die Charakteristiken von Cloud-Computing erfüllt. So können SaaS-Applikationen schnell und einfach skaliert werden und sind auf Thin- und Thick-Clients sofort verfügbar (vgl. Marinos & Briscoe, 2009).

Plass et al. (2013) nennt als eindrücklichstes Beispiel für eine SaaS-Applikation das CRM-System. Wird dieses als SaaS bezogen, so können Angestellte im Vertrieb jederzeit von extern auf das System zugreifen und ihre Daten verwalten. Einen Überblick über die konkreten Services, die in den Bereichen SaaS, IaaS und PaaS angeboten werden, gibt die Tabelle 2-2.

Modell	**Anbieter**	**Name**	**Kurzbeschreibung**
IaaS	Amazon	EC2	Virtueller Server
PaaS	Google	Google App Engine	Entwicklungsplattform
PaaS	Microsoft	Windows Azure	Entwicklungsplattform
SaaS	Google	Google Apps	Anwendung
SaaS	Microsoft	MS Office 365	Anwendung

Tabelle 2-2 Beispiele für Service-Modelle im Bereich Cloud-Computing (Berry, o.J.)

Zur Verdeutlichung, welche Rolle das Cloud-Computing für einzelne Personengruppen spielt, dient die Abbildung 2-4. Dabei werden die Beziehungen zwischen den Schichten und die Unterschiede zwischen den Rollen nochmals in grafischer Form dargestellt. Marinos und Briscoe (2009) bestätigen damit das Prinzip der Ebenen im Cloud-Computing.

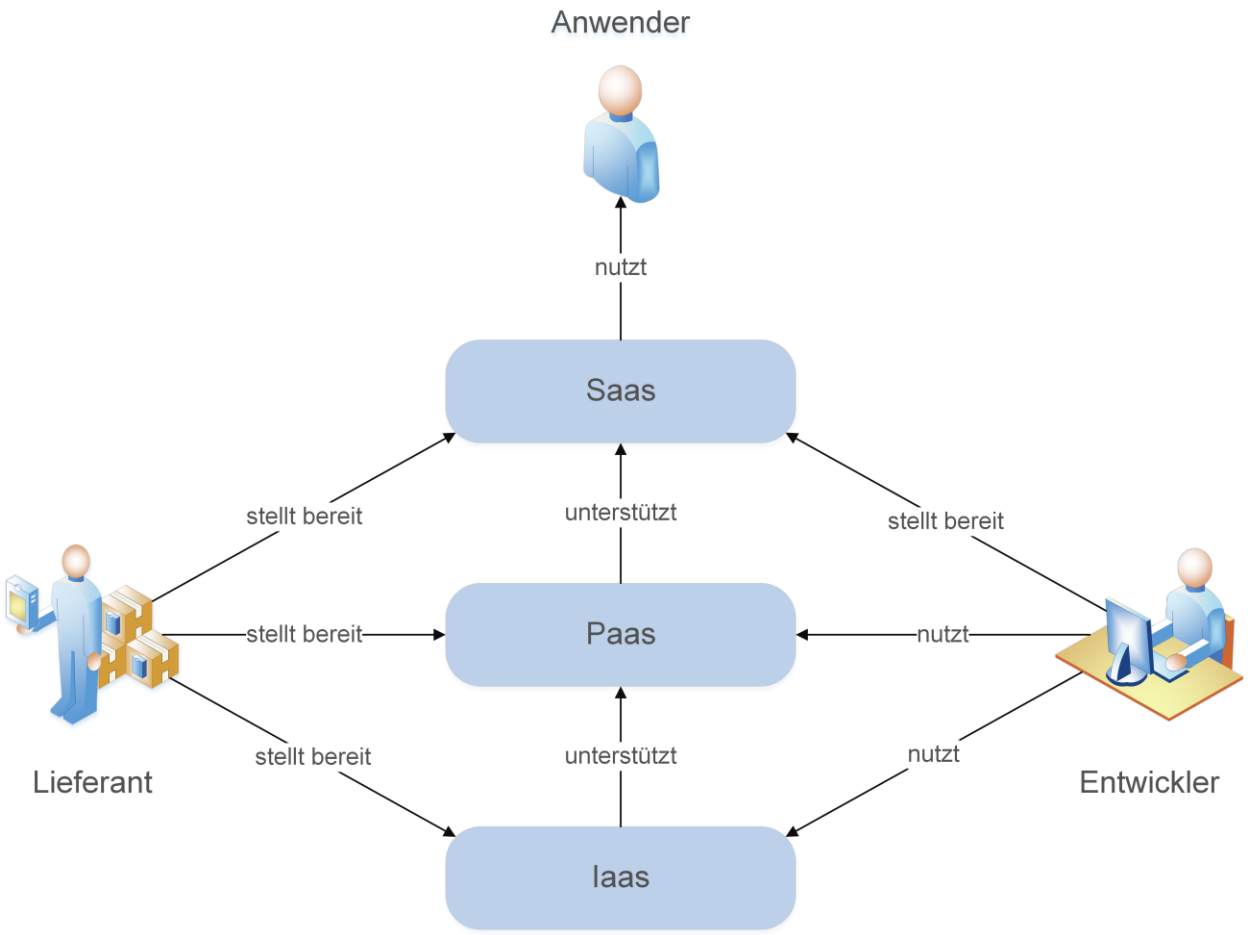


Abbildung 2-4 Ebenen im Cloud-Computing (Marinos & Briscoe, 2009)

Während der Cloud-Computing-Lieferant auf jeder Ebene etwas zur Verfügung stellt, nutzt die Entwicklerin oder der Entwickler der Services nur die beiden unteren Ebenen IaaS und PaaS dazu, um die Software über die Cloud der Endanwenderin oder dem Endanwender anzubieten. Die Endanwenderin oder der Endanwender hat im Gegensatz zu den beiden anderen Akteuren nichts mit den zwei unteren Ebenen zu tun, sondern stellt eine reine Konsumentin oder einen reinen Konsumenten der obersten SaaS-Schicht dar. Des Weiteren zeigt sich hier die Beziehung zwischen den drei Ebenen: So wird erkennbar, dass die jeweils untere Schicht die darüberliegende unterstützt (vgl. Marinos & Briscoe, 2009).

2.2.4 Bereitstellungsmodelle

Das Bereitstellungsmodell, das als erstes den Einzug in die IT gefunden hat, ist die Public Cloud. Mit der Public Cloud stellen die jeweiligen Anbieter ihre Services der öffentlichen Masse zur Verfügung. Das Modell bietet über das Internet skalierbare Ressourcen an, die für gewöhnlich auf Basis der verwendeten Ressourcen abgerechnet werden. Dadurch, dass kein Zugriff auf die Infrastruktur der Public Cloud besteht, sind die Nutzer auf den Cloud-Anbieter angewiesen und müssen dessen Systemen vertrauen. Die Ressourcen werden dabei mit den verschiedenen Anwendern geteilt (vgl. Furht & Escalante, 2010).

Während sich die Public Cloud im Privatleben bereits durchgesetzt hat, eignet sie sich für bestimmte Unternehmen nur bedingt. Durch immer strenger werdende Gesetze und Vorschriften, sei es vom Staat oder vom Unternehmen selbst, ist es beispielsweise nahezu unmöglich, Banken oder Versicherungen mit einer Public Cloud auszustatten. Der Weg aus dem eigenen Rechenzentrum sorgt vor allem in den Bereichen IT-Sicherheit, Performanz oder auch Unternehmensregularien für Probleme (vgl. Furht & Escalante, 2010).

Im Gegensatz zur Public Cloud gibt die Private Cloud die Verwaltung von Ressourcen wieder an das Unternehmen zurück. Die Firmen können dabei selbstständig Cloud-Services anbieten und diese im Unternehmensnetzwerk zur Verfügung stellen. Der Cloud-Anbieter und die Angestellten des Betriebes befinden sich somit im gleichen Unternehmen. Einen Zugang zum System können dabei die Mitarbeiterinnen und Mitarbeiter, die Kundinnen und Kunden und die Lieferantinnen und Lieferanten des Unternehmens erhalten, jedoch nicht die öffentliche Masse (vgl. Furht & Escalante, 2010).

Durch Schutzmechanismen, wie zum Beispiel eine Firewall, kann das Unternehmen selbstständig für die Sicherung der Daten sorgen. Dies dient als Hauptargument, wenn es um die Entscheidung zwischen einer Public und einer Private Cloud geht. Anstatt den Sicherheitsmechanismen des (unternehmensfremden) Cloud-Anbieters zu vertrauen, liegt es am Unternehmen selbst, sich um den Schutz der Daten zu kümmern. Dies ermöglicht die Einhaltung von Regularien, die in vielen Branchen mit der Public Cloud kaum zu bewältigen sind. Daraus lässt sich schließen, dass die Private Cloud nur für Großunternehmen sinnvoll ist (vgl. Baun et al., 2011).

Da die Private Cloud vom Unternehmen selbst aufgebaut und gewartet werden muss, lässt sich auf den ersten Blick kein Unterschied zu einem herkömmlichen Rechenzentrum erkennen. Die Private Cloud erfüllt dennoch alle Charakteristika des Cloud-Computings, die von einem Rechenzentrum nicht erfüllt werden. Besonders hervorzuheben ist dabei das Charakteristikum der gebündelten Ressourcen. Dadurch wird in der Private Cloud eine flexible Zuteilung der Ressourcen ermöglicht und durch Visualisierung bei den Kosten gespart (vgl. Plass et al., 2013).

Will das Unternehmen seine Lösung nach oben skalieren, so wird zu jeder Zeit die Auslagerung in die Public Cloud gewährleistet. Dabei muss auf eine saubere Trennung zwischen sicherheitskritischen und nicht sicherheitskritischen Daten erfolgen (vgl. Baun et al., 2011). Dem stimmen auch Furht und Escalante (2010) zu, die die Datenlagerung in der Private Cloud als Zwischenschritt zur Speicherung in der Public Cloud sehen. Als Beispiel nennen sie dabei E-Mails, die bereits den Weg in die Public Cloud gefunden haben.

Fehlen Fachkräfte, die sich um den Aufbau und die Verwaltung der Private Cloud kümmern, kann eine Unterteilung in zwei weitere Bereiche vorgenommen werden. Die eine Variante ist die Managed Private Cloud, bei der die Private Cloud auch weiterhin im eigenen Rechenzentrum und Unternehmensnetzwerk betrieben wird. Die Verwaltung obliegt jedoch nicht mehr dem Unternehmen, sondern einem externen Unternehmen, das sein Wissen zur Verfügung stellt und sich um den Aufbau und die Verwaltung der Managed Private Cloud kümmert. Durch diese Auslagerung können auch Unternehmen mit fehlendem Know-how die Vorteile der Cloud nutzen (vgl. Plass et al., 2013). Die zweite Variante der Private Cloud ist die Outsourced Private Cloud, die im Unterschied zur Managed Private Cloud nicht im eigenen Rechenzentrum betrieben wird.

Auch bei dieser Variante kommt ein externes Unternehmen ins Spiel, das seine Hard- und Software zur Verfügung stellt, um eine Private Cloud aufzubauen. Diese Hard- und Software wird jedoch nur für ein einzelnes Unternehmen bereitgestellt (vgl. Plass et al., 2013). Der Zusammenhang zwischen den genannten Bereitstellungsmodellen wird in Abbildung 2-5 nochmals grafisch dargestellt.

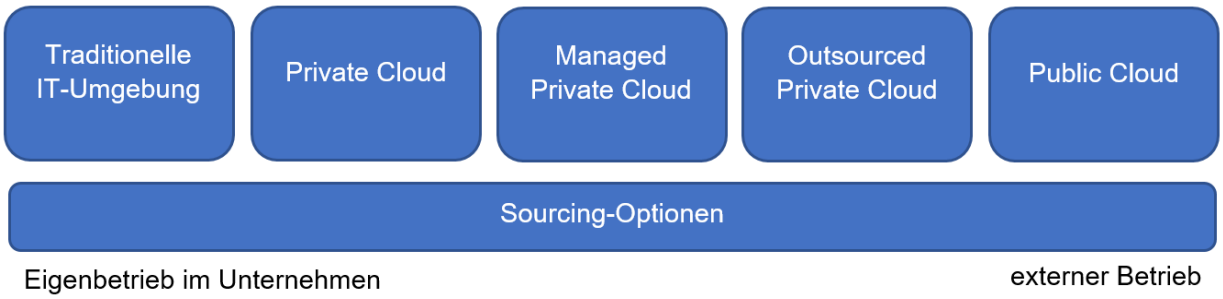


Abbildung 2-5 Übergange von der Private in die Public Cloud (Plass et al., 2013)

Neben der Private und der Public Cloud existiert zudem noch die Hybrid Cloud, die eine Mischform aus den beiden ersten Bereitstellungsmodellen ist. In diesem Fall betreibt ein Unternehmen grundsätzlich eine Private Cloud, nutzt jedoch zusätzlich Dienste aus der Public Cloud. Diese Dienste dienen der besseren Skalierung und zur Abdeckung von Lastspitzen, die während des Betriebes der Systeme auftreten können. Auch in Hinblick auf die Verwendung der Hybrid Cloud müssen im Vorfeld Überlegungen angestellt werden, welche Daten sicherheitskritisch sind und somit in der Private Cloud bleiben müssen. Das Unternehmen kann durch die Hybrid Cloud einerseits die Kontrolle über diese Daten behalten, andererseits aber auch von den Vorteilen der Public Cloud und deren Skalierungsmöglichkeiten profitieren (vgl. Plass et al., 2013).

Das vierte und letzte Bereitstellungsmodell stellt die Community Cloud dar. Diese ähnelt vom Grundprinzip her der Private Cloud. Der Unterschied ist jedoch, dass die Community Cloud mehrere Private Clouds miteinander verbindet. Das bedeutet, dass die Infrastruktur hinter der Cloud für mehrere Unternehmen mit den gleichen Interessen bereitgestellt wird. Die Verwaltung dieser Community Cloud kann dabei von einem der Unternehmen oder auch von einem externen Unternehmen durchgeführt werden (vgl. Mell & Grance, 2011).

Aus den Definitionen der vier Bereitstellungsmodelle lassen sich vor allem Unterschiede in den Bereichen der Datensicherheit und der Flexibilität erkennen. Diese zwei Dimensionen lassen sich für jedes Bereitstellungsmodell in Beziehung miteinander setzen, sodass die verschiedenen Eigenschaften nochmals verdeutlicht werden können. Abbildung 2-6 dient dabei als grafische Darstellung des zweidimensionalen Schemas (vgl. Lipsky, 2011).

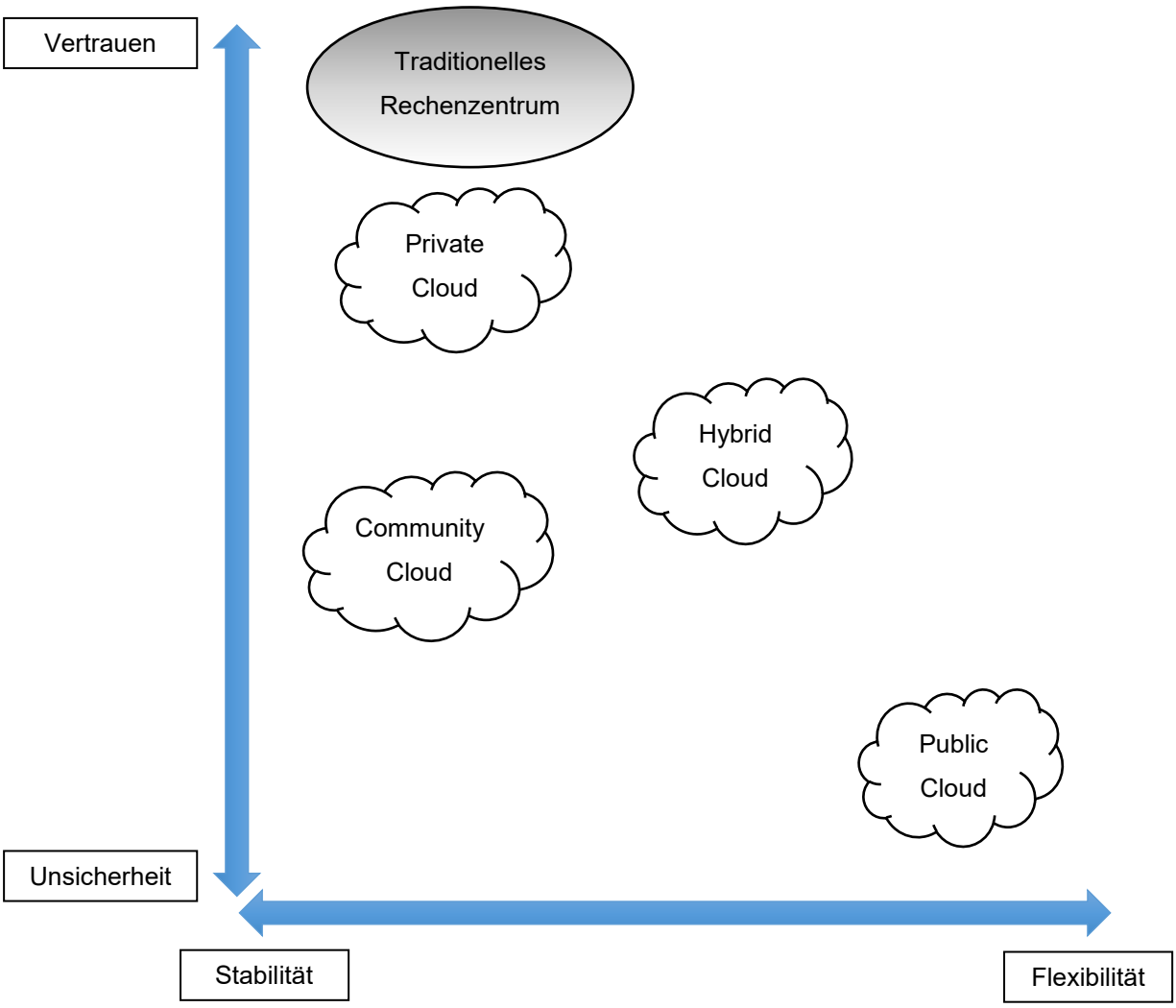


Abbildung 2-6 Vergleich der Bereitstellungsmodelle in der Cloud (Lipsky, 2011)

2.2.5 Begriffsabgrenzung

Da nun die Definition des Cloud-Computings, die dafür zu erfüllenden Charakteristika und mögliche Service- sowie Bereitstellungsmodelle herausgestellt wurden, ist es wichtig, den Begriff von anderen Technologien und Paradigmen schärfer abzugrenzen. Laut Zhang, Cheng und Boutaba (2010) wird Cloud-Computing vor allem mit den Technologien in Verbindung gesetzt, die im Folgenden kurz vorgestellt und voneinander abgrenzt werden:

- Grid-Computing
- Utility-Computing
- Virtualisierung
- Autonomic-Computing (vgl. Zhang et al., 2010)

Beim Grid-Computing handelt es sich um ein Paradigma, dessen Ziel es ist, verteilte Ressourcen in einem koordinierten Netzwerk zusammenzufassen. Beispielsweise benötigen Forschungsinstitutionen eine hohe Rechenleistung, die von den Ressourcen der einzelnen Institute nicht

erreicht werden kann. Aus diesem Grund werden diese zusammengeschlossen, um den fortlaufenden Betrieb von rechenintensiver Software zu gewährleisten. Das Cloud-Computing weist dabei Ähnlichkeiten mit dem Grid-Computing auf, da es ebenfalls versucht, verteilte Ressourcen zusammenzuschließen. Während Grid-Computing jedoch ein reiner Zusammenschluss von verteilter Hardware ist, geht Cloud-Computing einen Schritt weiter, da die Bereitstellung von Ressourcen durch Virtualisierung auf mehreren Ebenen erfolgt und eine dynamische Zuteilung ermöglicht (vgl. Zhang et al., 2010).

Utility-Computing meint ein Modell, das Ressourcen On-Demand zur Verfügung stellt und je nach Nutzung abrechnet. Cloud-Computing kann somit als Umsetzung des Utility-Computings verstanden werden. Es übernimmt dabei die Idee des leistungsbasierten Preisschemas und führt zu einer Maximierung der Auslastung und Minimierung der Betriebskosten auf Seiten der Anbieter (vgl. Zhang et al., 2010).

Virtualisierung dient als Basis des Cloud-Computings und stellt eine seiner Komponenten dar. Unter Virtualisierung werden dabei die Abstraktion von physikalischer Hardware und die Bereitstellung virtualisierter Ressourcen verstanden. Die Server nennen sich virtuelle Maschinen (VM) und werden beim Cloud-Computing für das dynamische Zuteilen von Ressourcen eingesetzt (vgl. Zhang et al., 2010).

Die letzte Technologie geht auf eine Entwicklung von IBM aus dem Jahre 2001 zurück und nennt sich Autonomic-Computing. Dabei geht es um den Aufbau von Systemen, die sich selbst verwalten können und dabei auf interne und externe Beobachtungen reagieren. Die Besonderheit liegt darin, dass dies ohne menschliches Zutun geschehen soll, womit für Abhilfe in Bezug auf die aufkommende Komplexität der IT gesorgt wird. Obwohl Cloud-Computing ebenfalls automatisierte Komponenten besitzt, geht es hierbei jedoch weniger um Automatisierung als um Kostenreduktion (vgl. Zhang et al., 2010).

Zusammengefasst lässt sich sagen, dass Cloud-Computing Virtualisierung als Basiskomponente nutzt, als Umsetzung von Utility-Computing angesehen werden kann und Gemeinsamkeiten mit dem Grid- und dem Autonomic-Computing aufweist. Somit können diese Begriffe klar vom Cloud-Computing abgegrenzt werden (vgl. Zhang et al., 2010).

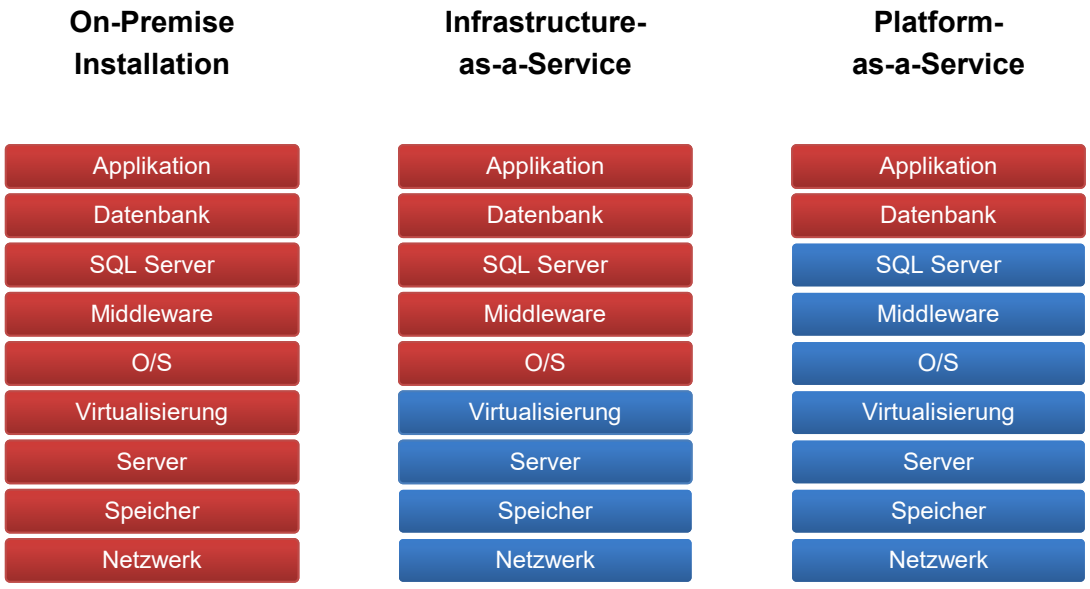
2.2.6 ERP in der Cloud

Zum Abschluss dieses Abschnittes soll ein Blick auf die Bedeutung von Cloud-Computing in Bezug auf ERP-Systeme geworfen werden. Wie bereits in der Einleitung dieser Arbeit erwähnt, können sich ERP-Systeme dem technologischen und sozialen Wandel nicht mehr entziehen. Im Bereich des Cloud-Computings liegt für ERP-Systeme eine SaaS-Lösung nahe, bei der das gesamte ERP-System in der Cloud betrieben und dem Unternehmen zur Verfügung gestellt wird. Mit dieser Lösung spart das Unternehmen vor allem Kosten in den Bereichen Administration, Verwaltung oder auch in Hinblick auf die Angestellten. Zusätzlich entfällt die Bearbeitung bestimmter Themen wie beispielsweise der IT-Sicherheit oder der Skalierung des ERP-Systems (vgl. Doedt, 2013). Die bisherige Literaturrecherche hat jedoch ergeben, dass diese Lösung in dieser Form nicht immer möglich ist (vgl. Abschnitt 2.2.4 Bereitstellungsmodelle).

Bereits jetzt lässt sich erkennen, dass jedes Servicemodell für ein ERP-System in der Cloud seine Vor- und Nachteile hat. Darum bieten Anbieter von ERP-Systemen auch mehrere Lösungen an, die den Anforderungen der unterschiedlichen Unternehmen gerecht werden. SAP, der Marktführer für ERP-Systeme, hat für dieses Problem seine eigenen Lösungen entwickelt. Neben der klassischen SaaS-Lösung wird mit der ‚SAP HANA Cloud Platform' eine PaaS-Lösung zur Verfügung gestellt, die bereits mehrere vordefinierte Schnittstellen bietet. Diese Schnittstellen beziehen sich dabei nicht nur auf andere Cloud-Lösungen, sondern dienen auch der Kommunikation mit On-Premise-Installationen (vgl. SAP, 2016).

Microsoft liefert mit der Azure Cloud ebenfalls eine Möglichkeit, ein ERP-System in der Cloud zu betreiben. Für das Produkt ‚Microsoft Dynamics NAV' gab es bis zur Version 2016 die Möglichkeit, die Azure Cloud als IaaS zu nutzen, seit dieser Version kann ‚Microsoft Dynamics NAV' über PaaS verwendet werden. Somit gibt es mehrere Varianten, ein ERP-System in der Cloud auszuführen (vgl. Chandrasekara, 2016).

Aus vorherigen Abschnitten ist bekannt, dass ‚Microsoft Dynamics NAV' auf der 3-Schichten-Architektur beruht. Wird dies auf die Servicemodelle umgelegt, so befinden sich die Anwendungs- und die Datenerhaltungsschicht bei der PaaS-Lösung in der Cloud. Nun ist es möglich, diese auf dem gleichen Server zu betreiben, was jedoch der Schichtenarchitektur widerspricht und von Microsoft nicht empfohlen wird, oder die beiden getrennt voneinander zu betreiben. Werden die beiden Schichten getrennt, dann befindet sich die Anwendungsschicht, wie gewohnt, auf einem eigenen Server in der Cloud. Die Datenerhaltungsschicht bekommt mit ‚SQL as a Service' eine weitere Möglichkeit für den Betrieb der Datenbank. Durch diese Variante wird für die Datenbank kein eigener Server mehr benötigt, sondern dieser lässt sich ebenfalls als Service beziehen, was alle Vorteile des Cloud-Computings mit sich bringt. Ein übersichtlicher Vergleich zwischen der PaaS-, der IaaS- und der On-Premise Lösung für ‚Microsoft Dynamics NAV' ist in Abbildung 2-7 dargestellt (vgl. Chandrasekara, 2016).



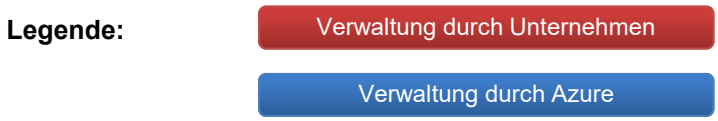


Abbildung 2-7 ‚Microsoft Dynamics NAV' Infrastrukturmöglichkeiten (Chandrasekara, 2016)

Neben den bereits erwähnten Möglichkeiten kann auch die Anwendungsschicht On-Premise betrieben werden, während sich die Datenbank in der Cloud befindet. Es fehlt jedoch ein Angebot für SaaS. Von Microsoft wird dieses Fehlen mit ‚Dynamics 365' gelöst, das nicht nur vom Namen her an ‚Office 365' erinnert. Auch hier ist es möglich, alle Leistungen als SaaS zu beziehen, wobei sich das Angebot bisher auf einige wenige Module beschränkt (vgl. Microsoft, 2017b).

Allen erwähnten Vorteilen stehen auf der anderen Seite auch einige Nachteile gegenüber. Wie beispielsweise bereits im Zuge von SaaS erwähnt, spielen Richtlinien und Gesetze für das Cloud-Computing eine übergeordnete Rolle. Diese Richtlinien und Gesetze sollen unter anderem die Sicherheit der Daten gewährleisten, denn während das Cloud-Computing Skalierbarkeit und Flexibilität mit sich bringt, können im Bereich der IT-Sicherheit Bedenken aufkommen (vgl. Plass et al., 2013).

2.3 IT-Sicherheit

Um zu verstehen, welche Bedenken es im Bereich der IT-Sicherheit bei ERP-Systemen in der Cloud geben kann, muss zunächst ein Verständnis über die Voraussetzungen geschaffen werden. Zu diesem Zweck werden in diesem Abschnitt Grundsätze der IT-Sicherheit sowie Gesetze, Verordnungen oder auch Normen vorgestellt, die für diese Arbeit Relevanz haben. Zu Beginn soll der Begriff IT-Sicherheit definiert werden.

2.3.1 Definition

Die IT-Sicherheit bezieht sich auf IT-Systeme. Bei einem IT-System handelt es sich um „ein geschlossenes oder offenes, dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen" (Eckert, 2013). Unter einem geschlossenen System wird dabei ein System verstanden, das nicht mit anderen Systemen kompatibel ist. Im Gegensatz dazu dient ein offenes System zum Austausch von Informationen und der weltweiten Vernetzung. Aus dieser Definition wird deutlich, dass sich bei ERP-Systemen um offene IT-Systeme handelt (vgl. Eckert, 2013).

Im Zuge der Sicherheit von IT-Systemen werden die vier Begriffe Funktions-, Informations- und Datensicherheit sowie der Datenschutz unterschieden. Funktionssicherheit meint dabei die Eigenschaft, dass die IST-Funktionalitäten den definierten SOLL-Funktionalitäten entsprechen müssen. Sie gewährleistet, dass ein IT-System zu jeder Zeit die definierte Funktionalität liefert. Bei der Informationssicherheit geht es nicht mehr um die Funktionalität, sondern darum, Systemzustände zu verhindern, die zu einer nicht erlaubten Änderung von Informationen führen. Die Informationssicherheit baut dabei auf ein funktionssicheres System auf. Datensicherheit

bedeutet, dass keine Systemzustände zustande kommen, die zu einer nicht erlaubten Änderung von Systemressourcen, meist Daten, führen. Dabei geht es auch um die Sicherung der Daten, sodass im schlimmsten Fall die Daten wiederhergestellt werden können. Im Gegensatz zu den vorigen drei Begriffen betrifft der Datenschutz das Verhalten der Benutzer. Zur Sicherung des Datenschutzes muss die Weitergabe von Informationen kontrolliert werden (vgl. Eckert, 2013).

Eckert (2013) definiert IT-Sicherheit auf Basis dieser vier Begriffe und zeigt dabei den Unterschied zwischen der Informationssicherheit (Schutz von Informationen) und Datensicherheit (Schutz der Daten) auf. Diese Definition ist somit genauer als die der ISO/IEC 27000:2016(en), die Standards im Bereich IT definiert. Hier ist IT-Sicherheit definiert als die Sicherstellung folgender drei Eigenschaften:

- Vertraulichkeit (confidentiality)
- Integrität (integrity)
- Verfügbarkeit (availability) (vgl. ISO/IEC 27000:2016(en))

Diese Eigenschaften nennt Easttom (2016) auch das ‚CIA triangle', wobei CIA als Akronym für deren englische Bezeichnungen Confidentiality, Integrity und Availability steht. Diese drei Prinzipien sollten in Bezug auf die IT-Sicherheit jederzeit bedacht werden. Zusätzlich können vier weitere Prinzipien für IT-Sicherheit festgelegt werden:

- Authentizität (authenticity)
- Verrechenbarkeit (accountability)
- Verbindlichkeit (non-repudiation)
- Zuverlässigkeit (reliability) (vgl. ISO/IEC 27000:2016(en))

Diese „Dreifaltigkeit der IT-Sicherheit" (Schneider, 2017), bestehend aus Vertraulichkeit, Integrität und Verfügbarkeit, kann als Grundsatz der IT-Sicherheit betrachtet werden. Die drei Prinzipien sollten dabei immer den gleichen Stellenwert haben (vgl. Schneider, 2017).

2.3.2 Grundsätze der IT-Sicherheit

Die im letzten Abschnitt genannten Grundsätze der IT-Sicherheit sollen in diesem Kapitel näher betrachtet werden. So wird unter Vertraulichkeit in der IT-Sicherheit die Vermeidung eines unautorisierten Zugriffs auf Informationen verstanden. Es muss gewährleistet sein, dass Informationen nur bei erteilter Berechtigung abgefragt werden dürfen. In IT-Systemen wird dies durch die Festlegung von Berechtigungen und Zugriffsrechten sichergestellt. Speziell bei ERP-Systemen muss dies sichergestellt werden, da die Angestellten im Unternehmen beispielsweise keine Einsicht in die Daten der Finanzbuchhaltung haben sollen (vgl. Eckert, 2013).

Eckert (2013) spricht auch bei Datenbanksystemen von Vertraulichkeit. Hier kann es möglich sein, dass einzelne Personendaten abgefragt werden, während die Anonymität der Personen aber dennoch gewährleistet bleiben muss. Vor allem die Verhinderung eines Reverse Engineerings, mittels dem anhand von Informationen auf eine Person zurückgeschlossen werden kann, stellt eine Herausforderung dar.

Anders als bei der Vertraulichkeit, geht es bei der Integrität, um ein anderes Prinzip, das Gadatsch und Mangiapane (2017) folgendermaßen definieren:

> *„Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf ‚Daten' angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf ‚Informationen' angewendet. Der Begriff ‚Information' wird dabei für ‚Daten' verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden." (Gadatsch & Mangiapane, 2017)*

An dieser Stelle soll auch auf die Wissenstreppe (siehe Abbildung 2-8) nach North, Brandner und Steininger (2016) verwiesen werden, die den Zusammenhang zwischen Daten und Information näher erläutert. Wie bereits Gadatsch und Mangiapane (2017) schreiben, werden durch das Herstellen von Zusammenhängen zwischen Daten Informationen erzeugt. Die Wissenstreppe nach North et al. (2016) zeigt in Treppenform, wie die einzelnen Stufen zusammenhängen. Die unterste Stufe stellt die Zeichen dar, die durch eine Syntax zu Daten werden. Nachdem im bereits genannten Schritt Daten zu Informationen wurden, wird durch das Hinzufügen einer Bedeutung Wissen generiert. Auf dieser Stufe ist Vorsicht geboten, da die Bedeutung von Informationen je nach Interpretation zu einem anderen Wissen führt. Besonders die kulturellen Kontexte sind laut North et al. (2016) bei diesem Phänomen zu beachten. Die letzte Stufe dieser Treppe stellt das Handeln dar, das durch Wissen in Kombination mit Vernetzung entsteht.

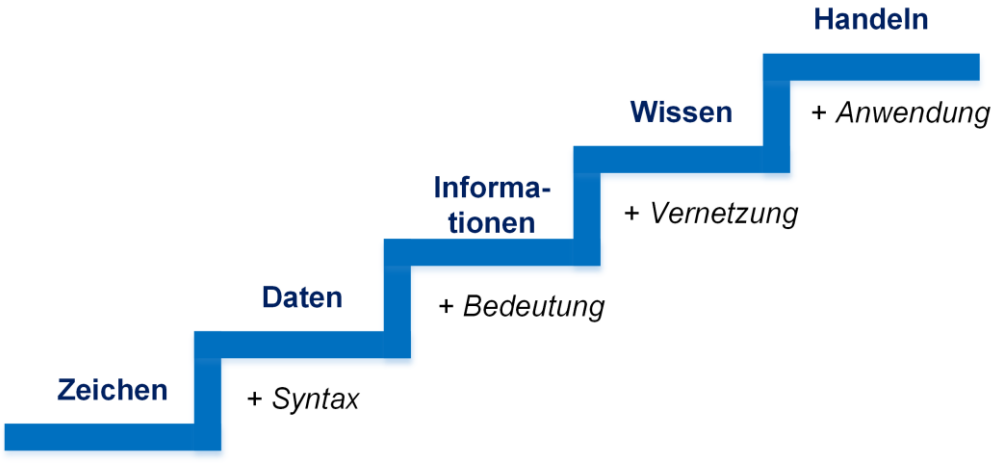


Abbildung 2-8 Wissenstreppe (North et al., 2016)

Um nun Integrität sicherzustellen, müssen Maßnahmen festgelegt werden, die dafür sorgen, dass Daten, Informationen und Funktionen während des Informationsverarbeitungsprozesses weder verändert werden können noch Schaden davontragen. Grundsätzlich kann nicht verhindert werden, dass es zu Datenänderungen kommt, es besteht jedoch die Möglichkeit, mithilfe bestimmter Sicherheitsmechanismen wie zum Beispiel Prüfsummen oder Sequenznummern,

festzustellen, ob eine Änderung vorgenommen wurde. So lässt sich feststellen, ob die Daten am Ende des Prozesses in ihrer ursprünglichen Form vorliegen (vgl. Gadatsch & Mangiapane, 2017).

In Bezug auf die Verfügbarkeit muss sichergestellt sein, dass ein IT-System genutzt werden kann, wenn eine Benutzerin oder ein Benutzer das möchte. Bei der Verfügbarkeit hat dabei vor allem der wirtschaftliche Aspekt Bedeutung. IT-Systeme in Produktionsunternehmen, die 24 Stunden am Tag und 7 Tage die Woche produzieren, müssen eine Verfügbarkeit nahe der 100 % gewährleisten, um wirtschaftliche Schäden zu verhindern. Eine mögliche Lösung dafür ist die Sicherstellung von Redundanzen, sodass im Falle eines Ausfalls ein zweites System sofort die Aufgaben des ersten übernehmen kann (vgl. Gadatsch & Mangiapane, 2017).

Zusammengefasst heißt das, dass ein IT-System jederzeit erreichbar sein sollte, der Zugriff auf die Daten geregelt ist und eine Datenänderung verhindert werden muss. In Tabelle 2-3 sollen zum besseren Verständnis Negativbeispiele für jedes dieser Prinzipien aufgezeigt werden.

Prinzip	**Beispiel**
Vertraulichkeit	Eine Bank verliert eine CD mit Kontodaten von Kunden.
Integrität	Falsche Noten werden an Studenten geschickt (vgl. Gadatsch & Mangiapane, 2017).
Verfügbarkeit	Ein Online-Shop fällt zur Weihnachtszeit mehrere Tage aus.

Tabelle 2-3 Beispiele für mangelnde IT-Sicherheit

Da die Prinzipien der Authentizität, Verrechenbarkeit, Verbindlichkeit und Zuverlässigkeit nur eine Erweiterung der Grundsätze darstellen, werden diese nicht im Detail betrachtet. Der Vollständigkeit halber sollen sie aber kurz vorgestellt werden.

Authentizität ist ein Teil der Integrität und stellt sicher, dass die Absenderin oder der Absender und die Empfängerin oder der Empfänger echt und somit die Person ist, die sie vorgibt zu sein. Bei der Verrechenbarkeit geht es darum, dass einzelne Personen spezifische Verantwortlichkeiten für die Informationssicherheit haben sollen. Die Verbindlichkeit sorgt dafür, dass Aktionen und Ereignisse verpflichtend sind. Dies ist beispielsweise im E-Commerce ein Problem, da die Frage beantwortet werden muss, ob eine Bestellung über das Internet in dieser Form rechtlich gültig ist oder nicht. Das letzte Prinzip, die Zuverlässigkeit, beschreibt, dass das IT-System gewährleisten muss, dass dessen Verhalten und Funktionen korrekt arbeiten (vgl. Gadatsch & Mangiapane, 2017).

Wie bereits in vorigen Abschnitten angesprochen, können nicht alle Unternehmen ihre Daten auf beliebige Server legen. Dies hat den Hintergrund, dass neben den Grundsätzen der IT-Sicherheit vor allem gesetzliche Regelungen, Vorschriften und Normen erfüllt werden müssen.

2.3.3 Gesetze, Verordnungen und Normen

Grundsätzlich muss die IT-Sicherheit durch den Einsatz geeigneter Technik sichergestellt werden, um so einer möglichen Sicherheitslücke bereits im Vorfeld entgegenzuwirken. Dem Rechtssystem ist es dabei kaum möglich, unmittelbar den neuesten Stand der Technik abzubilden und damit echte Schutzmechanismen gegenüber potentiellen Angreifern zu bieten. Aus diesem Grund greift das Recht anders in die IT-Sicherheit ein: Es schreibt den Unternehmen vor, wie es mit sensiblen Daten, wenn diese zum Beispiel personenbezogenen sind, umgehen soll. Das Rechtsystem beschäftigt sich dabei gerade in Zeiten der Digitalisierung zunehmend mit Themen der IT-Sicherheit (vgl. Brisch, 2017).

Im europäischen Raum gibt es darum die Richtlinie 95/46/EG des europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr eine Grundlage für nationale Datenschutzgesetze (vgl. Österreichische Datenschutzbehörde, 2017). Diese Richtlinie, auch Datenschutzrichtlinie genannt, findet „auf automatisch verarbeitete Daten (beispielsweise in einer Kundendatenbank) sowie auf Daten Anwendung, die in einer nicht automatisierten Datei enthalten sind oder für eine solche Datei bestimmt sind (herkömmliche papiergestützte Dateien)“ (Das europäische Parlament und der Rat der europäischen Union, 1995).

Inhaltlich berücksichtigt diese Richtlinie folgende Punkte:

- Rechtmäßige Verarbeitung von Daten
- Grundsätze der Qualität der Daten
- Rechte von Personen, deren Daten verarbeitet werden
- Einschränkungen von Personen, deren Daten verarbeitet werden
- Vertrauliche und sichere Datenverarbeitung
- Meldepflicht
- Übermittlung personenbezogener Daten (vgl. Das europäische Parlament und der Rat der europäischen Union, 1995)

Auf diese Datenschutzrichtlinie soll im weiteren Verlauf nicht näher eingegangen werden, da die Datenschutzrichtlinie die IT-Situation in den 1990er-Jahren widerspiegelt und in Zeiten von sozialen Netzwerken und der Digitalisierung als veraltet angesehen wird. Aus diesem Grund wurde die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG verabschiedet. Diese Verordnung, auch Datenschutz-Grundverordnung (DSGVO) genannt, setzt sich mit der Digitalisierung des 21. Jahrhunderts auseinander und tritt am 25. Mai 2018 in Kraft (vgl. Österreichische Datenschutzbehörde, 2017).

Die DSGVO vereinheitlicht über die gesamte europäische Union (EU) hinweg die Regeln für die Verarbeitung von Informationen. Als Verordnung sorgt sie für eine unmittelbare Wirkung in den Mitgliedsstaaten, kann aber durch nationale Gesetze begleitet werden (vgl. Duzdar, 2016). Dies

liegt unter anderem an zahlreichen Öffnungsklauseln, die den Mitgliedsstaaten Freiräume verschaffen. In Österreich wurde darum das ‚Datenschutz-Anpassungsgesetz 2018' beschlossen (vgl. Wirtschaftskammer Österreich, 2017).

Als Neuerung in der DSGVO ist beispielsweise der Entfall der Meldepflicht, unter anderem. bei einem Hackerangriff mit Datenverlust, enthalten, wodurch das Unternehmen sich nicht mehr bei der Datenschutzbehörde melden muss. Um der entfallenen Meldepflicht entgegenzuwirken, wird den Unternehmen mehr Verantwortung übertragen (vgl. Wirtschaftskammer Österreich, 2017):

- Dauerhafte Sicherstellung von Integrität, Vertraulichkeit und Verfügbarkeit
- Übersicht über die Datenverarbeitung, vor allem wenn Daten in ein Drittland übermittelt werden
- Einsetzen eines Datenschutzbeauftragten
- Erweiterte Informationspflicht gegenüber Betroffenen bei einer Datenschutzverletzung
- Hohe Strafen bei Nichteinhaltung (vgl. Wirtschaftskammer Österreich, 2017)

Bei Betrachtung dieser Gesetze und Regelungen wird deutlich, dass auch ein ERP-System, das in der Cloud betrieben wird, sich an diese neue Richtlinie zu halten hat. Dafür sind nicht nur die Unternehmen verantwortlich, die das ERP-System verwenden, sondern auch die Cloud-Anbieter, die ihre Cloud auf eine rechtssichere Basis stellen müssen. Neben rechtlichen Themen stellen jedoch auch noch andere Aspekte der IT-Sicherheit ein gewisses Risiko in Hinblick auf ein ERP-System in der Cloud dar.

2.3.4 IT-Sicherheit von ERP-Systemen in der Cloud

Von den Unternehmen wird zunehmend die Verwendung einer Cloud, deren Vorteile in diesem Kapitel bereits erläutert wurden, eingefordert. Priorität dabei hat jedoch weiterhin eine sichere Umgebung für die Daten des Unternehmens, die zusätzlich günstig sein soll. Die Herausforderung dabei besteht darin, dass die Daten nicht von unbefugten Personen gelesen oder gestohlen werden dürfen. Aus diesem Grund ist es für Unternehmen besonders wichtig, den Cloud-Anbieter im Vorfeld genau zu analysieren (vgl. Backofen, 2017). Folgende Fragen sollten dabei gestellt werden:

- Unter welches Recht fällt der Cloud-Anbieter und wo liegen meine Daten?
- Ist der Cloud-Anbieter vertrauenswürdig?
- Bringt die Cloud dem Unternehmen den gewünschten Vorteil?
- Kann der Datenschutz vom Cloud-Anbieter sichergestellt werden? (vgl. Backofen, 2017)

Eine Studie der nationalen Initiative für Informations- und Internet-Sicherheit e.V. (NIFIS) in Deutschland hat beispielsweise festgestellt, dass 87 % der deutschen Unternehmen großen Wert darauf legen, dass ihre Daten nicht von Unternehmen verwaltet werden, die ihre Daten in den USA speichern. Stattdessen werden auch bei Cloud-Lösungen Anbieter aus dem eigenen Land oder der EU bevorzugt. Zusätzlich weisen die Unternehmen darauf hin, dass ein stetes

Bewusstsein darüber bestehen muss, welche Daten einem anderen Unternehmen anvertraut werden (vgl. NIFIS, 2016).

Ein Problem, das sich ergibt wenn die Daten in anderen Ländern liegen, ist die Frage nach dem anwendbaren Recht. Da auch für Daten, die mit einem Drittland ausgetauscht werden, europäisches Recht gelten sollte, wurde im Jahr 2000 das ‚Safe-Harbor-Abkommen' mit den USA abgeschlossen. Als dieses am 06. Oktober 2015 als ungültig erklärt wurde, führte dies zu Unsicherheiten in der Rechtslage. Diese Unsicherheit sollte mit dem ‚Privacy Shield' gelöst werden. Trotz Bedenken hinsichtlich der 2018 eintretenden DSGVO wurde im Juli 2016 von der EU-Kommission festgestellt, dass das Abkommen die Anforderungen erfüllt. Die Cloud-Anbieter wichen nach diesen Vorfällen dennoch auf nationale Rechenzentren aus, um sich rechtlich abzusichern (vgl. Brisch, 2017).

Ein Sicherheitsrisiko, das sowohl bei einem eigenen Rechenzentrum als auch bei einer Cloud-Lösung besteht, ist immer der Mensch. Geht es um die IT-Sicherheit in Hinblick auf die technische Perspektive, so gibt es Möglichkeiten, um ein IT-System gegen Angreiferinnen und Angreifer zu schützen. Zusätzlich können bekannte Fehler in der Zukunft weitestgehend vermieden werden, wenn die Sicherheitslücke sofort geschlossen und nicht wieder geöffnet wird. Die Schwachstelle, die von Angreiferinnen und Angreifern in vielen Fällen ausgenutzt wird, ist aber insbesondere die Person, die durch die Annahme gefälschter E-Mails oder durch Social Engineering den Zugriff auf interne Daten eines Unternehmens ermöglicht (vgl. Neumann, 2017).

Die Frage, ob die Cloud den gewünschten Vorteil für den Betrieb des ERP-Systems bringt, stellen sich vor allem Großunternehmen. Im Gegensatz zu Klein- und Mittelunternehmen (KMU) haben Großunternehmen ausreichend Ressourcen, um das ERP-System auch ohne Cloud zu betreiben. Bei KMU fehlen diese Ressourcen, was dazu führt, dass es keine andere Möglichkeit gibt, als die Sicherheit des ERP-Systems einem Partner, der vertrauenswürdig ist, zu überlassen. Hier ist die Cloud die optimale Lösung zur Erreichung dieses Ziels (vgl. Backofen, 2017).

Damit ein ausreichender Schutz der Daten gewährleistet werden kann, ist es möglich, nicht nur die Verbindung in die Cloud, sondern auch die Daten selbst zu verschlüsseln. Dies führt dazu, dass nur Personen, die den entsprechenden Schlüssel besitzen, die Daten in ihrer eigentlichen Form lesen können. Bei einem Datenbesitz ohne Schlüssel ist es nicht möglich, auf die wahren Daten zuzugreifen. Hier kann lediglich versucht werden, durch Probieren den Schlüssel zu erraten (vgl. Prabhu & Paramesha, 2017).

2.4 Zusammenfassung

Die Theorie zeigt, dass die Cloud trotz ihrer Popularität im Privatleben bisher nur von wenigen Unternehmen, speziell für ERP-Systeme, genutzt wird. Durch eine Vielzahl an Möglichkeiten, die Cloud zu betreiben, werden zwar Optionen geschaffen, die zur Verwirklichung der Ansprüche an ein sicheres ERP-System beitragen können, jedoch äußern die Unternehmen weiterhin Bedenken dahingehend, dass die Cloud für das jeweilige ERP-System noch immer zu unsicher ist.

Insbesondere für KMU, die oftmals keine Ressourcen zum adäquaten Schutz ihres eigenen Unternehmensnetzwerkes zur Verfügung haben, bietet die Cloud eine optimale Lösung. Durch eine hohe Verfügbarkeit und einem nutzungsbasierten Abrechnungsmodell, können sich auch KMU eine sichere Umgebung in der Cloud schaffen. Großunternehmen, die genügend Ressourcen zur Verfügung haben, sehen hingegen keinen Grund, das ERP-System umzustellen und den Betrieb in die Cloud zu verlagern.

Trotz aller Vorteile haben Unternehmen Bedenken hinsichtlich der IT-Sicherheit, die bisher jedoch nicht konkret formuliert werden. Zu diesem Zweck bedarf es einer tiefergehenden Forschung, die herausfindet, welche Bedenken Unternehmen konkret gegenüber der Cloud äußern. Erst wenn diese Bedenken erforscht sind ist es möglich, diese im Folgeschritt zu vermindern. Zu diesem Zweck wird im nächsten Kapitel daher die dazu in dieser Arbeit durchgeführte Forschung vorgestellt.

3 EMPIRIE

Innerhalb der empirischen Sozialforschung werden Techniken und Methoden zur systematischen Wissensgewinnung eingesetzt. Dabei wird versucht, das Handeln der Menschen und soziale Begebenheiten zu erklären (vgl. Weischer, 2007). Mit der empirischen Sozialforschung ist außerdem ein Vergleich zwischen der Praxis und der Theorie möglich. Während die Praxis über Beobachtungen und Erfahrungen versucht Informationen zu gewinnen, bekommt die Theorie diese auf Basis von abstrakten Auseinandersetzungen mit der Hilfe einer anschließenden Reflexion (vgl. Schirmer & Blinkert, 2009).

Dieses Kapitel dient zur näheren Darstellung der Empirie dieser Arbeit und behandelt dabei unter anderem die bereits erwähnten Punkte der Datenerhebung und -analyse. Am Beginn der Forschung steht immer die Wahl der geeigneten Methode.

3.1 Methoden

Die Methode ist ein Bestandteil der empirischen Sozialforschung und dient der Gewinnung von Erkenntnissen durch geeignete Handlungen, die gewissen Regeln folgen. Die empirische Sozialforschung ist dabei nicht an bestimmte Inhalte gebunden, sondern kann sowohl für Untersuchungen im Mittelalter als auch bei Themen aus dem aktuellen Jahrtausend angewendet werden. Diese Anwendungsvielfalt wird darauf begründet, dass die empirische Sozialforschung zwar gewissen Grundregeln folgt, deren Inhalte aber gänzlich unterschiedlich sein können Dasselbe gilt auch für die Methoden, die im Zuge der empirischen Sozialforschung angewendet werden. Diese besitzen meist nur einen formalen Charakter, der sich beispielsweise bei der Auswahl der Testpersonen zeigt. So ist es egal, ob eine Zufallsauswahl getroffen wird oder ob Personen im Rahmen einer Wahlstudie befragt werden. In beiden Fälle muss im Vorfeld überlegt werden, wie hoch zum Beispiel die Irrtumswahrscheinlichkeit oder die Fehlerquote sein kann (vgl. Häder, 2015).

Neben dieser Überlegung ist ein weiterer Gedanke wichtig: Die Methoden entstammen oftmals dem täglichen Leben, was laut Häder nicht verwundert, da die Methoden der empirischen Sozialforschung aus eben diesen Informationen gewinnen soll.

Geht es um die konkrete Umsetzung der Methode, so wird von deren Technik gesprochen. Ein Beispiel dafür sind Personenbefragungen, die auf mehrere Arten durchgeführt werden können. Aufgrund der unterschiedlichen Arten der Befragung wird von derselben Methode, aber von unterschiedlichen Techniken gesprochen. Bei einer Befragung stellen beispielsweise das persönliche Interview und ein ausgesendeter Fragebogen zwei verschiedene Techniken für dieselbe Methode dar (vgl. Häder, 2015).

In der empirischen Sozialforschung hat sich außerdem die Unterteilung in quantitative und qualitative Methoden etabliert. Trotz aufkommender Kritik an dieser Unterteilung ist diese noch fest verankert und dient auch heute noch als Basis von wissenschaftlichen Arbeiten (vgl. Schirmer & Blinkert, 2009).

3.2 Qualitative Sozialforschung

Bei quantitativen Methoden geht es grundsätzlich um das Zählen und Messbarmachen von quantitativen Merkmalen. Die qualitativen Methoden hingegen beschäftigen sich mit der Analyse von Sprache und Text. Obwohl quantitative Verfahren, wie zum Beispiel bei Erhebungen durch einen Fragebogen oder Interviewverfahren, ebenfalls auf Sprache und Text beruhen, ist es das Ziel der quantitativen Methode, diese Daten in numerische Daten zu verwandeln. Im Anschluss daran erfolgt mit der Hilfe von Statistik eine Auswertung, die der Informationsgewinnung dient (vgl. Schirmer & Blinkert, 2009).

Ein weiterer Unterschied zwischen den beiden Methoden ist, dass die quantitative größere Stichproben als die qualitative Forschung behandelt. Dieser Unterschied beruht auf der Tatsache, dass die quantitative Forschung dazu dient, Hypothesen über neue Sachverhalte zu bestätigen, die qualitative Forschung hingegen theoretische Aussagen aufgrund von Entdeckungen herausfinden will (vgl. Brüsemeister, 2008). Dieser Unterschied bildet den Kern der Unterscheidung beider Methoden:

> *„Eine Entdeckung ist zum Beispiel schon anhand eines einzigen Interviews, einer Beobachtung oder eines Dokuments möglich. Um Wissenschaften mit qualitativen Methoden auf neue Spuren zu bringen, spielt also die Fallzahl eine erheblich geringere Bedeutung als in quantitativen Methoden[...]. Umgekehrt die „überprüfende" Logik quantitativer Forschungen. Sie verlangt nach signifikant messbaren Mengen, die eine zu überprüfende Hypothese widerlegen oder bestätigen können. Nicht wie der einzelne Fall einen Sachverhalt einschätzt, sondern ob große oder kleine Prozentanteile ganzer Populationen dies tun, interessiert. Eine solche Messung übernehmen quantitative Ansätze."* (Brüsemeister, 2008)

Im Zentrum der qualitativen Sozialforschung steht, anstatt der Auswertung von numerischen Daten wie bei den quantitativen Methoden, das Interesse an inneren Mechanismen und Handlungen von Personen (vgl. Brüsemeister, 2008). Nach Lamnek und Krell (2010) sind Menschen, die mit qualitativen Forschungsmethoden untersucht werden, anders als bei der quantitativen Sozialforschung, nicht als Untersuchungsobjekt, sondern als erkennendes Subjekt tätig. Der Mensch hat Erwartungen und muss je nach Kontext das Handeln beurteilen und interpretieren. Die Merkmale qualitativer Forschung werden daher wie folgt definiert:

- Interpretativ
- Naturalistisch
- Kommunikativ
- Reflexiv
- Qualitativ (vgl. Lamnek & Krell, 2010)

Einen weiteren Unterschied zwischen den Forschungsmethoden bildet die Vorgehensweise. Während die quantitative Sozialforschung sich an deduktiven Prinzipien orientiert, bildet die Induktion die Basis für die qualitative Sozialforschung und somit auch für diese Arbeit. Unter

Induktion wird dabei der Schluss von etwas Besonderem auf die Allgemeinheit verstanden (vgl. Endruweit, 2015). Dies deckt sich mit den Aussagen über die Stichprobengröße bei der qualitativen Forschung. Diese verfolgt zudem eine zirkuläre Strategie. Das heißt, dass es, anders als bei der quantitativen Forschung, keinen starren Plan gibt, der von Anfang bis Ende durchgeführt wird. Diese Strategie ermöglicht es dem Forschenden, die Methode anzupassen, wenn dies vonnöten ist (vgl. Lamnek & Krell, 2010).

Für die vorliegende Arbeit wird eine qualitative Methode gewählt, mit deren Hilfe die Bedenken im Bereich IT-Sicherheit gegenüber eines ERP-Systems in der Cloud herausgefunden werden sollen. Dieses Vorgehen soll Erkenntnisse darüber ermöglichen, warum der Cloud misstraut wird. Dank des in Abbildung 3-1 dargestellten qualitativen Vorgehens ist es möglich, die wichtigsten Beweggründe zu erforschen und in weiterer Folge zu verarbeiten. Die von Lamnek und Krell (2010) vorgestellten Schritte dienen gleichzeitig zur Unterteilung dieses Kapitels.

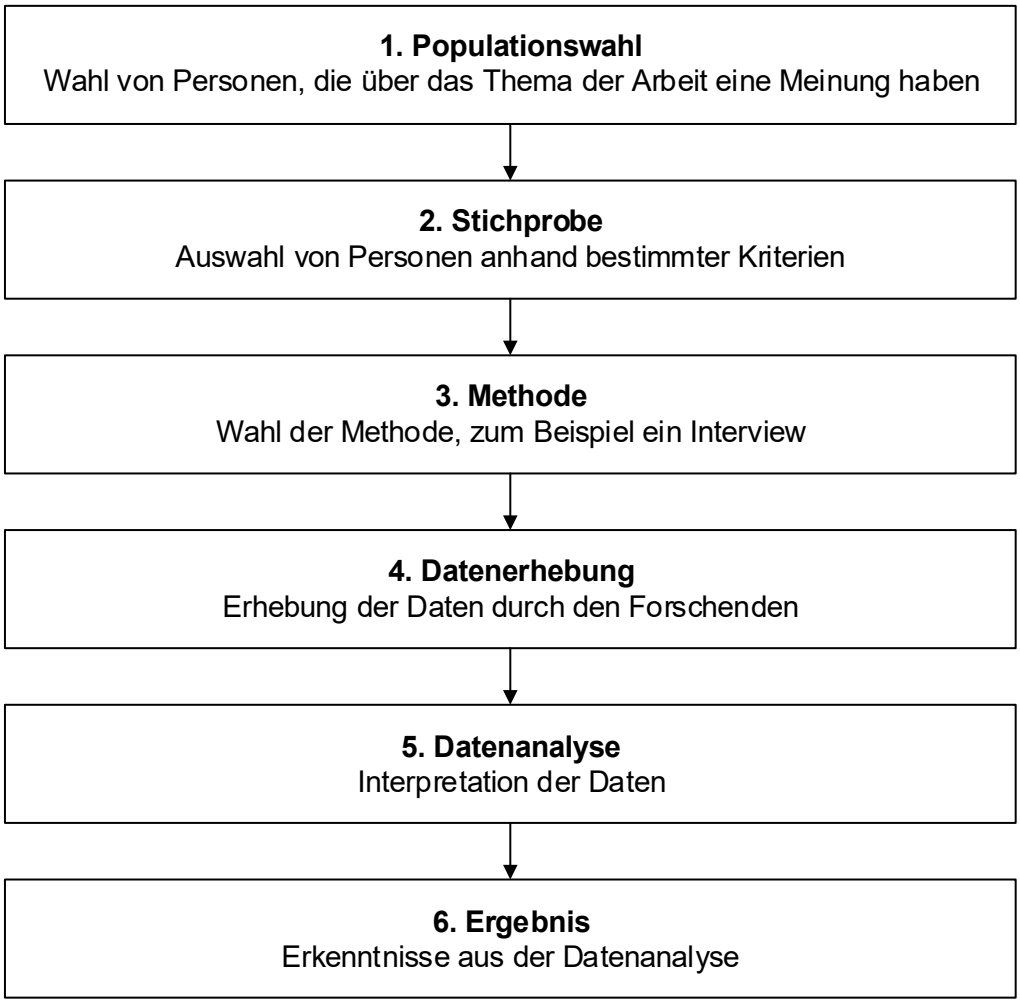


Abbildung 3-1 Vorgehen in der qualitativen Forschung (Lamnek & Krell, 2010)

Neben den genannten Gründen spricht noch ein weiterer Aspekt für die Wahl einer qualitativen Erhebungsmethode. Diesen weiteren und weitaus wichtigeren Grund nennt Matros (2012) :

> *„Gerade beim Cloud Computing bestehen keine scharfen Begriffsabgrenzungen, wodurch die Entwicklung eines standardisierten Fragebogens erheblich erschwert wird bzw. unmöglich erscheint. Ein ähnliches Problem ist im unterschiedlichen*

> *Wissensstand der Adressaten zu sehen, der gerade bei neuen Konzepten wie Cloud Computing besonders ausgeprägt ist. Bei Verwendung von standardisierten Methoden ohne persönliche Interaktion besteht die Gefahr der Scheinobjektivität.“* (Matros, 2012)

3.3 Stichprobenbeschreibung

Wie zu Beginn des Kapitels bereits erwähnt, arbeitet die qualitative Sozialforschung mit kleinen Stichproben. Um dem wissenschaftlichen Kriterium der Repräsentativität zu genügen, arbeitet sie mit dem Prinzip der Sättigung. Dies bedeutet, dass so lange Personen befragt werden, bis eine weitere Person keine neuen Erkenntnisse mehr bringt. Wann dieser Zeitpunkt eintritt, hängt vom konkreten Fall ab und kann nur ungefähr bestimmt werden (vgl. Brüsemeister, 2008).

Die Anzahl der Untersuchungspersonen wirkt sich direkt auf die Analyse aus. Je weniger Personen in der Stichprobe enthalten sind, desto genauer sollte das Auswertungsverfahren gestaltet sein. Die ungefähre Stichprobengröße beginnt bei sechs Personen und kann bis auf 120 Teilnehmerinnen und Teilnehmer ansteigen. Durch Randbedingungen, wie sie vor allem bei Abschlussarbeiten herrschen, ist Zeit eine der Ressourcen, die am öftesten fehlt. Vor allem die Zeit, die für die Transkription und Interpretation aufgewendet werden muss, spielt eine große Rolle (vgl. Helfferich, 2009). Dies zeigt sich in weitere Folge auch durch die Wahl der Stichprobe für diese Arbeit.

Die Methoden in der qualitativen Sozialforschung unterliegen trotz der Offenheit und Flexibilität bestimmten Regeln. Bezogen auf die Stichprobe betrifft das unter anderem die theoretischen Vorkenntnisse der befragten Personen. Besitzen diese vom erforschten Gebiet keine Kenntnisse, so wird die erfolgreiche, repräsentative Informationsgewinnung nahezu unmöglich. Die Forscherin oder der Forscher muss somit eine klare Vorstellung davon haben, wie die Personen aus der Stichprobe aussehen sollen (vgl. Lamnek & Krell, 2010).

Um den Anforderungen der Befragung im Rahmen dieser Arbeit zu genügen, muss eine Person daher folgende Voraussetzungen erfüllen:

- Betreuung oder Anwendung eines ERP-Systems
- Kenntnisse im Bereich IT-Sicherheit
- Kenntnisse im Bereich Cloud-Computing

Stellt sich im Zuge der Befragung heraus, dass eine der Voraussetzungen nicht erfüllt wird, so ist die befragte Person für die Datenauswertung nicht weiter zu berücksichtigen. Eine Übersicht über die Interviewpartner kann Tabelle 3-1 entnommen werden. Wie die Spalten neben dem Interviewpartner zustande kommen, soll im nächsten Abschnitt näher erklärt werden.

Interviewpartner	**Unternehmensgröße**	**Position**
Interviewpartner 1	Großunternehmen	IT-Mitarbeiter

Interviewpartner 2	Großunternehmen	IT-Mitarbeiter
Interviewpartner 3	Großunternehmen	IT-Leiter
Interviewpartner 4	KMU	IT-Leiter
Interviewpartner 5	KMU	IT-Mitarbeiter
Interviewpartner 6	Großunternehmen	IT-Leiter

Tabelle 3-1 Interviewpartner

Da sich nicht alle Personen mit der Veröffentlichung ihrer Daten einverstanden erklärt haben, wurden die Teilnehmerinnen und Teilnehmer anonymisiert. Jedoch handelte es bei allen Befragten um Männer, daher wird in weiterer Folge nur von Interviewpartnern gesprochen.

3.4 Methodenwahl

Die am häufigsten verwendete Art der Datenerhebung in der qualitativen Sozialforschung ist das Leitfadeninterview (vgl. Kleemann, Krähnke & Matuschek, 2013). Was ein Leitfadeninterview ist und wodurch es sich von einer quantitativen Methode unterscheidet, erklären Kleemann et al. (2013):

> *„Leitfadeninterviews sind dadurch gekennzeichnet, dass der Interviewer eine Reihe von vorab festgelegten (und im Leitfaden in Form von thematischen Aspekten oder konkreten Fragen niedergeschriebenen) Themenbereichen anspricht. Durch gezielte Fragen werden neue Gesprächsimpulse für den Probanden gesetzt. Allerdings werden die Fragen und Antwortmöglichkeiten nicht standardisiert vorgegeben wie bei der quantitativen Datenerhebung mittels Fragebogen. Oftmals benutzt der Interviewer lediglich Stichpunkte und der Leitfaden wird als eine flexible Checkliste gehandhabt. Selbst die Reihenfolge der Fragestellungen ist nicht zwingend vorgeschrieben.“* (Kleemann et al., 2013)

Durch diese Art der Befragung wird es der Interviewpartnerin oder dem Interviewpartner möglich, ein offenes Gespräch zu führen, in dem sie oder er seine Meinung ohne strikt festgelegten Fragenkatalog kundtun kann. Die Folge davon ist, dass einzelne Aspekte detaillierter besprochen und neue Blickwinkel auf das Thema eröffnet werden können (vgl. Kleemann et al., 2013).

Leitfadeninterviews haben zusätzlich den Vorteil, dass sie die Befragung auf Basis einer gewissen Struktur abwickeln, was dazu führt, dass die Auswertung der Befragungen erleichtert wird (vgl. Helfferich, 2009). An das Leitfadeninterview werden dennoch folgende Anforderungen gestellt:

- Erfüllung der Prinzipien der qualitativen Sozialforschung, speziell der Offenheit

- Beschränkung auf wenige Fragen, sodass es nicht in zu vielen Punkten zu sehr ins Detail geht
- Ermöglichen eines Erzählflusses ohne Sprünge
- Offenes Gespräch, ohne dabei die Fragen des Leitfadens abzulesen
- Konzentration auf das spontane Gespräch (vgl. Helfferich, 2009)

Unter Einhaltung aller genannten Kriterien wurde der hier verwendete Leitfaden für die Interviews erstellt. Dank den Erkenntnissen von Matros (2012) wurde bei der Erstellung darauf geachtet, dass Fragen eingebaut werden, die das Wissen der Interviewpartner über die Cloud testen. Die Fragen des Leitfadens stützen sich auf den theoretischen Teil der Arbeit, wodurch der Bezug zur Forschungsfrage herstellt wird.

Um die befragten Personen vergleichen zu können, wurden im Vorfeld Unterscheidungskriterien festgelegt:

- Unternehmensgröße
- Position im Unternehmen

Der Interviewleitfaden besteht aus offenen Fragen, die zum Erzählen einladen sollen. Im Vordergrund steht, wie bereits bekannt, nicht die systematische Abarbeitung der Fragen. Der gesamte Interviewleitfaden, inklusive der geschlossenen Fragen, kann dem Anhang entnommen werden. Nachdem der Leitfaden erstellt wurde und die Stichprobe festgelegt ist, kann mit der Erhebung der Daten begonnen werden.

3.5 Datenerhebung

Im ersten Schritt wurde ein Kontakt mit potentiellen Interviewpartnerinnen und Interviewpartnern hergestellt. Dieser erfolgte entweder per E-Mail oder über einen direkten Anruf, abhängig von den bekannten Kontaktinformationen. Im Zuge dieser ersten Kontaktaufnahme wurde gefragt, ob Interesse an der Teilnahme eines Interviews zum Thema dieser Masterarbeit besteht. Von sieben angefragten Personen konnten sechs für ein Interview gewonnen werden. Somit gaben ca. 85 % der angefragten Personen eine positive Rückmeldung.

Die Wahl, ob das Interview persönlich oder per Telefon stattfinden soll, wurde den Personen selbst überlassen. Selbiges trifft auch auf den Ort zu, der bei den persönlich stattfindenden Interviews festgelegt werden musste. Lamnek und Krell (2010) sind der Meinung, dass der Befragungsort eine wichtige Rolle spielt, da sich die Interviewpartnerin oder der Interviewpartner wohlfühlen sollte, um frei sprechen zu können. Personen, die nicht im näheren Umfeld von Graz oder Graz-Umgebung beheimatet waren, wurden seitens des Autors jedoch um ein telefonisches Interview gebeten, wodurch schlussendlich drei Interviews persönlich und drei per Telefon durchgeführt wurden.

Für die Transkription der Interviews war es notwendig, diese aufzuzeichnen. Aufgrund rechtlicher Vorschriften wird dazu im Vorfeld die Genehmigung der befragten Personen benötigt, die von allen erteilt wurde. Die Aufzeichnung fand bei allen Interviews mit dem Handy statt.

Die Einleitung der Interviews bildete eine kurze Vorstellung des Autors und der vorliegenden Arbeit. Im Anschluss daran wurde das Interview mit Hilfe des Interviewleitfadens durchgeführt. Der Leitfaden stellte dabei einen generellen Rahmen dar, der der thematischen Orientierung diente. Die Gefahr, dass bei dem eher lockeren Gespräch die Interviewpartnerin oder der Interviewpartner nicht mehr im Rahmen des Themas bleibt, sollte so minimiert werden. Trotzdem wurde darauf geachtet, dass die interviewte Person das Gespräch aktiv gestaltet, damit diese ihre Ansichten und Meinungen bestmöglich präsentieren konnte (vgl. Lamnek & Krell, 2010).

Neben den bereits erwähnten Regeln, wurden im Zuge des Interviews noch weitere Hinweise beachtet:

- Die Forschungsfrage sollte nicht direkt gestellt werden
- Es sollte eine lockere Atmosphäre herrschen, die zum Reden einlädt
- Die interviewte Person soll sich jederzeit als Expertin oder Experte fühlen (vgl. Helfferich, 2009)
- Natürlichkeit der Sprache, sodass diese dem Gegenüber angepasst ist (vgl. Lamnek & Krell, 2010)
- Flexibilität bei der Reihenfolge der Fragen
- Stellen einer Abschlussfrage (vgl. Helfferich, 2009)

Nach der Datenerhebung mussten diese in weiterer Folge ausgewertet werden (siehe 3.2 Qualitative Sozialforschung). Die qualitative Sozialforschung beinhaltet mehrere Methoden zur Analyse der Daten.

3.6 Datenauswertung

Eine Methode für die Auswertung von Daten ist die qualitative Inhaltsanalyse nach Philip Mayring, die im deutschen Sprachraum vorwiegend verwendet wird (vgl. Schnell, Schulz, Kolbe & Dunger, 2013). Die qualitative Inhaltsanalyse arbeitet dabei mit Material, das zuvor protokolliert wurde und in textueller Form vorliegt. Nach der Sichtung des Materials werden die Daten interpretiert, was viele Freiheiten zulässt und somit auch den größten Kritikpunkt darstellt. Dass die qualitative Inhaltsanalyse dennoch wissenschaftlichen Kriterien entspricht, soll im nächsten Kapitel im Detail besprochen werden (vgl. Mayring, 2010).

4 INHALTSANALYSE

Nach der erfolgten Datenerhebung, widmet sich dieses Kapitel der Auswertung. Die Auswertung soll mit Hilfe einer qualitativen Inhaltsanalyse nach Mayring (2010) vorgenommen werden. Das Ziel der Inhaltsanalyse ist es, die Bedenken, die hinsichtlich der IT-Sicherheit gegenüber ERP-Systemen in der Cloud geäußert wurden, herauszufinden und am Ende der Analyse darstellen zu können. Zu Beginn gibt dieses Kapitel eine Übersicht über die qualitative Inhaltsanalyse, bevor diese anschließend Schritt für Schritt durchgeführt wird.

4.1 Einführung in die qualitative Inhaltsanalyse

Die qualitative Inhaltsanalyse arbeitet mit Texten und Bildern, was bedeutet, dass das Material in einer protokollierten Form vorliegen muss. In dieser Arbeit wird die Grundlage durch die transkribierten Interviews gebildet, die im Anschluss systematisch ausgewertet und analysiert werden. Dieses Vorgehen ermöglicht die Verwendung einer nachvollziehbaren Methode, die auch für andere Personen überprüfbar wird (vgl. Mayring, 2010).

Die qualitative Inhaltsanalyse versucht da anzusetzen, wo auch die quantitative Inhaltsanalyse ihre Stärken hat. Die qualitative Inhaltsanalyse will dabei das Material analysieren, sowie regel- und theoriegeleitet vorgehen, um Rückschlüsse auf die Kommunikation ziehen zu können. Die Durchführung der Analyse erfolgt dabei mit der Hilfe geeigneter Techniken, von denen eine Auswahl im Folgenden kurz vorgestellt werden soll (vgl .Mayring, 2010).

Einbettung des Materials in den Kommunikationszusammenhang: Die Analyse des Materials steht immer in einem Kommunikationszusammenhang. Das bedeutet, dass im Zuge der Analyse angegeben werden muss, auf welchen Teil des Materials sich die Schlussfolgerungen beziehen (vgl. Mayring, 2010).

Systematisches, regelgeleitetes Vorgehen: Trotz einiger Freiheiten folgt die qualitative Inhaltsanalyse bestimmten Regeln, was in diesem Fall bedeutet, dass vorab Regeln für die Analyse des Materials festgelegt werden müssen. Dennoch muss die Inhaltsanalyse von Fall zu Fall an den Gegenstand angepasst werden und kann nicht auf die exakt gleiche Art und Weise erneut durchgeführt werden. Die wichtigste Regel, die es zu beachten gilt, ist, dass die Inhaltsanalyse so beschrieben werden muss, dass sie auch von einer anderen Person problemlos durchgeführt werden kann (vgl .Mayring, 2010).

Kategorien im Zentrum der Analyse: Kategorien bilden einen zentralen Aspekt der Inhaltsanalyse und stellen somit das Hauptinstrument für das Vorgehen dar. Die Kategorien dienen, ähnlich dem vorigen Punkt, zur besseren Nachvollziehbarkeit für andere Personen (vgl. Mayring, 2010).

Gegenstandsbezug statt Technik: Die letzten Punkte legen die Annahme nahe, dass sich die qualitative Inhaltsanalyse als eine Technik herausgestellt hat, die universell einsetzbar ist. Dem muss jedoch widersprochen werden, da ein zentraler Punkt der Analyse das Interesse am konkreten Fall ist (vgl. Mayring, 2010). „Das zeigt sich daran, dass die vorgestellten

Verfahrensweisen am alltäglichen Umgang mit sprachlichem Material orientiert sind.“ (Mayring, 2010) Dies lässt sich vor allem an den drei Grundverfahren der Zusammenfassung, Explikation und Strukturierung erkennen, die im Zuge dieses Kapitels noch näher vorgestellt werden sollen (vgl. Mayring, 2010).

Theoriegeleitetheit der Analyse: „Mit Theoriegeleitetheit ist gemeint, dass der Stand der Forschung zum Gegenstand und vergleichbaren Gegenstandsbereichen systematisch bei allen Verfahrensentscheidungen herangezogen wird. Inhaltliche Argumente sollten in der qualitativen Inhaltsanalyse immer Vorrang vor Verfahrensargumenten haben; Validität geht vor Reliabilität.“ (Mayring, 2010)

Gütekriterien: Auch die qualitative Inhaltsanalyse unterliegt bestimmten Gütekriterien. Diese werden gegen Ende des Kapitels vorgestellt, wobei auf jedes einzelne eingegangen wird, um zu prüfen, ob diese Arbeit mit ihrem Vorgehen die Gütekriterien erfüllt oder nicht. Laut Mayring (2010) wird jedoch speziell auf Objektivität, Reliabilität und Validität Wert gelegt.

Neben diesen Techniken folgt die qualitative Inhaltsanalyse drei Grundsätzen:

1. Orientierung am Alltag
2. Übernahme der Perspektive des anderen
3. Möglichkeit der Re-Interpretation des Materials (vgl. Mayring, 2010)

Auf Basis dieser Techniken und Grundsätze definiert Mayring nach der Sichtung des Materials, was in dieser Arbeit durch die Interviews vorliegt, ein Ablaufmodell für die qualitative Inhaltsanalyse: das allgemeine inhaltsanalytische Ablaufmodell.

4.2 Allgemeines inhaltsanalytisches Ablaufmodell

Das allgemeine inhaltsanalytische Ablaufmodell definiert die Reihenfolge an Analyseschritten, die ein systematisches und regelgeleitetes Vorgehen unterstützen. Die Analyseschritte werden im Vorhinein festgelegt und sind somit jederzeit nachvollzieh- und wiederholbar. Das allgemeine inhaltsanalytische Ablaufmodell ist daher die wissenschaftliche Methode, die als Basis für die Auswertung der für diese Arbeit erhobenen Daten genutzt wird. Die Analyseschritte können, angewendet auf den speziellen Forschungsgegenstand, zwar voneinander abweichen, dennoch ist eine Orientierung am allgemeinen Ablaufmodell möglich. Die in dieser Arbeit folgende Inhaltsanalyse orientiert sich an den in Abbildung 4-1 dargestellten Analyseschritten (vgl. Mayring, 2010).

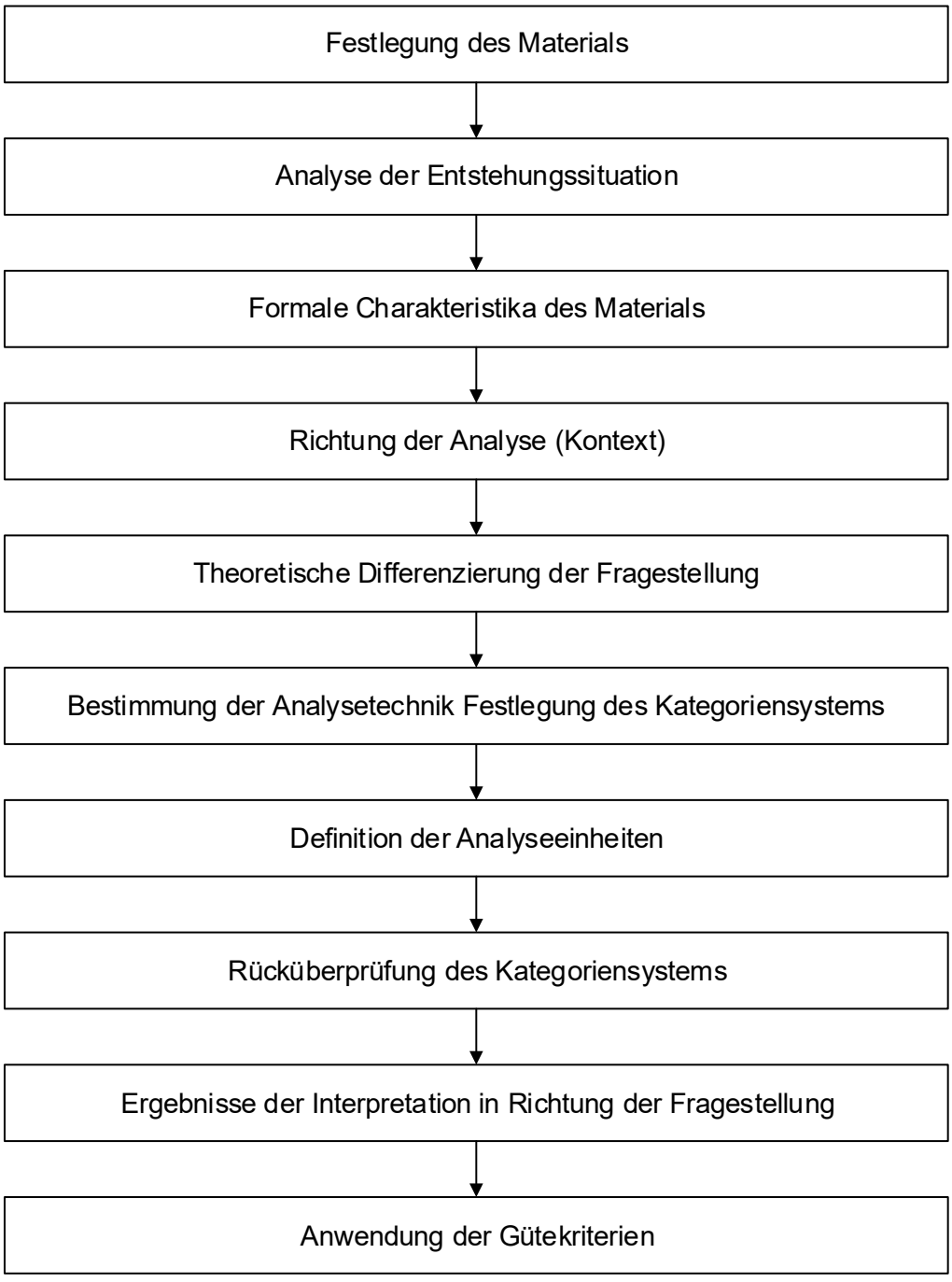


Abbildung 4-1 Ablaufmodell der qualitativen Inhaltsanalyse (Mayring, 2010)

4.3 Inhaltsanalyse nach Mayring (2010)

Die folgende Inhaltsanalyse beruht auf dem allgemeinen inhaltsanalytischen Ablaufmodell nach Mayring (2010), das nun Schritt für Schritt durchgeführt werden soll.

4.3.1 Festlegung des Materials

Der erste Schritt im allgemeinen inhaltsanalytischen Ablaufmodell ist die Festlegung des Materials. Das Material sollte im Zuge der Analyse nicht verändert werden und muss gewisse

Anforderungen erfüllen. Besonderes Augenmerk liegt hierbei auf der Wahl der Stichprobe, deren Umfang sich nach ökonomischen und repräsentativen Gesichtspunkten richtet. Die Stichprobe ist im Vorfeld genau zu definieren, was die Methode zur Wahl der Personen einschließt (vgl. Mayring, 2010).

Das Material dieser Arbeit sind die transkribierten Interviews, die nachträglich nicht mehr geändert und aus einer repräsentativen Stichprobe erstellt wurden. Die Stichprobe wurde bereits im Zuge dieser Arbeit näher vorgestellt und erfüllt die Voraussetzungen, die nach Mayring (2010) notwendig sind.

4.3.2 Analyse der Entstehungssituation

Da es bei der qualitativen Sozialforschung um das menschliche Handeln geht und zur Erhebung dessen Interviews geführt werden, ist es notwendig, dass eine genaue Beschreibung vorliegt, die zeigt, wie die Daten erhoben wurden (vgl. Mayring, 2010). Diese Beschreibung kann den Abschnitten 3.3 Stichprobenbeschreibung und 3.5 Datenerhebung entnommen werden. Während sich Abschnitt 3.3 Stichprobenbeschreibung den Personen selbst widmet und deren Hintergründe erläutert, befasst sich Abschnitt 3.5 Datenerhebung mit der grundsätzlichen Durchführung der Interviews. Zusammen ergeben diese beiden Abschnitte einen Überblick über die Entstehungssituation, die von Mayring (2010) gefordert wird.

4.3.3 Formale Charakteristika des Materials

Die formalen Charakteristika beschreiben, wie das Material, in diesem Fall die Interviews, vorliegt (vgl. Mayring, 2010). Die Interviews wurden, wie bereits erwähnt, transkribiert, womit diese in textueller Form vorliegen. Geht es nach Mayring (2010), so kann die Transkription auch anders als wortwörtlich erfolgen. Wichtig dabei ist, dass die Regeln, die bei der Transkription verfolgt werden, für jedes Interview gleich sind und im Vorhinein definiert werden. Die Transkription des Materials dieser Arbeit orientierte sich an folgenden Regeln:

- Kennzeichnung von besonders auffälligen Gesten
- Entfernung von Füllwörtern, wie zum Beispiel ‚äh' oder ‚hmm'
- Umformulierung in grammatikalisch richtige und deutsche Sätze, ohne dabei den Inhalt zu ändern
- Entfernung von halben Sätzen, die keinen Inhalt haben
- Einfügung eines Absatzes, wenn der Sprecher wechselt
- Anonymisierung von Firmen und Personen, die erwähnt wurden

4.3.4 Richtung der Analyse

Die Analyse des Materials kann sich von Fall zu Fall unterscheiden und sich dementsprechend an voneinander abweichenden Gesichtspunkten orientieren. Beispielsweise ist festzulegen, ob

das Material so analysiert werden soll, dass der fachliche Inhalt des Gespräches erfasst wird, oder ob etwas über die Teilnehmerin oder den Teilnehmer selbst herausgefunden werden soll (vgl. Mayring, 2010).

Bei den Interviews dieser Arbeit soll der Fokus rein auf den Text gelegt werden, wobei relevante Hintergrundinformationen zur interviewten Person in die Analyse einfließen. Die interviewten Personen sollten angeregt werden, ihre Meinung und Erfahrungen mit ERP-Systemen in Verbindung mit der Cloud zu teilen, wobei der Schwerpunkt auf der IT-Sicherheit liegen sollte.

4.3.5 Theoretische Differenzierung der Fragestellung

Die Inhaltsanalyse ist theoriegeleitet, was bedeutet, dass die Fragestellungen im Vorfeld bereits festgelegt wurden und die Basis für die Analyse des Materials darstellen (vgl. Mayring, 2010). Kritik an dieser Theoriegeleitetheit kann schnell entkräftet werden:

> *„Theorien, so wird häufig gesagt, würden das Material verzerren, den Blick zu sehr einengen, würden ein »Eintauchen in das Material« behindern. Begreift man jedoch Theorie als System allgemeiner Sätze über den zu untersuchenden Gegenstand, so stellt sie nichts anderes als die gewonnenen Erfahrungen anderer über diesen Gegenstand dar. Theoriegeleitetheit heißt nun, an diese Erfahrungen anzuknüpfen, um einen Erkenntnisfortschritt zu erreichen.* (Mayring, 2010)

Die Theorie liefert bereits Aussagen über Bedenken, die sich gegenüber ERP-Systemen in der Cloud bezüglich IT-Sicherheit ergeben. In der Empirie sollen diese Bedenken konkretisiert werden, indem aufbauend auf den theoretischen Grundlagen Personen interviewt werden. Die Empirie gibt somit nicht nur Aufschluss darüber, welche Bedenken es gibt, sondern auch, ob es überhaupt welche gibt.

4.3.6 Bestimmung der Analysetechnik

Im Gegensatz zur qualitativen Analyse, die fertige Abläufe auf das Material anwendet, wird bei der qualitativen Inhaltsanalyse das Material auf dessen Grundstruktur überprüft, um die geeignete Analysetechnik dafür zu finden. Grundsätzlich lassen sich die Analysetechniken der qualitativen Inhaltsanalyse auf die drei Techniken der Zusammenfassung, Strukturierung und Explikation zurückführen (vgl. Mayring, 2010).

Zusammenfassung: Das Ziel der Zusammenfassung bei der qualitativen Inhaltsanalyse ist eine Kürzung des Materials, bei der Kernaussagen erhalten bleiben und somit keine wesentlichen Erkenntnisse verloren gehen. Das Ergebnis spiegelt somit das Material in kompakter Art und Weise wider (vgl. Mayring, 2010).

Strukturierung: Die Analysetechnik der Strukturierung wird verwendet, um das Material auf Basis von vorher festgelegten Kriterien zu filtern. Im Anschluss daran wird das Material für die einzelnen Kriterien ausgewertet (vgl. Mayring, 2010).

Explikation: Im Gegensatz zu den ersten beiden Analysetechniken hat die Explikation das Ziel, das Material zu erweitern. Gibt es an bestimmten Stellen Unklarheiten, so wird zusätzliches Material beschafft, um daraus Erkenntnisse zu gewinnen (vgl. Mayring, 2010).

Diese drei Analysetechniken entsprechen laut Mayring (2010) auch dem grundsätzlichen Verständnis davon, wie an unbekannte Sachverhalte herangetreten werden kann. Dies verdeutlicht er anhand eines Beispiels:

> *„Man stelle sich vor, auf einer Wanderung plötzlich vor einem gigantischen Felsbrocken [...] zu stehen. Ich möchte wissen, was ich da vor mir habe. Wie kann ich dabei vorgehen? Zunächst würde ich zurücktreten, auf eine nahe Anhöhe steigen, von wo ich einen Überblick über den Felsbrocken bekomme. Aus der Entfernung sehe ich zwar nicht mehr die Details, aber ich habe das »Ding« als Ganzes in groben Umrissen im Blickfeld, praktisch in einer verkleinerten Form (Zusammenfassung). Dann würde ich wieder herantreten und mir bestimmte besonders interessant erscheinende Stücke genauer ansehen. [...] (Explikation). Schließlich würde ich versuchen, den Felsbrocken aufzubrechen, um einen Eindruck von seiner inneren Struktur zu bekommen [...] (Strukturierung).“* (Mayring, 2010)

Für diese Arbeit wird die Zusammenfassung als Analysetechnik gewählt. Die zusammenfassende Inhaltsanalyse ist ein Prozess, deren Ergebnis die Kernaussagen aus dem vorliegenden Material sind. Trotz dieser Reduzierung bleibt der eigentliche Inhalt erhalten und bildet damit die Basis für die Auswertung des Materials. Die zusammenfassende Inhaltsanalyse ist zudem eine repräsentative Methode zur Analyse des Materials und eignet sich dadurch zur Verwendung in dieser Arbeit (vgl. Mayring, 2010).

Wie bereits bekannt, reduziert die Zusammenfassung das Material auf die wesentlichen Inhalte. Diese Reduzierung ist ein Prozess, der das Material auf eine höhere Abstraktionsebene bringt und sich grob in die drei Schritte der Paraphrasierung, Generalisierung und Reduktion einteilen lässt (vgl. Mayring, 2010). Der detailliertere Ablauf, auf den im Folgenden eingegangen wird, wird in Abbildung 4-2 dargestellt.

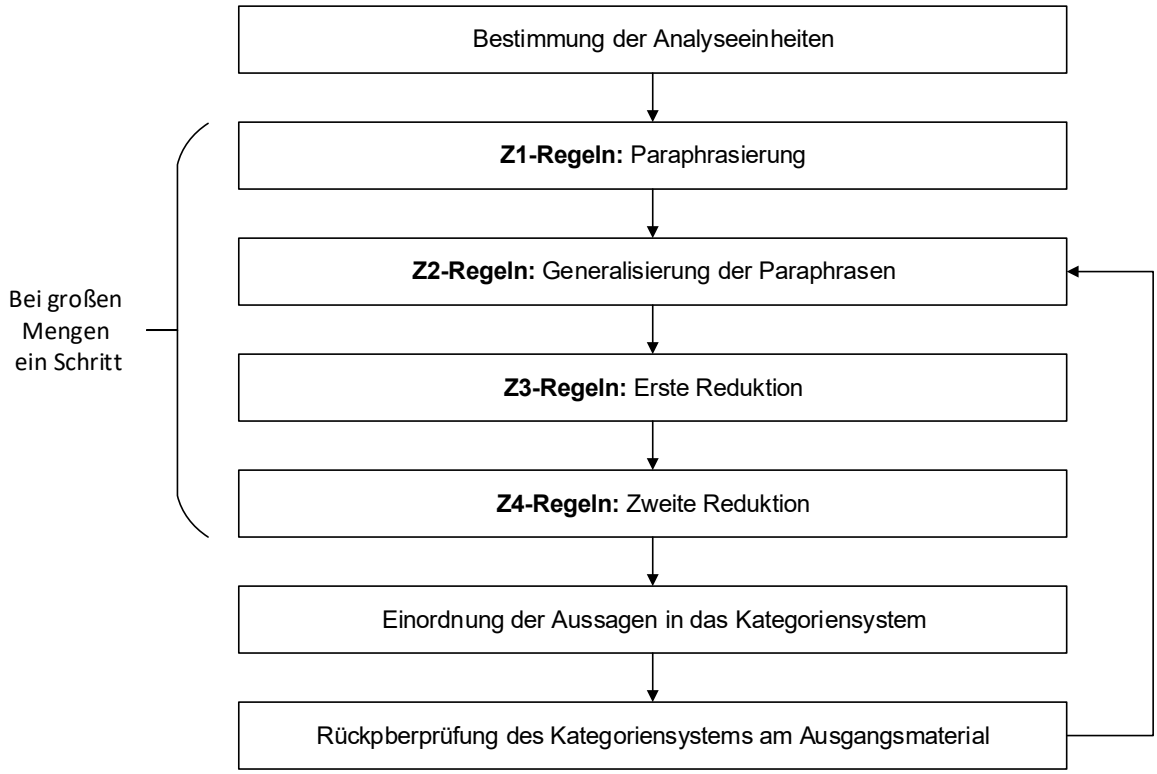


Abbildung 4-2 Zusammenfassende Inhaltsanalyse (Mayring, 2010)

Der erste Schritt in der zusammenfassenden Inhaltsanalyse, der in Abschnitt 4.3.7 erläutert wird, ist die Bestimmung von Analyseeinheiten. Nachdem die Analyseeinheiten bestimmt wurden, wird das Material so umgeschrieben, dass es einer einheitlichen Sprache folgt (Z1-Regel). Wichtig dabei ist die Umformulierung in die deutsche Sprache mit korrekter Grammatik, das Weglassen von inhaltlich wertlosen Textstellen und die Kürzung auf das Wesentliche (vgl. Mayring, 2010). Diese erste Transformation des Materials heißt Paraphrasierung und kann zum Beispiel so aussehen:

- Vorher: ‚Ja, also, ich denke schon, dass die Cloud sicher ist.'
- Nachher: ‚Ich denke, dass die Cloud sicher ist.'

Im nächsten Schritt, der Generalisierung, wird das Abstraktionsniveau erhöht, um im Anschluss daran die erste Reduktion durchführen zu können. Im Zuge der Generalisierung werden alle Paraphrasen, die sich unter dem angestrebten Abstraktionsniveau befinden, verallgemeinert. Paraphrasen, die das Niveau bereits erreicht haben, können so belassen werden (Z2-Regeln). Als Resultat dieses Schrittes wird das gesamte Material in Paraphrasen dargestellt, die inhaltlich gleich sind. Das Weglassen dieser Paraphrasen stellt die erste Reduktion dar (Z3-Regeln). Um das Material weiter zu reduzieren, wird das Material nun auf Paraphrasen untersucht, die sich aufeinander beziehen und inhaltlich das gleiche Thema behandeln. Diese Paraphrasen werden gebündelt und zu neuen Aussagen zusammengefasst (Z4-Regeln), was auch als zweite Reduktion bezeichnet wird. Die Aussagen können anschließend als Kategoriensystem dargestellt werden (vgl. Mayring, 2010).

Sind die Kategorien gebildet, so müssen diese mit dem Ausgangsmaterial gegengeprüft werden. Konkret bedeutet das, dass die Paraphrasen im Kategoriensystem aufgehen müssen. Ist dies nicht der Fall, so muss eine weitere Iteration erfolgen, was mit der Erhöhung des Abstraktionsniveaus erreicht werden kann. Die Kategorien stehen dabei im Zentrum der Analyse und verbinden unter anderem die Theorie mit dem Material aus der Praxis (vgl. Mayring, 2010).

Ein weiteres Problem kann die Größe des Materials darstellen. Bei einer großen Menge an Material ist es nicht möglich, für das gesamte Material Paraphrasen zu finden. In diesem Fall können mehrere Schritte zusammengefasst werden. Das Kategoriensystem zeigt dabei den induktiven Charakter der qualitativen Forschung. Im Gegensatz zur deduktiven Bildung der Kategorien, die aus der Theorie erfolgt, leiten sich die Kategorien aus dem Material ab (vgl. Mayring, 2010).

Nachdem das Material dieser Arbeit reduziert wurde, ergeben sich nach Bildung des Kategoriensystems folgende Kategorien:

- Bewertung des gegenwärtigen Stands der Technik hinsichtlich der Cloud
- Bewertung der Zukunftsaussichten für ERP-Systeme in der Cloud
- Cloudbasierte ERP-Systeme – KMU und Start-ups vs. Großunternehmen
- Gegenwärtige IT-Infrastruktur im Unternehmen
- Rechtliche Aspekte von ERP-Systemen in der Cloud
- Verantwortung für IT-Systeme
- Verfügbarkeit von IT-Systemen
- Verständnis der Cloud und der IT-Sicherheit
- Vertrauen in den Anbieter der Cloud vs. die IT-Abteilung im Unternehmen
- Vertraulichkeit in IT-Systemen

4.3.7 Definition der Analyseeinheit

Um die Präzision der qualitativen Inhaltsanalyse zu erhöhen, werden Analyseeinheiten festgelegt:

- Kodiereinheit: kleinster Textteil, der unter eine Kategorie fällt
- Kontexteinheit: größter Textteil, der unter eine Kategorie fällt
- Auswertungseinheit: Reihenfolge der Auswertung von Textteilen (vgl. Mayring, 2010)

„Bei der Bestimmung der Analyseeinheiten muss zunächst festgehalten werden, dass bei Zusammenfassung Auswertungs- und Kontexteinheit zusammenfallen“ (Mayring, 2010), wodurch die gebildeten Kategorien beides repräsentieren. Die Kodiereinheiten bilden die Paraphrasen, die aus dem Material hervorgegangen sind.

4.3.8 Rücküberprüfung des Kategoriensystems

Nach der Rücküberprüfung des Kategoriensystems mit dem eigentlichen Material ist das Material bereit, um die Ergebnisse daraus zu abzuleiten. Die kontinuierliche Reduzierung des Materials soll mit der Hilfe von Abbildung 4-3 nochmals veranschaulicht werden.

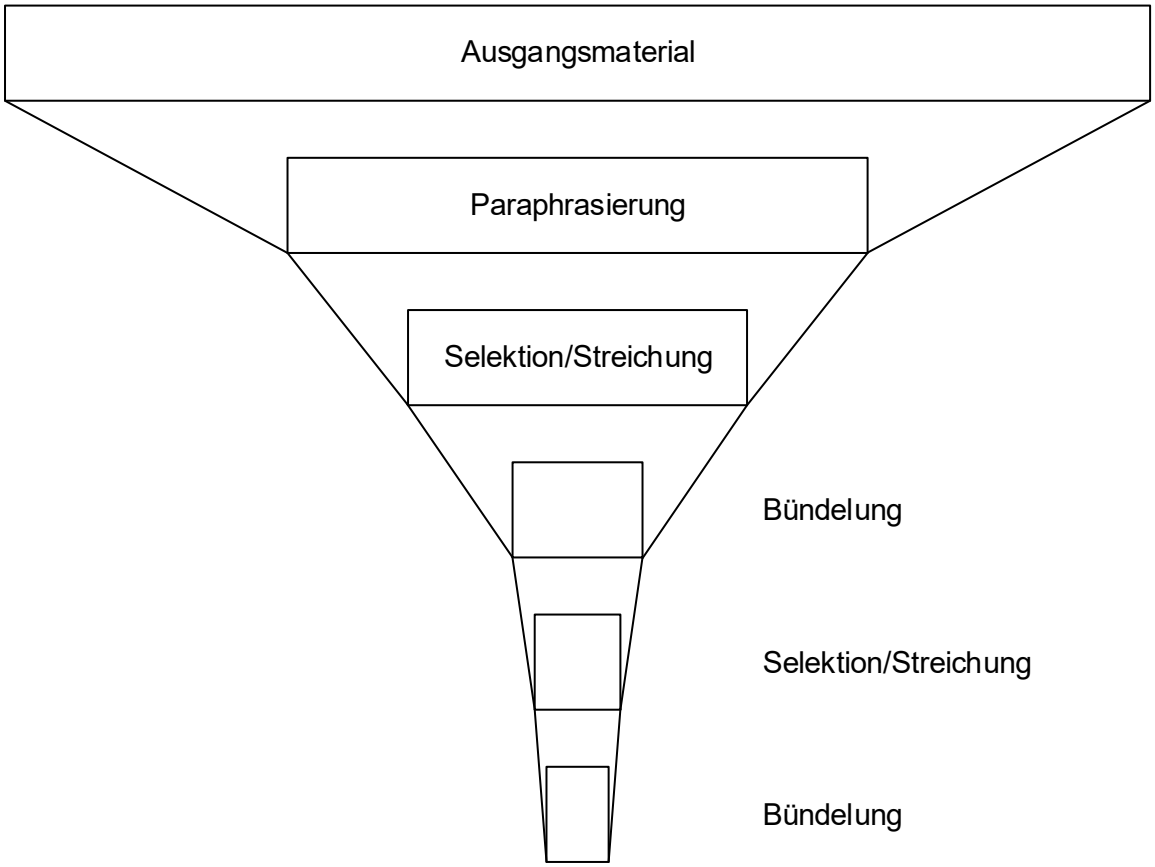


Abbildung 4-3 Reduzierung des Materials (Mayring, 2010)

4.3.9 Zusammenstellung der Ergebnisse

Mit dem letzten Schritt ist die Bildung der Kategorien abgeschlossen, wodurch es nun möglich ist, die Ergebnisse der zusammenfassenden Inhaltsanalyse zu präsentieren. Dazu werden im nächsten Schritt die Kernaussagen pro Kategorie interpretiert und mit Zitaten untermauert, um die Repräsentativität zu steigern.

Verständnis von Cloud und IT-Sicherheit

In der ersten Kategorie geht es um das generelle Verständnis der Begriffe Cloud und IT-Sicherheit. Diese Kategorie ist vor allem darum wichtig, weil bereits aus der Theorie bekannt ist, dass diese Begriffe scharf voneinander abgegrenzt werden müssen. Aus diesem Grund wurde zu Beginn der Interviews darauf Wert gelegt, die Definition der jeweiligen interviewten Person zu erfahren. Diese Definition wurde im Anschluss verwendet, um einen gemeinsamen Wissensstand identifizieren zu können.

Der Begriff ‚Cloud' führte wie erwartet zu den verschiedensten Definitionen. Problematisch für die Interviewpartner war die Unterscheidung zwischen einer Private Cloud und einem eigenen Rechenzentrum. Der Grund dafür lag in der Annahme, dass mit der Virtualisierung ebenfalls Skalierbarkeit und Flexibilität in der IT-Infrastruktur erreicht werden kann, wie die Aussage von Interviewpartner 3 zeigt:

> *„Über VPN und Server ist man die letzten 20 Jahre schon von Außenstellen oder Office-Arbeitsplätzen auf die Systeme gekommen. Das ist in meinen Augen keine klassische Cloud-Lösung. Für mich ist Cloud die klassische Public Cloud. Das heißt, dass unsere Daten bei unseren Lieblingsanbietern Amazon, Google oder MS Azure und außerhalb meines physikalischen Bereich liegen. Wenn ich das in meinem Rechenzentrum laufen lasse und einen Zugang von außen habe, dann würde ich das noch nicht als Cloud bezeichnen." (Interviewpartner 3, 2017)*

Wie aus diesem Zitat hervorgeht, war die Definition der Public Cloud wesentlich einfacher und offensichtlicher für die Interviewpartner als die Definition des Rechenzentrums. Das liegt daran, dass aufgrund der Schwierigkeit der Unterscheidung zwischen der Private Cloud und dem eigenen Rechenzentrum, die Public Cloud als Synonym für die Cloud verwendet wurde. Bezogen auf diesen Begriff waren alle Interviewpartner der Meinung, dass es sich hierbei um die Bereitstellung von Infrastruktur oder kompletter Software handelt, wobei die Hardware von einem anderen Unternehmen verwaltet wird. Bezogen auf die Public Cloud gaben die Interviewpartner zusätzlich an, dass nicht bekannt ist, wo die Daten liegen und wie die Public Cloud im Hintergrund funktioniert.

> *„Ich verstehe unter der Cloud, dass man einerseits Infrastruktur von kleinen oder großen Anbietern, wie zum Beispiel Google oder Amazon, zur Verfügung gestellt bekommt. Andererseits geht es um die Software und Services an sich. Gewisse Dienstleistungen, Software und Programme liegen nicht mehr am lokal gehosteten Server, sondern auf einer anderen Infrastruktur." (Interviewpartner 5, 2017)*

Der zweite Begriff, der im Rahmen der Interviews von Bedeutung war, ist ‚IT-Sicherheit'. Geht es um IT-Sicherheit, so wird vor allem von den drei Säulen Verfügbarkeit, Vertraulichkeit und Integrität gesprochen. Jedoch zeigte sich auch bei diesem Begriff, dass es wichtig ist, ihn im Vorfeld genau abzugrenzen.

Von den Interviewpartnern wurde zur Bestimmung der IT-Sicherheit überwiegend nur der Punkt der Vertraulichkeit genannt. Ein ERP-System in der Cloud ist für sie dann sicher, wenn es vor unberechtigtem Zugriff, wie zum Beispiel gegen Angriffe von außen, geschützt wird. Interessant war die Aussage von einem Interviewpartner, der IT-Sicherheit gänzlich abseits der drei Begrifflichkeiten definierte. Für ihn ist IT-Sicherheit eine Richtlinie im Unternehmen, die zu Beginn niedergeschrieben werden muss. Die technische Umsetzung ist dann dem IT-Leiter oder der zuständigen Person überlassen.

> *„IT-Sicherheit ist ein sehr weit gefasster Begriff. Da ist die Frage was man unter IT-Sicherheit anschauen will. Geht es um Zugriffsrechte, Übertragungssicherheit,*

> *Sicherheit im Programm. Es kommt drauf an aus welcher Sicht man das betrachtet. Aber im Großen und Ganzen ist es, dass einfach kein unberechtigter Zugriff auf die Daten stattfindet.“ (Interviewpartner 1, 2017)*

Grundsätzlich konnten beim Verständnis der beiden Begriffe keine signifikanten Unterschiede in Bezug auf die Position im Unternehmen oder die Größe des Unternehmens festgestellt werden.

Bewertung des gegenwärtigen Stands der Technik hinsichtlich Cloud

Im Zuge der Interviews sollte unter anderem herausgefunden werden, welche Position die Personen zum Thema ERP-Systeme in der Cloud beziehen. Während es keine Unterschiede hinsichtlich der Unternehmensgröße der Interviewpartner gab, zeigten sich Differenzen zwischen IT-Leitern und IT-Mitarbeitern. Die IT-Leiter vertraten im Gegensatz zu den IT-Mitarbeitern eine negative Meinung zur Cloud, sodass sie für den Einsatz von ERP-Systemen in der Cloud zum Zeitpunkt des Interviews so gut wie keine Chance sahen. Die Bedenken liegen dabei im Bereich der IT-Sicherheit, da davon ausgegangen wird, dass sie das eigene System besser schützen können. Die einzige Ausnahme bildet dabei eine Cloud-Lösung, bei der selbst für die Sicherheit gesorgt werden kann, wie zum Beispiel bei IaaS.

> *„Wenn ich in der Public Cloud bin, dann ist auch Microsoft nicht davor geschützt einem Hacker zum Opfer zu fallen. Ich glaube, dass man das in einer Private Cloud eher gewährleisten kann als in einer Public Cloud. Wobei, wenn ich die Daten bei mir vor Ort habe [...], dann ist die Sicherheit schon höher. [...] Solange du die Cloud nicht selbst betreibst oder nicht jedes Detail von dieser Cloud kennst, weißt du nicht wer mitschaut, Verschlüsselung hin oder her.“ (Interviewpartner 6, 2017)*

Weniger kritisch wird die Cloud von IT-Mitarbeitern bewertet. Obwohl es hier auch vereinzelt Zweifel an der Sicherheit der Cloud gibt, stehen diese dem Thema weitaus positiver gegenüber. Werden deren Aussagen betrachtet, so wird schnell klar, dass die Cloud bereits im Privatleben eine große Rolle spielt und den Unternehmen anscheinend der Mut fehlt, diese Lösung auch für berufliche Zwecke zu nutzen. Dies lässt sich gut an einer provokanten Aussagen von Interviewpartner 5 zeigen:

> *„Die Leute stellen sich zuhause Alexa hin, wo, rein theoretisch, Amazon pausenlos mithören könnte was man in den eigenen vier Wänden sagt. Auf der anderen Seite kommt dann Angst auf, dass ich meine ERP-Daten dort habe.“ (Interviewpartner 5, 2017)*

Eine Meinung, die IT-Leiter und IT-Mitarbeiter miteinander teilen, ist die Einstellung zur Public Cloud. Diese wird für ERP-Systeme als untauglich angesehen, da sie zu wenig Sicherheit bietet. Die Bedenken dabei sind vor allem, dass nicht bekannt ist, wo die Daten liegen und wie die Hintergrundprozesse im Detail aussehen. Hier ist es allen Interviewpartnern lieber, wenn sie zumindest einen Private-Cloud-Anbieter haben, der im Idealfall seinen Hauptsitz im eigenen Land hat.

Bewertung der Zukunftsaussichten für ERP-Systeme in der Cloud

Neben dem Verständnis der Cloud und der IT-Sicherheit sowie der aktuellen Situation ist vor allem die Bewertung der Zukunftsaussichten von Bedeutung. Dabei geht es um die Einschätzung, wie sich das Thema ‚ERP-Systeme in der Cloud' in Zukunft entwickeln wird. Ähnlich wie beim Verständnis von Cloud und IT-Sicherheit lassen sich hier keine Unterschiede zwischen der Konzerngröße und der eingenommenen Position im Unternehmen erkennen.

Die Interviewpartner sind sich einig, dass in Zukunft die Anbieter von ERP-Systemen ebenfalls dem Trend folgen und die Systeme nur noch in der Cloud anbieten werden. Das bedeutet, dass die Kunden früher oder später umsteigen müssen, wenn die Anbieter diese Richtung vorgeben. Ein Interviewpartner erwähnte als Beispiel dafür den Versuch von Microsoft mit ihrem ERP-System Axapta, welches in der neuesten Version nur noch als Cloud-Lösung angeboten wurde. Es gab jedoch viele Probleme und dieser Schritt wurde nicht belohnt. Während ERP-Systeme noch Zeit brauchen, sind CRM-Systeme bereits einen Schritt weiter.

> *„Gerade wenn man in das benachbarte Feld CRM schaut, dann sind die drei marktführenden Systeme nur in der Cloud. Salesforce komplett, Microsoft Dynamics CRM wird stark in die Cloud Ecke geschoben und SAP mit Cloud for Customer." – (Interviewpartner 3, 2017)*

> *„Spätestens jetzt mit Dynamics365 ist das ein Thema. Das Argument Sicherheit kann man technisch nicht lösen und das ist eher eine Grundsatzentscheidung vom Unternehmen. Viele Kunden arbeiten mit Office365 und einem Exchange Server in der Cloud. Die Mails sind auch irgendwo in der Cloud, gleich wie die Dokumente. Warum also nicht das ERP-System auch?" – (Interviewpartner 5, 2017)*

Die einzige Einschränkung liegt dabei im rechtlichen Bereich. Aufgrund der DSGVO, die ab dem Jahr 2018 Gültigkeit besitzen wird, achten Unternehmen weiter zunehmend darauf, wo ihre Daten liegen und welche Daten überhaupt außerhalb des eigenen Netzwerkes gespeichert werden dürfen.

Zusätzlich muss erwähnt werden, dass IT-Sicherheit immer ein Vorstandsthema ist, dem sich dieser nicht entziehen kann. Oftmals ist es so, dass KMU sich keine ausreichend große und kompetente IT-Abteilung leisten kann, was dazu führt, dass Alternativlösungen gesucht werden. Eine dieser Lösungen ist die Cloud. Was die Cloud für KMU bedeutet, wird im Zuge der Zusammenfassung in einer eigenen Kategorie behandelt.

> *„Ich glaube es hat [...] Zukunft, weil in den höheren Positionen [...] oft technisches Unverständnis herrscht. Man betrachtet nur die Kostenseite […]. Man überlegt sich nicht welche anderen Sachen dahinterliegen. Welche Kosten eine Datenpanne oder ein Datenleck verursacht, das interessiert niemanden, das ist auch nicht bezifferbar. […] Es wird deshalb erfolgreich werden, weil es initial günstiger wird und der Entscheidungsträger kurzsichtig ist. Später wird es darauf hinauslaufen, dass die ERP-Anbieter genügend Marktmacht haben." – (Interviewpartner 2, 2017)*

Gegenwärtige IT-Infrastruktur im Unternehmen

Die ERP-Systeme, die derzeit in den Unternehmen der Interviewpartner im Einsatz sind, werden bis auf eine Ausnahme im lokalen Rechenzentrum betrieben. Die Gründe dafür sind zwar verschieden, es lassen sich jedoch Gemeinsamkeiten in Bezug auf die Kriterien feststellen. Von den IT-Leitern kommen klare Aussagen, dass es momentan zum Beispiel aufgrund von Sicherheitsbedenken nicht in Frage gekommen wäre, das ERP-System in der Cloud zu betreiben. Auf der anderen Seite lässt sich bei den IT-Leitern erkennen, dass diese generell negativ gegenüber Veränderungen eingestellt sind. Eine typische Floskel, die dabei zu hören ist, lautet ‚Never change a running system', was bedeutet, dass bestehende Systeme, die funktionieren, nicht geändert werden sollten. Der Grund dafür liegt in der Tatsache, dass eine Umstellung Ressourcen benötigt und Probleme schafft, was vermieden werden sollte, wenn keine Notwendigkeit besteht. Als weitere Folge der Umstellung könnten die Angestellten unzufrieden sein, wenn das ERP-System nicht wie gewohnt funktioniert und kein sofort sichtbarer Nutzen generiert wird. Auch hier spielt die Unterscheidung zwischen einem Unternehmen und einem Kleinunternehmen oder Start-up, das in naher Zukunft skalieren möchte, eine große Rolle. Dieser Unterscheidung ist jedoch eine eigene Kategorie gewidmet.

> *„Da gibt es natürlich einige, die Nutznießer sind, aber die großen Firmen sehen da nicht unbedingt den großen Vorteil. Die müssen nicht von 0 beginnen und Server und Rechenzentrum aufbauen, da ist schon alles da. Wenn ich denke ich hätte ein älteres SAP-System und ich will unbedingt in die Cloud, dann muss ich vielleicht einen Release-Wechsel machen, dann kostet mich das ein paar hunderttausend Euro, weil ich einen SAP-Release-Wechsel machen muss. Das sind zusätzliche Nachteile dafür, dass ich davor ein laufendes System habe. ‚Never change a running system', wie es so schön heißt." – (Interviewpartner 3, 2017)*

Während die IT-Leiter auf dem aktuellen System beharren, unter anderem auch, weil sie die Verantwortung dafür tragen, sieht die Meinung der IT-Mitarbeiter anders aus. Bei ihnen ist der Wille in die Cloud zu gehen ersichtlich, scheitert aber beispielsweise an rechtlichen Themen. Der theoretische Teil dieser Arbeit hat sich bereits mit den rechtlichen Aspekten, die Auswirkungen auf die Praxis haben, beschäftigt. Auch wenn ein Unternehmen gerne in die Cloud möchte, so ist dies bei vielen Branchen, zum Beispiel im Bildungssektor, aufgrund von Vorschriften und Richtlinien nicht möglich.

Neben diesen Branchen gibt es jedoch auch andere, für die rechtlich gesehen keine Probleme bestehen. Dort unterstellen die IT-Mitarbeiter jedoch fehlenden Mut seitens des Unternehmens. Dies deckt sich mit der Meinung der IT-Leiter, die ein bestehendes und funktionierendes System nicht ändern wollen. Auch hier ist der Größenunterschied zwischen den Unternehmen relevant.

> *„Das ist auch dadurch begründet, dass in einem Großunternehmen Leute da sind, die das System aufgebaut haben und wissen wie das funktioniert. Und nach dem Motto ‚Never touch a running system' bleibt es so. Wenn aber die ältere Garde in Pension geht und konzeptionell ein Projekt angestoßen wird, dann wird es mittelfristig auch in*

> *Großunternehmen Erfolg haben, wenn junge Leute das treiben und sich mit dem Thema auseinandersetzen.“ (Interviewpartner 5, 2017)*

Rechtliche Aspekte in Bezug auf ERP-Systeme in der Cloud

Wie bereits in anderen Kategorien und der Theorie erwähnt, spielen rechtliche Aspekte eine große Rolle bei der Entscheidung, ob ein ERP-System in der Cloud betrieben wird oder nicht. An dieser Stelle sei mit aller Deutlichkeit noch einmal auf die ab Mai 2018 gültige DSGVO hingewiesen. Die Entscheidung, wie mit sensiblen Daten umgegangen werden muss, wird ab diesem Zeitpunkt in der Verordnung festgelegt, deren Nichteinhaltung zu Strafzahlungen führt. Die DSGVO wurde auch von beinahe allen Interviewpartnern erwähnt und deren Einfluss beschrieben. Während die Position im Unternehmen der Interviewpartner keine Rolle spielte, ließen sich bei der Unternehmensgröße Unterschiede in Bezug auf die Einschätzung der DSGVO feststellen. Hierbei war vor allem auffallend, dass Großunternehmen darin kein großes Problem sehen, weil die meisten Punkte, die darin gefordert werden, ohnehin schon im Unternehmen umgesetzt werden. Beispielsweise schreibt die DSGVO vor, dass gewisse Daten im eigenen Land liegen oder Katastrophenfälle vorbereitet sein müssen. Wird jedoch mit Personen in Großunternehmen gesprochen, so gibt es bereits seit Jahren Pläne, die im Katastrophenfall (zum Beispiel Infektion aller Clients mit einem Virus) zum Tragen kommen. Das Bewusstsein für IT-Sicherheit ist dort somit bereits gegeben.

> *„Uns tun Serverausfälle nicht weh. Wir haben Szenarien, wo wir sogar die Client-PCs komplett sichern. Damit können auch Szenarien abgedeckt werden, wo Rechner kaputtgehen und nicht mehr bootfähig sind etc. Dann sind in 1–2 Tagen wieder alle Rechner mit kleiner Mannschaft online.“ – (Interviewpartner 3, 2017)*

Zusätzlich war es bereits in der Vergangenheit leichter, die Daten im eigenen Land gespeichert zu wissen, um rechtliche Probleme zu vermeiden. Ein weiterer Aspekt dabei ist das Vertrauen, das in die Anbieter der IT-Infrastruktur bestehen muss. Viele Unternehmen fühlen sich von vornherein wohler, wenn sie von einem Unternehmen aus der Umgebung betreut werden, das zusätzlich noch eine gute Reputation genießt.

> *„Das macht für mich einen großen Unterschied, da ich der Meinung bin, dass sehr viele Entscheidungsträger es haben wollen, dass der Lieferant der gleichen Nationalität entspricht. Bzw. kann man sich dann leichter an der Gesetzgebung orientieren. Das würde also einen großen Unterschied zwischen Private und Public Cloud machen. Ganz einfach deswegen, weil die juristischen Teile wesentlich einfacher wären.“ – (Interviewpartner 2, 2017)*

Anders sieht es bei KMU aus, in denen kaum ein Bewusstsein für die Inhalte der DSGVO vorhanden zu sein scheint. Hier ist in einem Katastrophenfall nicht klar definiert, wer sich kümmert oder wie das System wiederhergestellt werden kann. Grundsätzlich ist es für KMU derzeit schwer, da sie sich plötzlich veränderten Herausforderungen gegenübergestellt sehen. Umso interessanter sind die Aussagen eines Interviewpartners, in denen von einem IT-Sicherheitskonzept die Rede ist, dass den Kunden des Cloud-Anbieters genau zeigt, wo die

Daten physikalisch liegen und dass eine Begehung der Serverräume jederzeit möglich ist. Dies ist einer der großen Unterschiede zwischen einem kleinen Cloud-Anbieter und Unternehmen wie Google oder Microsoft. Bei den großen Cloud-Anbietern kommen schnell Zweifel daran auf, ob die Daten wirklich am vom Unternehmen angegebenen Ort liegen.

> *„Und das, was schlussendlich überbleibt ist, dass ich nicht weiß, wo alles physikalisch liegt und dass ein Großkonzern im Hintergrund, wenn er will, die Daten abgreifen kann und tun kann was er will.“ – (Interviewpartner 5, 2017)*

Verfügbarkeit von IT-Systemen

Verfügbarkeit ist einer der drei Grundätze in der IT-Sicherheit und spielte auch in den Interviews eine große Rolle. Die Schwerpunkte lagen dabei auf der Frage nach einem weiteren Vorgehen, wenn die Internetverbindung ausfällt und was passiert, wenn ein Server ausfällt.

Geht es um die Internetverbindung, so sind sich alle Interviewpartner einig, dass diese eine Grundvoraussetzung für die Nutzung eines ERP-Systems in der Cloud ist (unter der Prämisse, dass keine Private Cloud im eigenen Rechenzentrum betrieben wird, die im internen Netzwerk verfügbar ist). Die Frage, die sich Unternehmen bei einem ERP-System in der Cloud stellen müssen, ist: ‚Was tue ich, wenn die Internetverbindung ausfällt?’ Werden im Vorfeld keine Vorkehrungen getroffen und dieses Risiko besprochen, so stellt ein solches Szenario das Unternehmen vor eine schwere Aufgabe. Auf der anderen Seite kann es natürlich auch passieren, dass im eigenen Rechenzentrum ein zentraler Switch ausfällt und das Netzwerk zusammenbricht. Auch auf dieses Szenario muss ein Unternehmen vorbereitet sein. Hier zeigt sich wiederum der Unterschied zwischen den Großunternehmen und einem KMU. Während Großunternehmen genügend Vorkehrungen für alle möglichen Risiken treffen, stehen KMU kaum Ressourcen zur Verfügung, um jedes Risiko komplett abdecken zu können, wenn es zu einem Notfall kommt.

> *„Wir im Handel haben das Problem, dass ohne Internet dann alles stehen würde und das wäre eine Katastrophe.“ – (Interviewpartner 4, 2017)*

> *„Aber zum Beispiel heute, da hatten wir seit drei Jahren das erste Mal ein Problem mit der Internetleitung. Wenn ich nun sehr viel in der Cloud habe, dann stehe ich mit fast allen Applikationen, so stehe ich halt mit dem Internet. Das Mail kommt dadurch vielleicht etwas langsamer herein. Praktisch könnten wir das Internet abdrehen und könnten ein paar Tage davon leben.“ – (Interviewpartner 3, 2017)*

Ähnlich wie in Bezug auf die rechtlichen Aspekte sind Großunternehmen gut auf Risiken eingestellt, während KMU dahingehend noch Aufholbedarf haben. Die Internetleitung bringt dabei ein weiteres Problem mit sich: Performanz. Gerade außerhalb der Städte ist eine schnelle Internetleitung ein Problem, da diese entweder nicht existiert, oder im Vergleich zu Städten extrem teuer ist. Auch hier muss sich ein Unternehmen die Frage stellen, ob es sinnvoll ist, das ERP-System in der Cloud zu betreiben, oder ob die Verfügbarkeit ein zu großes Risiko darstellt.

> *„Das Problem ist, dass wir am Land keine vernünftige Infrastruktur haben. Ich habe keine vernünftige Leitung bräuchte mindestens eine 100-Mbit-Anbindung. Das ist in der*

> *Stadt kein Problem, aber bei uns am Land [...]. Die Infrastruktur am Land ist einfach nicht vorhanden. Ich zahle zum Beispiel 1000 € im Monat für eine 20-Mbit-Leitung. [...] Es gibt drei Stufen in Österreich: Stufe 1 ist Wien, Stufe 2 sind alle Bundeshauptstädte und Stufe 3 ist der Rest. [...] In Wien bekommt man dadurch eine 100-Mbit-Leitung [...] nachgeschmissen. Und bei uns kostet es über 1000 € für 20 Mbit. Fazit ist, dass ich sicher nicht mit meinem ERP-System in die Cloud gehe, wenn ich nur eine 20-Mbit-Leitung habe." – (Interviewpartner 4, 2017)*

Da die Internetverbindung unabhängig vom eingesetzten ERP-System ist, handelt es sich hier um ein generelles Bedenken, das von den Interviewpartnern durchgängig genannt wurde. Neben der Internetverbindung erwähnen die Interviewpartner ein weiteres Problem, das im Zuge der Benutzung eines ERP-Systems in der Cloud auftritt. Obwohl die Internetleitung in Ordnung ist, kann es zu einem Ausfall des ERP-Systems kommen. Dieser Ausfall kann zahlreiche Gründe haben, wie zum Beispiel den Ausfall eines Servers. In diesem Fall ist es normalerweise die Aufgabe der IT, das Problem zu beheben und das ERP-System wieder verfügbar zu machen. Wird das ERP-System nun in der Cloud und nicht im eigenen Rechenzentrum betrieben, so entsteht das Problem, dass die Wiederherstellung des Zugriffs auf das System nicht in der eigenen Hand liegt, sondern in der des Cloud-Anbieters.

Hier zeigt sich, dass IT-Leiter den Cloud-Anbietern zwar vertrauen, es aber trotzdem lieber hätten, wenn sie die Wiederherstellung selbst lenken könnten. Obwohl das Unternehmen sich im Vorhinein rechtlich gegen solche Szenarien absichert, so ist den IT-Leitern wohler, wenn sie ihren eigenen Mitarbeitern diese Aufgabe übertragen können. Vor allem Großunternehmen teilen diese Meinung, was jedoch auch daran liegt, dass genügend Ressourcen zur Verfügung stehen.

Grundsätzlich teilen die Interviewpartner die Meinung, dass ein Anbieter der Cloud die nötige Kompetenz hat, um solche Probleme zu lösen. Bedenken äußern sich aber dahingehend, dass ein gewisses Vertrauen notwendig ist, das dem Cloud-Anbieter entgegengebracht werden muss.

> *„Hier würde ich bei der Private Cloud [...] den Vorteil sehen, dass deren Administratoren viel mehr Erfahrung in Sachen Desaster-Management haben und deswegen schneller sind. Denn sie haben das schon bei mehreren Unternehmen gesehen, im Gegensatz dazu, wo das Unternehmen selbst dafür zu sorgen hat. Denn das kennt nur sich selbst und hat womöglich weniger Erfahrung davon. Die Frage ist, was wirklich passiert, wenn die Datenbank plötzlich abstürzt. Jeder geht davon aus, dass man genügend Racks und Sicherungen hat, aber hat man die Garantie? Das sehe ich als Problem. Denn bei der Cloud muss ich darauf vertrauen, dass es jemand anders kann. Bei meinem Rechenzentrum kann ich das selbst bestimmen." (Interviewpartner 2, 2017)*

Vertraulichkeit in IT-Systemen

Ein weiterer Grundsatz der IT-Sicherheit ist die Vertraulichkeit. Dabei geht es grundsätzlich darum, dass nur Personen auf die Daten zugreifen dürfen, die dazu berechtigt sind. Dennoch unterscheiden sich hier die Sichtweisen von IT-Leitern und IT-Mitarbeitern.

IT-Leiter sehen bei einem ERP-System in der Cloud vor allem das erhöhte Risiko, Ziel eines Angriffes zu werden. Den Grund dafür sehen sie darin, dass ein Cloud-Anbieter mehrere Unternehmen gleichzeitig auf seinen Servern verwaltet. Dabei kann es leicht passieren, dass ein Unternehmen mit interessanten Daten dabei ist, auf die mögliche Angreifer gerne zugreifen würden. Bei einem solchen Angriff werden die Daten eines anderen Unternehmens evtl. ebenfalls mitgelesen oder weitergegeben, obwohl diese nicht das primäre Ziel des Angreifers waren. Wie bereits bekannt ist, ist die genaue Funktionalität der Cloud den Interviewpartnern nicht bekannt. Das bedeutet, dass sich das obige Szenario nicht ausschließen lässt, solange keine Klarheit darüber besteht, wie die Cloud im Hintergrund funktioniert und ob eine strikte Trennung zwischen den Daten der verschiedenen Unternehmen stattfindet.

> *„Das ist sicher ein Problem. Die Frage ist wie schnell sie zu den Daten hinkommen. Die werden sicher nicht als Datei auf einer Festplatte abgelegt sein, sondern sicher woanders liegen. Das ist sicher eine Überlegung wert[...]. Aber ich gehe davon aus, dass wenn jemand sowas anbietet, dann macht er es richtig. Und ich denke, dass sie die Kundendaten so trennen, dass man von einem nicht auf den anderen schließen kann. Wenn es Hackerangriffe gibt, dann sind das meistens keine Amateure, sondern Profis.“ (Interviewpartner 4, 2017)*

Grundsätzlich vermuten die Interviewpartner in der Cloud ein erhöhtes Schutzniveau, was jedoch nicht nur Vorteile mit sich bringt. Durch das obige Problem muss sich das Unternehmen wieder über die Frage nach dem Risiko und dessen Folgen Gedanken machen. Wird das ERP-System mit den Daten im eigenen Rechenzentrum betrieben, so muss das Unternehmen das primäre Ziel eines Angreifers sein. Zusätzlich sollte ein Bewusstsein darüber bestehen, dass es keinen 100%igen Schutz gibt und es sich bei Angreifern selten um Amateure handelt, sondern um professionelle Angreifer, die genau wissen was sie wollen und wie sie ihr Ziel erreichen können.

> *„Bei IT-Sicherheit ist es, wenn man mögliche Angriffsszenarien und Schutzmechanismen anschaut, so, dass man bei Anbietern von Cloud-Lösungen natürlich ein höheres Schutzniveau hat, als wenn man es selbst macht. Das steht außer Zweifel, das schafft man nicht. Es besteht natürlich mehr Gefahr, indem mehr ‚böse Buben’ angelockt werden. Das heißt, dass mehr Angriffe auf Public Clouds und deren Rechenzentren stattfinden, als auf meinen eigenen Server, den ich zuhause stehen habe.“ – (Interviewpartner 3, 2017)*

> *„Trotzdem ist man nicht davor gefeit, dass die gehackt werden. Das ist man aber als Einzelanbieter natürlich auch nicht. Ich kenne es aus Erfahrung von Unternehmen, die in der Forschung tätig sind. Diese Forschungen sind natürlich interessant (Interviewpartner 6, 2017)*

Die IT-Mitarbeiter haben im Gegensatz zu den IT-Leitern eine etwas andere Sichtweise hinsichtlich der Vertraulichkeit in ERP-Systemen in der Cloud. Die Mitarbeiter erkennen ebenfalls, dass es sich bei der Cloud um ein attraktiveres Angriffsziel handelt, das trotz besserer Schutzmechanismen ein leichteres Ziel darstellt. Anders als die IT-Leiter machen die IT-

Mitarbeiter sich jedoch Gedanken um die technische Umsetzung des Schutzes. Eine Art und Weise, wie dieses Problem zu lösen sein könnte, ist nach den Interviewpartnern der Einsatz von IaaS, bei dem die Verwaltung der Betriebssysteme und der Software beim Unternehmen liegt. Dieses ist auch selbst für die Verschlüsselung von Daten zuständig, kann aber gleichzeitig die Vorteile der Cloud nutzen.

Zusätzlich gaben die IT-Mitarbeiter an, dass vor allem bei SaaS unbekannt bleibt, auf welche Daten der Cloud-Anbieter auf seinem Server Zugriff hat. Diese Zweifel weisen eine Ähnlichkeit zu den Bedenken hinsichtlich der unbekannten Funktionsweise der Cloud im Hintergrund auf. Speziell bei SaaS ist es vor allem bei großen Anbietern wie Google oder Amazon nicht möglich zu wissen, wie die technische Umsetzung im Hintergrund aussieht. Die Erfahrung zeigt, dass auch große Anbieter nicht vor Angriffen geschützt sind und Daten auch bei diesen Unternehmen unberechtigterweise gelesen und anschließend veröffentlicht werden können.

> *„Für den Betrieb eines ERP-Systems in der Cloud würde ich auf keinen SaaS-Anbieter zugreifen, sondern nur auf IaaS, um alles selbst konfigurieren zu können [...] denn so kann ich die Hardware auslagern und brauche mich nicht um das kümmern. [...] Nachdem ich die Software selber betreibe und die Betriebssysteme verwalte, kann ich z. B. definieren, dass standardmäßig alles verschlüsselt wird. […] Ich kann in die Software oder die Funktionalität vom Anbieter nicht hineinschauen. Und wer weiß, ob da nicht Hintertüren drinnen sind.“ – (Interviewpartner 1, 2017)*

Signifikante Unterschiede zwischen den Aussagen der Mitarbeiter von Großunternehmen und KMU konnten währenddessen nicht festgestellt werden.

Vertrauen in Anbieter der Cloud vs. die IT-Abteilung im Unternehmen

Im Gegensatz zum Betrieb des ERP-Systems im eigenen Rechenzentrum wird dieses bei der Nutzung der Cloud Personen anvertraut, zu denen vor allem bei den großen Anbietern wie Google oder Microsoft keinerlei Bezug besteht. Während die Mitarbeiter der IT-Abteilung bereits über einen längeren Zeitraum bekannt sind und zu ihnen eine gewisse Basis an Vertrauen aufgebaut werden konnte, handelt es sich bei Cloud-Anbietern womöglich um Personen, zu denen kein persönlicher Kontakt vorhanden ist. So muss dem Cloud-Anbieter ein Vertrauensvorschuss dahingehend gewährt werden, dass er sich sorgfältig um das ERP-System des Unternehmens kümmert, obwohl er nicht bekannt ist.

In Bezug auf diesen Punkt gehen die Meinungen von IT-Leitern und IT-Mitarbeitern abermals auseinander. Das Vertrauen gegenüber Cloud-Anbietern ist grundsätzlich gegeben, vor allem weil abgeschlossene Verträge das Unternehmen rechtlich absichern. Dennoch würden sich die IT-Leiter für eine Lösung entscheiden, bei der der Betrieb von ihren eigenen IT-Mitarbeitern übernommen wird. Im Hinterkopf behalten die IT-Leiter dabei immer die Risiken, die durch den Betrieb von IT-Systemen entstehen. Fällt beispielsweise das ERP-System aus, so sind die eigenen Mitarbeiter leichter zu lenken als fremde Personen, die für den Cloud-Anbieter arbeiten. Hier stellt sich zusätzlich die Frage, wie schnell ein Cloud-Anbieter die Systeme wieder online zur Verfügung stellen kann, sodass ein stabiler Betrieb gewährleistet wird. Bei diesem Punkt

überschneidet sich diese Kategorie mit der Verfügbarkeit von IT-Systemen, die bei der Cloud ebenfalls gegeben sein sollte, obwohl die IT-Infrastruktur nicht in den eigenen Händen liegt.

Der zentrale Punkt dieser Kategorie beschäftigt sich jedoch mit dem Bedenken, dass ein Mitarbeiter die Daten des Unternehmens unbefugt weitergibt. Hier steht das Vertrauen im Fokus, das den IT-Mitarbeitern oder den Mitarbeitern des Cloud-Anbieters entgegengebracht wird. Wie bereits erwähnt bevorzugen die IT-Leiter die Variante, in der die eigenen Mitarbeiter den Betrieb des ERP-Systems in der Cloud übernehmen, auch wenn ein gewisses Vertrauen gegenüber den Cloud-Anbietern vorhanden ist. Die IT-Mitarbeiter beziehen einen anderen Standpunkt und bringen den Anbietern der Cloud das Vertrauen entgegen, dass alles reibungslos funktioniert. Dies erfolgt jedoch nur auf Basis einer Bedingung: Der Cloud-Anbieter benötigt eine gewisse Reputation. Das Vertrauen steigt dabei, wenn der Cloud-Anbieter bereits namhafte Unternehmen zu seinen Kunden zählen kann und auch die Öffentlichkeit eine gute Meinung über ihn hat.

Im Endeffekt stehen hinter jedem IT-System nur Menschen, die jederzeit Fehler machen können. Sogenannte ‚schwarze Schafe' kann es immer und überall geben, sodass diese auch im eigenen Unternehmen vorhanden sein könnten. Für die IT-Leiter ist es darum wichtig, dass sie die Personen hinter dem System persönlich kennen und bis zu einem gewissen Grad auch über sie entscheiden können.

> *„Aber wenn ich den persönlich kenne, dann ist das was anderes als der Apple Mitarbeiter in Asien, der die Zugangsdaten verkauft. Da ist mir lieber ich kenne den und weiß wer das ist. Dann habe ich mehr Vertrauen, als wenn meine Daten irgendwo liegen und irgendwer zugreifen kann." (Interviewpartner 3, 2017)*

> *„Da wird es natürlich mehrere schwarze Schafe geben. Ob man das hinreichend absichern kann, zum Beispiel mit Mehrfaktor- oder Mehrpersonenauthentifizierung, das wird nicht in allen Bereichen gehen. Denn irgendwo wird du immer wen haben müssen, der auf alles hinkommt im Administrationsbereich. Da gibt es trotz Absicherungen immer wen, der auf deine Daten kommt." (Interviewpartner 6, 2017)*

Die Unterscheidung zwischen KMU und Großunternehmen spielt bei diesem Aspekt eine untergeordnete Rolle. Ein Vorteil, den die Cloud diesbezüglich für KMU bringt, ist, dass die Wiederherstellung des stabilen Betriebes durch professionelle Mitarbeiter gesichert wird, die durch ihre Tätigkeiten unterschiedlichste Unternehmen bereits kennen und daher eine große Menge an Erfahrung mitbringen. Diese Erfahrung und vor allem die Ressourcen sind in KMU oftmals nicht vorhanden. Schlussendlich kann diese Kategorie mit folgenden Aussagen eines Interviewpartners kurz zusammengefasst werden:

> *„Sie [Anm. d. Verf.: die Kunden der Cloud-Anbieter] müssen definitiv Vertrauen haben, aber das müssen sie auch haben, wenn die Daten im Haus existieren. Denn als Partner und Betreuer des ERP-Systems kann man erst wieder auf die Daten zugreifen. Ob dieses Vertrauen im Betreuer gegeben ist oder nicht hat mit der Cloud nichts zu tun. Natürlich haben bei Unternehmen, die für einen Kunden Daten bereitstellen, mehrere Personen die Möglichkeit, auf die Daten zuzugreifen. Dieses Vertrauen muss da sein,*

aber das muss ich bei meinem IT-Partner, der mir die Umgebung aufsetzt und Fernwartungszugänge hat, genauso haben.“ (Interviewpartner 5, 2017)

Verantwortung für IT-Systeme

Der Betrieb eines ERP-Systems bedeutet auch, dass die IT die Verantwortung dafür trägt, dass alles ordnungsgemäß funktioniert. Mit der Cloud gibt es nun die Möglichkeit, dass diese Verantwortung zu einem Teil ausgelagert werden kann. Hier zeigen sich wieder unterschiedliche Meinungen von IT-Leitern und IT-Mitarbeitern, denn die IT-Leiter sehen, trotz Betrieb in der Cloud, keinen richtigen Vorteil. Der Cloud-Anbieter kümmert sich um die IT-Infrastruktur im Hintergrund und trägt (insofern das im Vertrag geregelt ist) die Haftung, wenn das ERP-System beispielsweise über einen längeren Zeitraum nicht verfügbar ist. Die IT-Leiter bemängelten jedoch, dass im Unternehmen trotzdem Personen gebraucht werden, die sich in Katastrophenfällen auskennen Das Verschieben der Verantwortlichkeiten funktioniert laut ihnen nicht so einfach, wie man es erwartet.

Zusätzlich muss unterschieden werden, welches Betriebsmodell in der Cloud verwendet wird. Bei IaaS und PaaS sind zwar Bedenken wegen der Hardware unnötig, da sich der Cloud-Anbieter um diese kümmert, eine funktionierende Software liegt jedoch in der eigenen Verantwortung. Gefährlich dabei sind vor allem wechselseitige Schuldzuweisungen, die entstehen können, wenn verschiedene Akteure beteiligt sind. Hier fühlen sich die IT-Leiter deutlich wohler, wenn das ERP-System in der eigenen Hand liegt und selbst verwaltet werden kann. Zudem gibt es von Seiten der IT-Leiter Bedenken hinsichtlich der Reaktionszeit des Cloud-Anbieters. Hier wurde ein Gefühl der Hilflosigkeit genannt, da die IT-Leiter sich darauf verlassen müssen, dass der Cloud-Anbieter das System in einem angemessenen Zeitrahmen wieder zur Verfügung stellen kann.

„Ein klassischer ERP-Partner ist meistens nicht so groß, dass er diese Kompetenzen im Haus hat. Insofern gab es hier immer eine Diskrepanz zwischen denen, die sich um die Infrastruktur und Datenbank kümmern, und denen, die schlussendlich das ERP-Projekt umgesetzt haben. Natürlich gibt es das beim Thema Cloud auch. Aber spätestens, wenn ich an Dynamics365 denke, und ich mich um dieses Thema nicht mehr kümmern muss, weil es Teil des Office-365-Paketes ist und in der Microsoft Cloud ist, finde ich es gerade für kleinere Betriebe den richtigen Weg.“ (Interviewpartner 5, 2017)

Hinzu kommt, dass Großunternehmen, die sensible Daten im Unternehmen haben, sich das entsprechend kompetente Personal leisten, das auch in Katastrophenfällen eine schnelle Lösung liefern kann. Diese Ressourcen sind in KMU und Start-ups wenig bis gar nicht vorhanden, was dazu führt, dass vor allem die IT-Mitarbeiter die Cloud als eine Option sehen, um die Verantwortung für das ERP-System auszulagern. Dabei profitieren sie von der Erfahrung des Cloud-Anbieters, dessen Kerngeschäft es ist, sich um die Administration von IT-Systemen zu kümmern.

Die Meinung, dass die Verantwortung bei einem ERP-System in der Cloud bis zu einem gewissen Grad abgegeben wird, teilen alle Interviewpartner. Interessant ist dabei dennoch die Sicht der IT-Leiter, die darauf hinweisen, dass die Cloud damit nicht alle Probleme löst, sondern weiterhin

eine Administration notwendig ist. Es wird dennoch kompetentes Personal benötigt wird, das im Katastrophenfall die richtigen Maßnahmen setzt, um die Funktionen des ERP-Systems wiederherzustellen. Dass durch die Auslagerung jedoch quasi kein Risiko mehr für die Hardware getragen wird, bejahen nicht nur die IT-Mitarbeiter, sondern auch die IT-Leiter. Die IT-Leiter sehen dabei aber vor allem bei Großunternehmen keinen Vorteil, da diese Risiken mit entsprechender Vorbereitung auch selbst minimiert werden können.

> *„Wenn uns ein Core-Switch eingeht und alle Server sind weg, dann kann ich es vielleicht anders routen oder irgendwas tricksen. Dann habe ich einen kurzen Ausfall, aber kann selber etwas tun. Das ist dann ein Gefühl, wo man sich dann nicht mehr ganz so hilflos vorkommt. Man ruft dann bei einem Call-Center an und landet in der Warteschleife. In der Zwischenzeit gehen die Applikationen nicht. Das ist ein Gefühl der Hilfslosigkeit, wenn man es nicht in der Hand hat. Hier kann ich drei Leute hinschicken und sagen, dass sie sich das anschauen sollen. Aber das machen die Anbieter ja auch, das muss man ehrlich sagen." (Interviewpartner 2, 2017)*

Cloudbasierte ERP-Systeme – KMU und Start-ups vs. Großunternehmen

Diese Kategorie behandelt den Unterschied zwischen KMU und Start-ups auf der einen und Großunternehmen auf der anderen Seite. Von Bedeutung ist hier vor allem, für welche Art von Unternehmen ein ERP-System in der Cloud geeignet ist und für welches nicht. Bei den Interviewpartnern herrschte bei diesem Thema eine klare Meinung. Während die Cloud für KMU und Start-ups als optimale Lösung erscheint, so ist sie für Großunternehmen wenig geeignet.

KMU haben das Problem, dass sich die IT bei vielen verschiedenen Schnittstellen und Programmen zu einem komplexen Konstrukt entwickeln kann. Zusätzlich muss dafür Sorge getragen werden, dass die Daten geschützt sind und es Vorkehrungen für Katastrophenfälle gibt. Um dies alles gewährleisten zu können, fehlen den KMU jedoch die Ressourcen. Hier kommt die Cloud ins Spiel. Wird die IT-Infrastruktur in die Cloud verlegt, so muss von Seiten des Unternehmens nur noch die Administration sichergestellt werden und Risiken werden dabei zum Anbieter der Cloud weitergeschoben. Auf diese Art und Weise ist es auch für KMU leicht möglich, eine sichere IT-Infrastruktur zu haben, die besser geschützt ist als im eigenen Rechenzentrum und weniger Ressourcen aus dem eigenen Unternehmen benötigt.

Selbiges gilt für Start-ups, die in der Anfangsphase wenig Zeit für IT haben und diese dann in die Cloud auslagern können, in der sich andere Personen um die Infrastruktur kümmern. Den größten Vorteil für KMU und Start-ups bildet dabei die Skalierbarkeit in alle Richtungen. Gerade bei Start-ups kann es leicht passieren, dass die Größe sich innerhalb kurzer Zeit rasant verändert und die Mitarbeiterzahl innerhalb von wenigen Jahren von beispielsweise 5 auf 40 wächst. In solchen Fällen werden in der Cloud keine zusätzlichen Ressourcen benötigt, so wie es in einem Rechenzentrum der Fall wäre. Gerade in der heutigen Zeit, in der IT sich in Richtung Serviceorientierung entwickelt, stellt die Cloud damit ein einfaches Mittel dar, um den Anforderungen gerecht zu werden.

> *„Immer mehr kleinere Firmen werden dazu übergehen müssen, mehr in Richtung Serviceorientierung zu gehen und da helfen ERP-Systeme. Es wird sich eine kleine*

> *Firma auch nicht immer leisten können, dass sie das selbst betreibt. Deswegen wird sie auf Cloud-ERP-Systeme setzen.“ (Interviewpartner 1, 2017)*

Werden die Vorteile für KMU und Start-ups betrachtet, wird schnell ersichtlich, warum die Cloud für Großunternehmen nur bedingt einen Vorteil mit sich bringt. Im Gegensatz zu den KMU und Start-ups sind in den Großunternehmen genügend Ressourcen vorhanden, um eine sichere und gut geschützte IT-Infrastruktur betreiben zu können. Großunternehmen heben sich vor allem dadurch ab, dass die Skalierbarkeit so gut wie keine Rolle spielt. Trotz kleinerer Schwankungen, wie zum Beispiel vermehrter Urlaub im Sommer/Winter, ist die IT so gut aufgestellt, dass eine Cloud keinen Vorteil bringt und daher nicht benötigt wird. Dies gilt vor allem für Produktionsunternehmen, die bereits mehrere Jahre am Markt sind und sich als Großunternehmen etabliert haben. In diesen Unternehmen ist die IT so gut wie kein Problem, da das Unternehmen über Jahre hinweg stabil funktioniert und keine großen Änderungen innerhalb kurzer Zeit erfolgen. Natürlich gibt es auch Ausnahmen, vor allem durch die Übernahme von anderen Unternehmen. Dies stellt jedoch ebenfalls keinen entscheidenden Grund für einen Gang in die Cloud dar.

> *„Bei den Veranstaltungen habe ich mir immer gedacht wovon die reden, aber zum Glück war ich nicht der einzige. Die gestandenen IT-Leiter haben gesagt, dass sie mal schauen und warten oder ein bisschen probieren. Wenn man aber nicht wie Start-ups den Anlassfall hat, dann würde ich es nicht so sehen.“ (Interviewpartner 3, 2017)*

Zusätzlich unterscheiden sich die Großunternehmen dahingehend, dass in der IT um einiges leichter auf Reserve eingekauft werden kann als in KMU und Start-ups. Dies liegt am weitaus größeren Budget, das einem Großunternehmen zur Verfügung steht. Auch hier zeigt sich der Vorteil einer Cloud für KMU und Start-ups. Anstatt sich um die Wartung der IT-Infrastruktur zu kümmern, wird diese ausgelagert und der Cloud-Anbieter trägt die Verantwortung. Die IT-Leiter sehen in der Wartung dabei keinen großen Aufwand, weshalb IaaS für sie auch nicht in Frage kommt, weil es nur Kosten verursacht und keinen Nutzen bringt.

Dass der Unterschied zwischen KMU bzw. Start-ups und Großunternehmen vor allem in Bezug auf die Kosten deutlich wird, merkte insbesondere einer der Interviewpartner an. Laut ihm ist IT-Sicherheit für KMU und Start-ups zwar relativ einfach zu erreichen, hat aber auch seinen Preis. So bieten mehrere Datenbankhersteller, wie zum Beispiel Oracle, eine Verschlüsselung auf Datenebene an. Dies führt beispielsweise dazu, dass ein Softwareentwickler zwar Zugriff auf alle Datenbanken hat, aber in den Spalten, die Unternehmenskennzahlen beinhalten, nur verschlüsselte Werte sieht. Auch wenn der Erwerb für die Lizenzen solcher Systeme bei mehreren Datenbankherstellern möglich ist, müssen dennoch die hohen Kosten bewältigt werden können.

Allerdings spielen auch bei Großunternehmen die Kosten eine Rolle. Aus den bisherigen Kategorien sind bereits einige Bedenken in Bezug auf einen Betrieb des ERP-Systems in der Cloud aufgekommen. Die Kombination dieser Bedenken und der Kosten, die eine Umstellung mit sich bringt, stellt für IT-Leiter in Großunternehmen ein zu hohes Risiko dar.

„Die KMU werden eher dazu genötigt auf Cloud umzusteigen und werden dies aufgrund der Kostenthematik viel eher tun. Denn der Fixkostenanteil ist dort viel erdrückender als bei einem Konzern. Bei Konzernen gibt es viel mehr Ressourcen […]. Dort gibt es keine Probleme, dass man fähige Leute findet und Geld ist auch vorhanden. [...] Das können sich KMU nicht leisten. Die KMU werden viel sparsamer mit der Hardware umgehen und wenn sie es brauchen, sich flexibel die Ressourcen hochdrehen lassen in der Cloud. [...] Ein Konzern tut sich viel leichter beim Serverkauf und stellt viel leichter einen Server hin, der nichts tut. Ein KMU kann das hingegen nicht tun.“ (Interviewpartner 2, 2017)

„Die Erfahrung hat gezeigt, dass sich vor allem KMU mehr mit der Cloud anfreunden können, da bei Großunternehmen die Ressourcen ohnehin schon da sind und man keine direkten Vorteile davon erkennen kann. Die fühlen sich auch sicherer, wenn sie alles in der eigenen Hand halten.“ (Interviewpartner 5, 2017)

4.3.10 Inhaltsanalytische Gütekriterien

Damit die Inhaltsanalyse als wissenschaftliche Forschungsmethode anerkannt wird, muss sie sich Gütekriterien stellen. Wegen der Kritik an den ‚klassischen' Gütekriterien (Validität und Reliabilität) wurden für die qualitative Forschung eigene Gütekriterien eingeführt. Dabei teilen sich die Kriterien in sechs Bereiche, die auf die vorliegende Inhaltsanalyse geprüft werden sollen (vgl. Mayring, 2002).

Verfahrensdokumentation: „Das schönste Ergebnis ist wissenschaftlich wertlos, wenn nicht das Verfahren genau dokumentiert ist, mit dem es gewonnen wurde.“ (Mayring, 2002) Den Nachweis über die durchgeführte Forschung stellt dieses Dokument dar. Im Zuge des Dokumentes wurden alle Vorgehen erläutert und nachvollziehbar gemacht. Trotz genau angepasster Methoden und Techniken ist es möglich, das Vorgehen auf die gleiche Art und Weise zu wiederholen.

Argumentative Interpretationsabsicherung: Anders als bei der qualitativen Forschung, bei der die Statistiken und Zahlen eine klare Interpretation zulassen, ist es notwendig, dass bei der qualitativen Forschung das Interpretieren des Materials mit der Hilfe von Argumenten durchgeführt wird. Dieses Gütekriterium ist unter anderem ein Grund für die Theoriegeleitetheit der Analyse (vgl. Mayring, 2002). Im Zuge der Interpretationen wurde besonders darauf geachtet, diese schlüssig zu halten, wobei die Theorie eine Unterstützung dafür war. Durch die Verfahrensdokumentation lassen sich die Interpretationen überprüfen.

Regelgeleitetheit: Die Freiheiten der qualitativen Forschung wurden in dieser Arbeit bereits hinreichend erläutert. Dennoch mussten auch hier immer wieder gewisse Regeln für einzelne Schritte festgelegt werden. Dies ist genau das, was Mayring (2002) unter Regelgeleitetheit versteht. Aus diesem Grund definiert er für viele Schritte ein Ablaufmodell, um ein systematisches Vorgehen gewährleisten zu können. Da sich die Inhaltsanalyse auf genau diese Ablaufmodelle von Mayring stützt, ist diese Gütekriterium ausreichend erfüllt.

Nähe zum Gegenstand: „Qualitative Forschung will an konkreten sozialen Problemen ansetzen, will Forschung für die Betroffenen machen und dabei ein offenes, gleichberechtigtes Verhältnis herstellen […] Durch diese Interessenannäherung erreicht der Forschungsprozess eine größtmögliche Nähe zum Gegenstand.“ (Mayring, 2002). Nach dieser Definition erfüllt das Vorgehen in dieser Arbeit das Gütekriterium, da die Interviews auf genau diese Art und Weise durchgeführt wurden.

Kommunikative Validierung: Unter kommunikativer Validierung wird die Überprüfung der Ergebnisse mit der Hilfe der befragten Personen verstanden. Nach Zusammenstellung der Ergebnisse können diese den befragten Personen vorgelegt werden. Erkennen sich die Interviewpartner in den Ergebnissen wieder, so gilt dieses Gütekriterium als erfüllt (vgl. Mayring, 2002). Die kommunikative Validierung wird im Zuge des nächsten Kapitels dargelegt.

Triangulation: Triangulation bedeutet, dass die Forschung mit verschiedenen Methoden und Techniken oder von verschiedenen Interpretern durchgeführt werden soll, um die Ergebnisse im Anschluss daran miteinander zu vergleichen. Dabei werden Stärken und Schwächen der einzelnen Verfahren aufgezeigt, die aber alle zu den gleichen Ergebnissen führen sollten. Mit diesem Gütekriterium ist es möglich, unterschiedliche Lösungswege zu finden (vgl. Denzin, 2006). Aufgrund der zeitlichen Beschränkung kann dieses Kriterium nicht erfüllt werden.

4.4 Zusammenfassung der Ergebnisse

In diesem Kapitel wurden die Ergebnisse der zusammenfassenden Inhaltsanalyse vorgestellt, die das Material auf die wesentlichen Punkte reduziert hat. Den substanziellen Teil dabei stellte die Interpretation der Ergebnisse in Bezug auf die Kategorien dar. Bei den Kategorien fiel vor allem auf, dass von den drei Grundsätzen der IT-Sicherheit nicht alle als Kategorie abgebildet wurden. Während die Verfügbarkeit und Vertraulichkeit zu den Schwerpunkten gehörten, wurde Integrität kaum erwähnt. Dies liegt daran, dass Integrität nichts mit der Unterscheidung zwischen Rechenzentrum und Cloud zu tun hat. Bedenken hinsichtlich der Integrität beziehen sich bei den befragten Personen rein auf die Software selbst.

Aus der Analyse ergibt sich auch, dass IT-Leiter der Cloud wesentlich kritischer gegenüberstehen und hier auf ihr Bauchgefühl setzen. Sie fühlen sich wohler, wenn sie die Daten selbst verwalten können und keinem anderen Unternehmen anvertrauen müssen. Die IT-Leiter sehen in ihrem Unternehmen ausreichend Kompetenzen und haben gleichzeitig die Ressourcen, um selbst für hohe IT-Sicherheit zu sorgen. Hier wird vor allem der Unterschied zwischen KMU/Start-ups und Großunternehmen deutlich. Durch die Cloud kann ein KMU/Start-up das ERP-System und deren IT-Infrastruktur auslagern und muss sich um weitaus weniger Dinge kümmern als bei einem eigenen Rechenzentrum.

Die Interviews zeigen auch, dass es Bedenken gibt, die völlig unabhängig vom ERP-System und der Unternehmensgröße sind. Zum Beispiel wurde von den befragten Personen richtig erkannt, dass bei der Nutzung einer Cloud, die nicht selbst betrieben wird, eine dauerhafte und performante Internetverbindung bestehen muss. Hier hat sich gezeigt, dass nicht jedes Unternehmen aufgrund seiner örtlichen Lage diese Voraussetzungen für die IT-Abteilung

zufriedenstellend erfüllen kann. Zusätzlich kann die Cloud ein attraktiveres Angriffsziel darstellen, was vor allem große Cloud-Anbieter, wie zum Beispiel Google oder Microsoft, betrifft. Dabei muss das Unternehmen nicht einmal das primäre Ziel sein.

Besonders KMU müssen sich in Zukunft mit der DSGVO auseinandersetzen, die zahlreiche, auch für die Cloud relevante Einschränkungen mit sich bringt. Anders als die Großunternehmen, die ohnehin schon ein Risikomanagement betreiben, werden KMU hier vor große Herausforderungen gestellt. Um trotz DSGVO die Daten in die Cloud zu legen, braucht es deshalb auch Vertrauen in den Cloud-Anbieter, der womöglich dauerhaft Zugriff auf die Unternehmensdaten hat.

Im Zuge der Inhaltsanalyse konnten somit mehrere Bedenken gegenüber ERP-Systemen in der Cloud hinsichtlich der IT-Sicherheit identifiziert werden. Zur leichteren Nachverfolgbarkeit werden die in Tabelle 4-1 dargestellten Bedenken mit ihrer jeweiligen Kategorie verknüpft.

Nr.	Bedenken	Kategorie
1	Es ist nicht bekannt, wo bei der Public Cloud die Daten liegen.	Bewertung des gegenwärtigen Stands der Technik hinsichtlich Cloud
2	Bei der Cloud ist unklar, wie im Hintergrund alles genau funktioniert.	Bewertung des gegenwärtigen Stands der Technik hinsichtlich Cloud
3	Die Cloud kann nicht so gut geschützt werden wie das eigene Rechenzentrum.	Bewertung des gegenwärtigen Stands der Technik hinsichtlich Cloud
4	Die Umstellung des aktuellen ERP-Systems in die Cloud bringt mehr Kosten/Aufwand mit sich als Nutzen.	Gegenwärtige IT-Infrastruktur im Unternehmen
5	Die Datenschutz-Grundverordnung kann mit der Cloud nicht eingehalten werden.	Rechtliche Aspekte von ERP-Systemen in der Cloud
6	Die Cloud benötigt eine ausfallssichere Internetverbindung.	Verfügbarkeit von IT-Systemen
7	Die Cloud benötigt eine performante Internetverbindung.	Verfügbarkeit von IT-Systemen
8	Es muss darauf vertraut werden, dass der Cloud-Anbieter das ERP-System im Katastrophenfall in annehmbarer Zeit wieder zum Laufen bringt.	Verfügbarkeit von IT-Systemen
9	Es ist wesentlich wahrscheinlicher, dass ein Hacker die Cloud angreift als das Rechenzentrum eines Unternehmens.	Vertraulichkeit in IT-Systemen

10	Der Anbieter der Cloud kann die Daten jederzeit mitlesen.	Vertraulichkeit in IT-Systemen
11	Mitarbeiter von Cloud-Anbietern können unbefugt die Daten weitergeben/-verkaufen.	Vertrauen in Anbieter der Cloud vs. die IT-Abteilung im Unternehmen
12	Die Vorteile der Cloud (z. B. Skalierbarkeit, Flexibilität) haben keinen Nutzen.	Cloudbasierte ERP-Systeme – KMU und Start-ups vs. Großunternehmen

Tabelle 4-1 Bedenken hinsichtlich der IT-Sicherheit bei ERP-Systemen in der Cloud

Im nächsten Kapitel sollen diese Bedenken priorisiert werden, um im Anschluss daran die kritischsten Bedenken zu vermindern.

5 VERMINDERUNG DER BEDENKEN

Im letzten Kapitel wurden die Bedenken hinsichtlich der IT-Sicherheit bei ERP-Systemen in der Cloud herausgestellt. In diesem Kapitel soll nun versucht werden, diese Bedenken zu priorisieren und im Anschluss daran die wichtigsten davon näher zu betrachten. Im Zuge dieser Betrachtung liegt das Hauptaugenmerk auf der Verminderung der Bedenken, sodass zu jedem davon zumindest ein Lösungsvorschlag vorliegt.

5.1 Priorisierung

Die Priorisierung der Bedenken erfolgte durch eine Rückfrage bei den Interviewpartnern, wodurch ein wissenschaftliches Vorgehen sichergestellt werden sollte. Den Interviewpartnern wurde dafür per E-Mail die Liste an Bedenken geschickt, die sie von 1 bis 12 bezüglich deren Priorität einschätzen sollten. Für das größte Bedenken sollte die 1 und für das kleinste Bedenken sollte die 12 verwendet werden. Konnte der Interviewpartner ein Bedenken nicht als Problem identifizieren, so konnte er dieses einfach auslassen.

Durch die Priorisierung der Bedenken mit Hilfe der Interviewpartner wurde unter anderem das Gütekriterium der kommunikativen Validierung erfüllt. Die Ergebnisse der qualitativen Inhaltsanalyse wurden den Interviewpartnern somit indirekt nochmals zur Überprüfung übergeben. Da die Interviewpartner jedoch keine Bedenken verworfen haben, kann dieses Gütekriterium als erfüllt angesehen werden.

Nachdem die Interviewpartner die Bedenken priorisiert hatten, wurden pro Bedenken die Mittelwerte über deren Priorisierung gebildet. Mit dieser Methode sollte gesichert werden, dass der Meinung jedes Interviewpartners die gleiche Bedeutung zukommt. Das Bedenken mit dem niedrigsten Mittelwert stellte dadurch das größte Bedenken über alle Interviewpartner hinweg dar.

Die Priorisierung ergab, dass das Vorhandensein einer performanten Internetverbindung das größte Bedenken ist, das die Interviewpartner hinsichtlich der IT-Sicherheit bei ERP-Systemen in der Cloud haben. Des Weiteren ist in Abbildung 5-1 ersichtlich, dass das zweitgrößte Bedenken dem Vertrauen gegenüber dem Cloud-Anbieter gilt. Die Zahl vor dem Bedenken stellt die Referenz zum vollständig formulierten Bedenken in Tabelle 4-1 dar. Zusätzlich befindet sich im Anhang eine detaillierte Tabelle, die die Priorisierung pro Interviewpartner und Bedenken zeigt, sodass die endgültige Priorisierung nachvollziehbar ist.

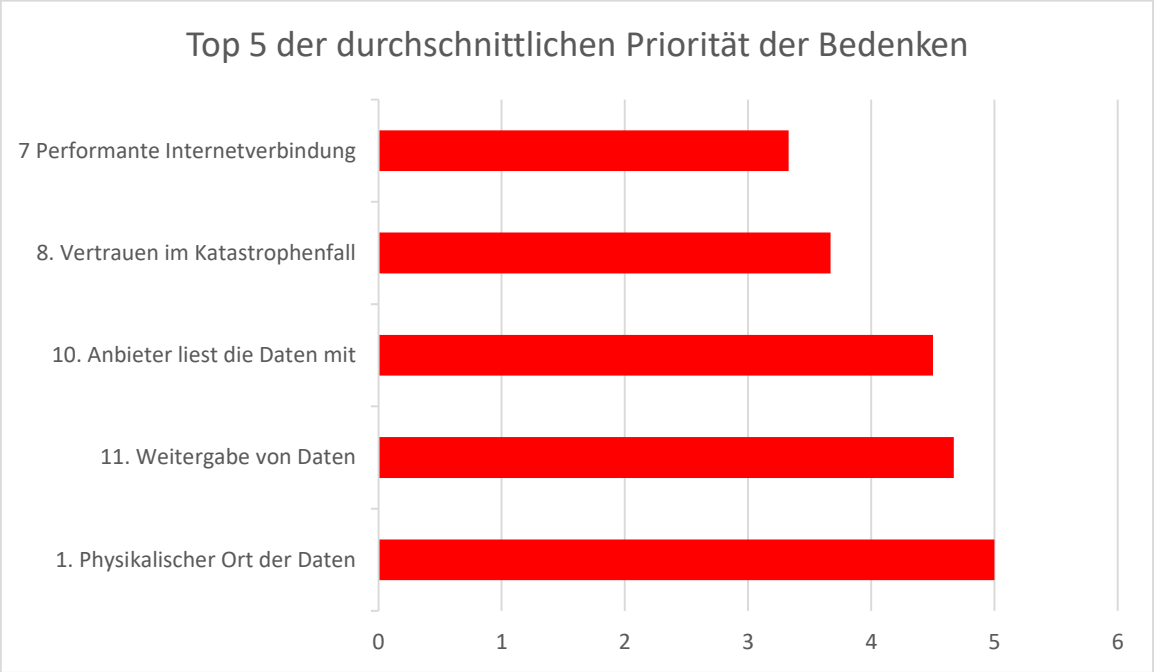


Abbildung 5-1 Priorisierte Bedenken hinsichtlich der IT-Sicherheit bei ERP-Systemen in der Cloud

Wie bereits in der Einführung dieser Arbeit erwähnt, sollen nicht alle Bedenken im Zuge dieser Arbeit vermindert werden. Dies war unter anderem der Grund für die Priorisierung. Im nächsten Schritt werden deswegen die fünf kritischsten Bedenken näher betrachtet und für diese ein Verminderungsversuch unternommen.

5.2 Bedenken 1 – Performante Internetverbindung

Bei einem ERP-System in der Cloud stellt das Vorhandensein einer performanten Internetverbindung das größte Bedenken hinsichtlich der IT-Sicherheit dar. Damit steht vor allem der IT-Sicherheitsgrundsatz ‚Verfügbarkeit' im Mittelpunkt. Das Bedenken scheint auf den ersten Blick einleuchtend, da sich im Gegensatz zur Cloud das eigene Rechenzentrum bereits in einem performanten Netzwerk befindet und die Aufrüstung damit in der eigenen Hand liegt. Bei der Cloud hingegen wird ein Zugriff nach Außen benötigt, ausgenommen es wird eine Private Cloud im herkömmlichen Sinn verwendet, die im eigenen Rechenzentrum betrieben wird. Dies wäre bereits die erste Möglichkeit, um diesem Bedenken entgegenzuwirken. Wie aus dem letzten Kapitel bereits bekannt ist, soll die Cloud vor allem für KMU eine Entlastung dahingehend sein, dass die Pflege der IT-Infrastruktur ausgelagert werden kann. Aus diesem Grund liegt hier der Fokus auf dem eigentlichen Bedenken: der Sicherstellung einer performanten Verbindung zum Cloud-Anbieter.

Das Problem, das durch ein ERP-System in der Cloud auftritt, ist, dass der Internetverkehr rapide ansteigt, da die Verbindung zum ERP-System nun über das Internet läuft. Darauf sind viele Unternehmensnetzwerke jedoch nicht ausgelegt, da die Software im eigenen Netzwerk verfügbar ist (vgl. Zscaler, 2017).

Um dieses Problem zu lösen, haben sich die Cloud-Anbieter ein System ausgedacht, das den Zugriff auf die Cloud-Dienste über eine private Netzwerkverbindung anstatt über das öffentliche Internet gewährleistet. Der Unterschied zur herkömmlichen Verbindung ins Internet besteht dabei darin, dass der Nutzer nicht über mehrere Stationen zum gewünschten Endpunkt geleitet wird, sondern über eine direkte Verbindung. Als Beispiel sei an dieser Stelle der Cloud-Anbieter Amazon genannt, der dies mit seinem Produkt ‚AWS Direct Connect' ermöglicht (vgl. Interxion, 2015).

Mit AWS Direct Connect ist es möglich, die Daten über eine private Netzwerkverbindung, getrennt vom öffentlichen Internet, in die Cloud zu übertragen und abzuholen. Dies bietet für Unternehmen einige Vorteile, die sich unter anderem auf die Performanz auswirken (vgl. Amazon, 2017a):

- Reduzierung der Bandbreite beim Internetserviceprovider
- Konsistenz in der Netzwerklatenz
- Nichtöffentliche Verbindung zu den Daten (vgl. Amazon, 2017a)

Besonders der zweite Punkt trägt zu einer Verminderung dieses Bedenkens bei. Während Latenzzeiten und Bandbreiten über das Internet variieren können, können diese so konstant gehalten werden, was zu einer vorhersagbaren Übertragungsgeschwindigkeit führt. Zusätzlich können diese Punkte für Unternehmen Teil eines sogenannten Service Level Agreements (SLA) sein, das festlegt, mit welcher Geschwindigkeit die Übertragung stattfinden muss. Auf diese Art und Weise kann eine performante Internetverbindung sichergestellt werden (vgl. Interxion, 2015).

Die gleiche Art der Lösung gibt Microsoft mit der ‚ExpressRoute' in der Azure Cloud. Hier ermöglichen Internetserviceprovider über die Multi-Protocol-Label-Switching- (MPLS-)Technologie eine direkte Verbindung zur Cloud. MPLS stellt dabei eine Datenübertragungstechnik dar, die Daten über den kürzesten Weg zum empfangenden Gerät bringt, anstatt das Internet zu nutzen. Der Vorteil der besseren Performanz wird dadurch erreicht, dass auf diese Art und Weise komplexe Zwischenstationen und Weiterleitungen vermieden werden (vgl. Klaffenbach, Damaschke & Michalski, 2017).

Das erste Bedenken kann somit als vermindert angesehen werden, da entsprechende Lösungsansätze vorhanden sind.

5.3 Bedenken 2 – Vertrauen im Katastrophenfall

Bei diesem Bedenken geht es darum, dass dem Cloud-Anbieter dahingehend vertraut werden muss, dass auch beim Ausfall eines Servers oder einer Datenbank der Betrieb sichergestellt ist. Während die IT in den Unternehmen für diesen Fall präventiv Backups und Spiegelungen der Server erstellt, muss hier darauf vertraut werden, dass der Cloud-Anbieter ebenfalls solche Sicherheitsmaßnahmen vornimmt.

Zunächst muss grundsätzlich unterschieden werden, ob als Betriebsmodell der Cloud SaaS, PaaS oder IaaS verwendet wird. Mit der Ausnahme von SaaS kann durch die Verwendung von mehreren Cloud-Servern ebenfalls die gewünschte Redundanz erzeugt werden, die zur

Ausfallssicherheit beiträgt. Dennoch bleibt die Sorge, dass im schlimmsten Fall alle Server, auf denen die Daten liegen, gleichzeitig ausfallen. Aus diesem Grund stellen die Cloud-Anbieter Mechanismen zur sogenannten Data Loss Prevention (DLP) zur Verfügung, die einen Datenverlust in der Cloud verhindern sollen. Sicherheits- und Netzwerkunternehmen wie Symantec, McAfee oder Cisco haben darüber hinaus Lösungen für DLP über ein gesamtes Netzwerk entwickelt (vgl. Kazim & Zhu, 2015).

Bei Notfallwiederherstellungen in der Cloud kann das Unternehmen bereits konkrete Vorkehrungen treffen, um die Betriebsbereitschaft des ERP-Systems nach einem Serverausfall wiederherstellen zu können. Die Zeit des Ausfalls kann unter anderem durch die Art des Wiederherstellungsmodells selbst festgelegt werden. Bei den Modellen wird grundsätzlich in Hot, Cold und Warm Standby unterschieden (vgl. Schröder & Schulte, 2011).

In allen drei Modellen ist es möglich, das gesamte System ohne Datenverlust auf einem anderen Server weiterhin zu betreiben. Bei einem Hot Standby wird das laufende ERP-System auf einem zweiten Server zeitgleich betrieben. Kommt es zu einem Ausfall des Hauptservers, so übernimmt der zweite Server den Betrieb des ERP-Systems. Da der zweite Server laufend über aktuelle Daten verfügt und bereits konfiguriert und gestartet ist, muss nur noch im Hintergrund eine Umschaltung auf diesen Server erfolgen. Im Optimalfall wird dies automatisch erledigt, sodass für das Unternehmen kein merkbarer Ausfall spürbar ist. Somit handelt es sich bei einem Hot Standby um einen zweiten Server, der jederzeit einsatzbereit ist und die Tätigkeiten des eigentlichen Servers übernehmen kann (vgl. Schröder & Schulte, 2011).

Das zweite Modell ist ein Cold Standby. Im Gegensatz zu einem Hot Standby wird der zweite Server nicht laufend betrieben und aktualisiert. Kommt es nun bei einem Cold Standby zu einem Ausfall des Servers, so muss der zweite Server erst gestartet werden und es müssen ggf. Daten eingespielt werden, um einen aktuellen Datenstand zu besitzen. Der Vorteil bei diesem Modell liegt darin, dass der zweite Server nicht ständig in Betrieb ist und dadurch einen geringeren Verschleiß aufweist (vgl. Schröder & Schulte, 2011).

Bei einem Warm Standby handelt es sich um einen Mix aus beiden Varianten. Hier ist der zweite Server wie bei einem Hot Standby dauerhaft in Betrieb, die Daten liegen jedoch auf einem anderen Server. Dadurch müssen im Notfall die Daten erst in den zweiten Server eingespielt werden. Abbildung 5-2 zeigt nochmals die vorhandenen Verfügbarkeitsmodelle (vgl. Whitehouse & Buffington, 2012).

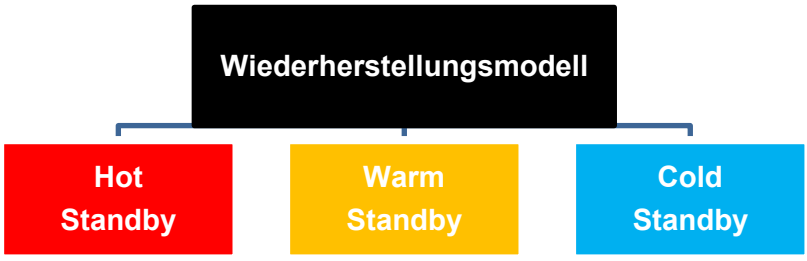


Abbildung 5-2 Notfallwiederherstellungsmodelle

Durch die Möglichkeiten dieser Modelle lässt sich jederzeit die Verfügbarkeit des ERP-Systems in der Cloud steuern, da die Ausfallszeiten selbst bestimmt werden können. Die Zeit, die es schlussendlich für die Wiederherstellung des primären Systems braucht, sollte zusätzlich vertraglich festgelegt werden.

5.4 Bedenken 3 – Anbieter liest Daten mit

In der Cloud wird die Infrastruktur von einem anderen Unternehmen zur Verfügung gestellt, was die Frage aufwirft, ob der Cloud-Anbieter dadurch jederzeit in der Lage ist, die Daten der Kundinnen und Kunden mitzulesen. Schiefer (2012) unterscheidet dabei aus der Perspektive der Hardware ein dreistufiges Modell:

1. Hardware des Besitzers
2. Hardware eines lokalen Cloud-Anbieters
3. Hardware im Rechenzentrum des Cloud-Anbieters (vgl. Schiefer, 2012)

In jeder Stufe wird dabei die Vertrauenswürdigkeit geringer. Auf der Hardware, die selbst verwaltet wird, können die Daten jederzeit so gut es geht geschützt werden und das Unternehmen ist dafür selbst verantwortlich. Bei der Hardware des lokalen Cloud-Anbieters, die zum Beispiel aus rechtlichen Gründen benötigt wird, ist zwar durch Zertifizierungen ein gewisses Vertrauen vorhanden, es ist jedoch geringer als bei der ersten Stufe. In dieser Stufe besteht eine zusätzliche Absicherung mit Verträgen, was das Vertrauen etwas bestärken soll. In der letzten Stufe, dem eigentlichen Cloud-Anbieter, ist die Vertrauenswürdigkeit kaum gegeben. Hier basiert der Schutz der Daten auf Vertrauen, da mit dem Anbieter weder eine vertraglich noch irgendeine andere Art der Verbindung besteht. Ein Beispiel hierfür wäre die Azure Cloud von Microsoft als dritte Stufe, ein Microsoft-Partner im eigenen Land, der die Azure Cloud vertreibt, als zweite Stufe und das Unternehmen mit seinen Angestellten als erste Stufe (vgl. Schiefer, 2012, S. 7).

Grundsätzlich gibt es eine einfache Möglichkeit, um das unbefugte Mitlesen der Daten zu verhindern: Verschlüsselung. Mit Verschlüsselungsalgorithmen wie zum Beispiel dem AES können Daten so sicher verschlüsselt werden, dass ein unberechtigter Zugriff nicht möglich ist, es sei denn, der Angreifer besitzt den Entschlüsselungscode (vgl. Prabhu & Paramesha, 2017).

Die Konsequenz daraus ist, dass die Daten unter Zuhilfenahme des entsprechenden Schlüssels jederzeit gelesen werden können. Prabhu und Paramesha (2017) schlagen vor, den Schlüssel nicht in der Cloud zu hinterlegen, sondern ihn selber zu verwalten. Damit wäre eine Speicherung der Daten gewährleistet, die verhindert, dass unbefugte Personen, wie auch die Cloud-Anbieter, Zugriff auf diese haben. Hier besteht allerdings das Problem, dass nicht alle Anbieter diese Möglichkeit zur Verfügung stellen.

Große Cloud-Anbieter wie Amazon, Microsoft oder Google sind bezüglich der IT-Sicherheit transparent, was dazu führt, dass sie den Ort des Schlüssels für den AES bekannt geben. In Tabelle 5-1 sind Beispiele für Cloud-Anbieter und deren Produkte aufgelistet, die einen Überblick verschaffen sollen, welcher Cloud-Anbieter die Verwaltung des AES-Schlüssels selbst übernimmt.

Cloud-Anbieter	Produkt	Verwaltung des AES-Schlüssels
Amazon	AWS	Selbstverwaltung oder Key Management Service (KMS) (vgl. Amazon Web Services, 2016)
Google	Google Cloud Platform	Selbstverwaltung oder Google (vgl. Google, 2017)
Microsoft	Azure	Microsoft (vgl. Microsoft, 2017a)

Tabelle 5-1 Verwaltung der AES-Schlüssel bei verschiedenen Cloud-Anbietern

Somit gibt es Cloud-Anbieter, die über die Verschlüsselung sicherstellen, dass die Daten ohne den AES-Schlüssel nicht unbefugt mitgelesen werden können. An dieser Stelle sei jedoch erwähnt, dass auch hier dem Cloud-Anbieter ein gewisses Vertrauen entgegengebracht werden muss. So heißt es beispielsweise in der Dokumentation von Google: „If you provide a customer-supplied encryption key, Cloud Storage does not permanently store your key on Google's servers or otherwise manage your key." (Google, 2017) Ob dies nun wirklich der Realität entspricht, kann natürlich nicht nachgewiesen werden. Selbiges trifft auf Amazon zu, das in der Dokumentation versichert, dass Mitarbeiter keinen Zugriff auf die Schlüssel im System haben:

> *„Wie vorstehend dargelegt, hat AWS keine Kontrolle darüber, welche Art von Inhalten der Kunde bei AWS speichert und zu welchem Zweck dies geschieht. AWS hat keinen Einblick in diese Inhalte (einschließlich der Frage, ob diese Inhalte personenbezogene Daten enthalten). AWS kann die Betroffenen, deren personenbezogene Daten der Kunde in AWS gespeichert hat, nicht identifizieren und hat keinen Kontakt zu ihnen (mit Ausnahme der Fälle in denen die Daten sich auf den Kunden selbst beziehen). AWS kann daher den jeweiligen Betroffenen keine Informationen liefern. AWS ist nicht in der Lage, Daten, die auf AWS gespeichert sind, mit einer bestimmten Person in Verbindung zu bringen. Diese Information liegt ausschließlich in der Kontrolle des Kunden." (Amazon Web Services, 2014)*

Dieses Bedenken kann somit auf Basis der vorliegenden Informationen der Cloud-Anbieter zumindest als vermindert angesehen werden. Die Tatsache, dass dem Cloud-Anbieter bis zu einem gewissen Grad vertraut werden muss, besteht jedoch weiterhin.

5.5 Bedenken 4 – Weitergabe von Daten

Neben den Bedenken gegenüber der Technik hinter der Cloud bestehen auch Bedenken gegenüber den Angestellten der Cloud-Anbieter. Konkret geht es dabei um die Angst, dass die Daten des Unternehmens unbefugt von Angestellten des Cloud-Anbieters weitergegeben oder weiterverkauft werden könnten.

Dass diese Sorge nicht unberechtigt ist, zeigt ein erst kürzlich aufgetretener Fall in Asien, wo ein lizensierter Apple-Händler die Daten von Benutzerinnen und Benutzern an einen Interessierten veräußert hat. Auf diese Art und Weise konnten die Angestellten mehrere Millionen Dollar lukrieren. Apple hält sich bei diesem Fall zurück und eine Aussage, ob auch Daten aus der Apple-Cloud verkauft wurden, ist bisher noch nicht geklärt (vgl. Futurezone, 2017).

Die Verminderung dieses Bedenkens kann, da es sich um sogenannte ‚schwarze Schafe' handelt, die in jedem Unternehmen vorhanden sein können, nicht zur Gänze erfolgen. Stattdessen soll an dieser Stelle der Vergleich mit der Situation eines eigenen Rechenzentrums vorgenommen werden. So musste beispielsweise eine Schweizer Bank feststellen, dass ein einzelner Angestellter ausreicht, um Daten von den Unternehmensservern weiterzuverkaufen. Dabei wurden Daten von deutschen Unternehmen kopiert und dem deutschen Finanzamt übergeben, was dem Angestellten der Schweizer Bank über 1 Million Euro eingebracht hat (vgl. Süddeutsche Zeitung, 2013).

Wulkan, Condello und Pogemiller et al. (2017) zeigen zudem auf, dass immer mehr Personen versuchen, über das sogenannte ‚Dark Web' Angestellte dazu zu bewegen, sensible Daten aus ihrem Unternehmen zu verkaufen. Die Anzahl der Versuche hat sich innerhalb eines Jahres verdoppelt, wie auch aus Abbildung 5-3 hervorgeht.

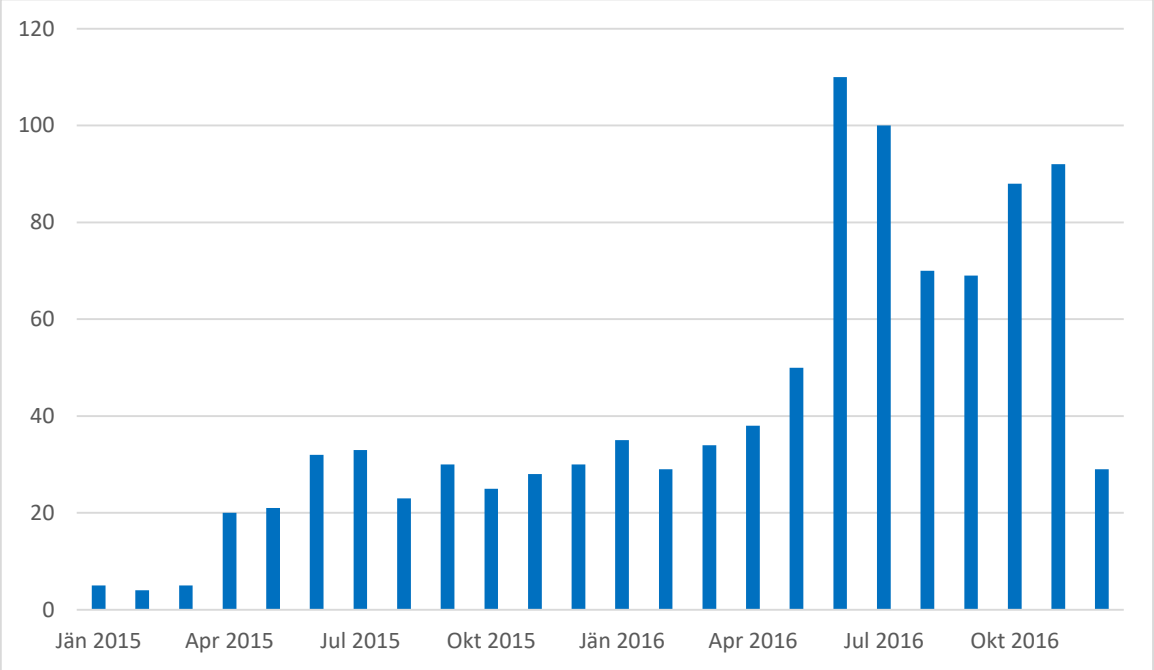


Abbildung 5-3 Anzahl der Versuche im Dark Web Daten zu kaufen (Wulkan et al., 2017)

Dieses Bedenken hängt somit nicht von der Unterscheidung zwischen Cloud oder Rechenzentrum ab, sondern kann als generelles Bedenken in der IT gesehen werden, dem alle Unternehmen mit sensiblen Daten ausgesetzt sind.

5.6 Bedenken 5 – Physikalischer Ort der Daten

Das letzte der kritischsten Bedenken, das in diesem Kapitel behandelt wird, hat mit der Sorge um den physikalischen Ort der Daten des ERP-Systems in der Cloud zu tun. Dabei geht es vor allem um die Angst dabei, wenn sich Daten an einem unbekannten Ort, der Cloud, befinden. Dieses Bedenken trifft abermals nur auf die Public Cloud zu. Wie aus den Interviews hervorgeht, gibt es für die Arten der Private Cloud bereits Konzepte, bei denen Unternehmen über den physikalischen Ort ihrer Daten informiert werden. Dadurch ist es auch jederzeit möglich, zur Festplatte, auf der die Daten liegen, zu gelangen. Somit ist jederzeit ein Nachweis über den Speicherort möglich.

Durch die DSGVO stehen Unternehmen nun generell vor der Herausforderung, dass sie nachweisen müssen, wo die Daten liegen. Vor allem die Übertragung der Daten in Drittländer wird dabei mit strengen Vorschriften geregelt. Dies wird von den Interviewpartnern bei einer Public Cloud als problematisch angesehen, da laut ihnen nicht genau gesagt werden kann, wo die Daten schlussendlich gespeichert werden. Nicht nur die juristische Seite ist dabei wichtig, sondern auch die Tatsache, dass es quasi keinen echten Zugriff auf die eigenen Daten des Unternehmens gibt, wenn nicht bekannt ist, wo sich die Server befinden.

Ein Blick auf die Angebote der großen Cloud-Anbieter zeigt, dass bei einer Public Cloud der physikalische Standort der Daten selbst ausgewählt werden kann, damit mögliche Richtlinien eingehalten werden können. Zu diesem Zweck weisen beispielsweise Amazon (2017b) und Lynch (2017) explizit auf die Sicherstellung der Einhaltung der Änderungen durch die DSGVO hin. Kunden der Cloud-Anbieter können den physikalischen Standort somit jederzeit selbst wählen und wissen dadurch auch bei der Public Cloud über die Lage der Daten Bescheid (vgl. Amazon Web Services, 2016). Wichtig dabei ist, dass eine Absicherung mit Verträgen vorgenommen und festlegt wird, dass die Daten vom Cloud-Anbieter nicht ohne weiteres in ein anderes Land verschoben werden dürfen.

Neben der Public Cloud gibt es ein weiteres Bereitstellungsmodell, das den physikalischen Standort der Daten nachvollziehbar macht. Im Gegensatz zu einer Public Cloud stellt die Outsourced Private Cloud sicher, dass ein Unternehmen seine eigene Hardware in der IT-Infrastruktur des Cloud-Anbieters bekommt. Damit ist gewährleistet, dass die Daten des Unternehmens getrennt von anderen Unternehmen abgelegt sind. Dies kann unter anderem durch Partner der Cloud-Anbieter umgesetzt werden, die einem Unternehmen eine Outsourced Private Cloud zur Verfügung stellen. Entschließt sich ein Unternehmen die Cloud auf diese Art und Weise zu betreiben, so wählt es im Normalfall einen Cloud-Anbieter aus dem eigenen Land aus. Dadurch wird vor allem die juristische Situation etwas entschärft, da sich der Cloud-Anbieter an die nationalen Gesetze halten muss (vgl. ACP, 2017).

6 DISKUSSION DER ERGEBNISSE

Da nun alle Ergebnisse bekannt sind, sollen diese auf die Fragestellung umgelegt werden. Im Anschluss daran werden die Ergebnisse interpretiert, um bestehende Unklarheiten aufzuzeigen, besonders bedeutsame Erkenntnisse hervorzuheben und die Bedeutung für die Wissenschaft zu erläutern. Als Abschluss erfolgen eine kritische Betrachtung der gesamten Arbeit, sowie ein Ausblick in die Zukunft.

6.1 Ergebnisse in Bezug auf die Fragestellung

Unter Betrachtung der Ergebnisse und Erkenntnisse, die in den letzten Kapiteln vorgestellt wurden, soll nun zunächst die Hypothese dieser Arbeit betrachtet werden. Die Nullhypothese dieser Arbeit lautete: ‚Bei einem ERP-System in der Cloud gibt es keine Bedenken hinsichtlich der IT-Sicherheit.' Diese Hypothese wird aufgrund der Ergebnisse verworfen, womit die Hypothesenprüfung erfolgreich war. Der Grund für die Verwerfung wird in Tabelle 4-1, die die Liste der zwölf Bedenken enthält, ersichtlich. Die Interviews und deren Analyse haben somit gezeigt, dass es Bedenken hinsichtlich der IT-Sicherheit gibt, wenn ein ERP-System in der Cloud betrieben wird. Dennoch sei an dieser Stelle erwähnt, dass es, vor allem bei Großunternehmen, ganz andere Gründe als den der IT-Sicherheit gibt, die das Betreiben des ERP-Systems in der Cloud verhindern. Der wohl bedeutendste Grund dafür ist die Angst, dass ein bestehendes und funktionierendes System angepasst werden muss, um in die Cloud zu kommen. Hier spielen vorrangig die Kosten und die Kundenzufriedenheit eine Rolle.

Da die Hypothese erfolgreich geprüft wurde, soll nun die Forschungsfrage ‚Welche Maßnahmen führen zu einer Verminderung der Bedenken im Bereich IT-Sicherheit bei der Einführung eines ERP-Systems in der Cloud?' beantwortet werden. Im Zuge der Arbeit wurden zwölf IT-Sicherheitsbedenken gegenüber ERP-Systemen in der Cloud eruiert, wovon die fünf kritischsten näher betrachtet wurden. Dabei stellte sich heraus, dass nicht alle Bedenken vollständig vermindert werden konnten, wie in Tabelle 6-1 dargestellt wird.

Bedenken	**Verminderung durch**
Die Cloud benötigt eine performante Internetverbindung.	Private Verbindung zur Cloud
Es muss darauf vertraut werden, dass der Cloud-Anbieter das ERP-System im Katastrophenfall in annehmbarer Zeit wieder zum Laufen bringt.	Auswahl des geeigneten Verfügbarkeitsmodells
Der Anbieter der Cloud kann die Daten jederzeit mitlesen.	Verschlüsselung der Daten

Mitarbeiter von Cloud-Anbietern können unbefugt die Daten weitergeben/-verkaufen.	Keine Verminderung möglich; hängt nicht direkt mit der Cloud zusammen
Es ist nicht bekannt, wo bei der Public Cloud die Daten liegen.	Physikalischer Ort der Daten in der Cloud ist wählbar

Tabelle 6-1 Verminderung der kritischsten Bedenken

Diese Ergebnisse lassen eine klare Antwort auf die Forschungsfrage zu. Bis auf das Bedenken, dass der Cloud-Anbieter die Daten des Unternehmens weiterverkauft, können für alle Bedenken Lösungsansätze bereitgestellt werden. Bei diesem einen Bedenken handelt es sich jedoch nicht um ein Risiko, das sich rein auf die Cloud beschränkt. Das Problem der sogenannten ‚schwarzen Schafe' kann in jedem Unternehmen auftreten, unabhängig davon wie und wo das ERP-System betrieben wird.

Um eine performante Internetverbindung sicherzustellen, bieten Cloud-Anbieter technische Möglichkeiten, um dies zu ermöglichen. Über eine eigene Verbindung, die nicht den Weg über mehrere Stationen nimmt, können eine direkte Kommunikation mit der Cloud und eine festgelegte und konstante Bandbreite sichergestellt werden. Auch das Bedenken, dass der Cloud-Anbieter das ERP-System im Katastrophenfall nicht wieder zum Laufen bekommt, kann mit Verweis auf die technischen Möglichkeiten der Cloud-Anbieter minimiert werden. Wie bereits bekannt, gibt es drei Verfügbarkeitsmodelle, wobei bei einem Hot Standby die Ausfallszeit auf ein paar Sekunden beschränkt werden kann. Somit können diese zwei Bedenken aus der IT-Sicherheitskategorie ‚Verfügbarkeit' mit den genannten Maßnahmen als vermindert angesehen werden.

Für das Bedenken ‚Der Anbieter der Cloud kann die Daten jederzeit mitlesen' kann mit der Verschlüsselung der Daten eine entsprechende Maßnahme gesetzt werden, die jedoch nicht gänzlich zufriedenstellend ist. Obwohl die Daten verschlüsselt sind, können diese mit dem dazugehörigen Code wieder entschlüsselt werden. Während Microsoft offen zugibt, dass sie den Schlüssel speichern (und somit jederzeit Zugriff auf die Daten haben), versprechen andere Cloud-Anbieter, dass dieser geheim bleibt und nicht gespeichert wird.

Das letzte Bedenken, das sich auf den physikalischen Ort der Daten bezieht, ist ebenfalls von den Cloud-Anbietern gelöst worden. Sobald die Hardware gemietet wird, kann ausgewählt werden, wo diese platziert werden soll. Eine weitere Variante ist die Nutzung eines nationalen Cloud-Anbieters, der seine Server im gleichen Land stehen hat, was vor allem rechtlich gesehen von Vorteil ist. Somit können bereits im Vorfeld geeignete Maßnahmen gesetzt werden, um jederzeit den physikalischen Ort der Unternehmensdaten zu kennen.

Werden nun alle Maßnahmen zusammengefasst und gegebenenfalls um weitere Bedenken erweitert, so kann daraus ein Konzept erstellt werden. Dieses Konzept kann den IT-Abteilungen vorgelegt werden, um IT-Sicherheitsbedenken für ein ERP-System in der Cloud bereits frühzeitig zu vermindern oder gar auszuräumen. Diese Art der Vorabinformation wurde unter anderem bereits von einem Interviewpartner erwähnt.

6.2 Interpretation der Ergebnisse

Besonders hervorzuheben in dieser Arbeit ist die Liste an konkreten Bedenken, die von den interviewten Personen geäußert wurden. In der Literatur finden sich in der Regel allgemeine Formulierungen, dass die Cloud zu unsicher ist und die Daten nicht geschützt sind. Aus dieser Arbeit geht klar hervor, was sich hinter diesen Aussagen verbirgt und wo die tatsächlichen Bedenken der IT-Abteilungen liegen. Zusätzlich konnte gezeigt werden, dass es zwar viele Bedenken, jedoch auch bereits Lösungsansätze von den Cloud-Anbietern gibt, um diesen Bedenken entgegenzuwirken.

Grundsätzlich muss aber gesagt werden, dass es auch einen gewissen Grad an Vertrauen braucht, der dem Cloud-Anbieter entgegengebracht werden muss. Es bleibt unklar, ob sich große Konzerne wie Google, Amazon oder Microsoft auch wirklich an das halten, was sie propagieren (beispielsweise, dass Google den Schlüssel zur Datensicherung nicht speichert). Da es jedoch nicht möglich ist, hinter die Türen der einzelnen Unternehmen zu blicken, bedarf es Vertrauen (oder einer rechtlichen Absicherung, soweit dies möglich ist), um seine Daten einem Cloud-Anbieter zu überlassen.

Bezogen auf die Problemstellung dieser Arbeit bedeutet es jedoch auch, dass zumindest bekannt ist, um welche Bedenken es sich konkret handelt, und dass die Cloud-Anbieter bereits Maßnahmen zur Verminderung gesetzt haben. In der Praxis bedeutet höhere Sicherheit allerdings auch immer einen gleichzeitigen Anstieg der Kosten, wodurch das Maß der IT-Sicherheit von einer Kosten-Nutzen-Abschätzung abhängt. Für die weitere Forschung bleibt nun zu prüfen, ob mit den Maßnahmen wirklich eine Verminderung der Bedenken stattfinden kann.

6.3 Kritische Betrachtung der Arbeit

Besonders kritisch müssen in dieser Arbeit die Ansätze zur Verminderung der Bedenken betrachtet werden. Dabei wurde so vorgegangen, dass, unabhängig von Anbietern und Technologie, Lösungsansätze vorgestellt werden konnten. Eine weitere Variante wäre die Wahl einer speziellen Technologie von lediglich einem Anbieter gewesen (z. B. Amazon mit dem AWS). Zwar hätten so auch nur die Bedenken in Bezug auf das AWS vermindert werden können, es wäre jedoch sofort klar gewesen, dass sich alle Bedenken auch mit einem einzigen System eines Anbieters vermindern lassen und es keiner Kompromisslösung bedarf.

Des Weiteren wäre es durchaus möglich, die Bedenken viel detaillierter zu betrachten, wenn es um Maßnahmen zu deren Verminderung geht. Jedoch wurde durch die große Anzahl an Möglichkeiten entschieden, dass sich nur auf einige wenige Maßnahmen konzentrieret werden sollte. Diese wurden auf Basis der derzeit größten Anbieter der Cloud ausgewählt.

Ein wichtiger Punkt, der bewusst in dieser Arbeit außen vor gelassen wurde, sind die Kosten, die eine Umlagerung des ERP-Systems vom eigenen Rechenzentrum in die Cloud mit sich bringt. Dabei geht es nicht nur um die Kosten für den Betrieb der Cloud, sondern auch um die Kosten für die Umstellung. Da ältere Versionen von ERP-Systemen noch keine Cloud unterstützen, bedarf es hier beispielsweise einer zusätzlichen Migration auf die neueste Version. Viele

Unternehmen besitzen dafür jedoch nicht die ausreichenden Ressourcen. Die Folge daraus ist, dass durch die Cloud zwar ein höherer Sicherheitsstandard erreicht wird, dieser jedoch mit hohen Initialkosten verbunden sein kann.

6.4 Ausblick in die Zukunft

Werden die Ergebnisse der Arbeit betrachtet, so liegt die weitere Forschung auf der Hand. Im nächsten Schritt wäre zu prüfen, ob durch präventive Informationen über IT-Sicherheit in der Cloud die Unternehmen ihre Bedenken tatsächlich verlieren und das ERP-System vom eigenen Rechenzentrum in die Cloud migrieren. Etwas Ähnliches wurde bereits in einem der Interviews erwähnt, in dem der Interviewpartner angab, dass dem Unternehmen bereits im Vorfeld ein umfassendes Sicherheitskonzept vorgelegt wurde. So konnten Fragen zur IT-Sicherheit bereits im Vorfeld beantwortet werden. Diese Vorgehensweise gilt es nun zu prüfen.

Neben einer geeigneten Vorgehensweise ist es der Stand der Technik, der gerade in Bezug auf IT-Sicherheit in der Cloud genau verfolgt werden muss. Durch die Schnelllebigkeit der IT und den stetigen Wandel von Paradigmen ist es nötig, dass die IT-Sicherheitsbedenken laufend überprüft und neu priorisiert werden. Würde es beispielsweise dazu kommen, dass flächendeckend eine performante Internetverbindung vorherrscht, so würde damit das aktuell größte Bedenken eliminiert werden. Neben dem Stand der Technik ändern sich jedoch auch die beschränkenden Gesetze, wie die DSGVO zeigt.

Die Priorisierung der Interviews ergab zwar, dass die Einhaltung der DSGVO, die im Mai 2018 in Kraft tritt, bei ERP-Systemen in der Cloud so gut wie kein Problem darstellt, dennoch hat die DSGVO einen Einfluss auf andere Bedenken, wie zum Beispiel den physikalischen Speicherort der Daten oder dem Vertrauen im Katastrophenfall. Diese Bedenken sind unter anderem Teil der DSGVO, deren Nichteinhaltung hohe Strafen nach sich zieht. Obwohl die Einhaltung der DSGVO für die Unternehmen anscheinend kein Problem ist, spielt sie in Zukunft eine der wichtigsten Rollen.

7 ZUSAMMENFASSUNG

In dieser Arbeit ging es um die IT-Sicherheit von ERP-Systemen in der Cloud und welche Bedenken es dabei seitens der IT-Abteilung gibt. Während die Cloud im täglichen Leben bereits Einzug gefunden hat, wehren sich Unternehmen bei ihren ERP-Systemen noch gegen eine Umstellung. Die Hauptgründe dafür sind die Kosten und die Sicherheit ihrer Daten, die dabei vom eigenen Rechenzentrum in die Cloud wandern. Da diese Gründe in Bezug auf die IT-Sicherheit jedoch viel zu allgemein gefasst sind, wollte diese Arbeit herausfinden, welche konkreten Bedenken es dabei gibt und wie diese vermindert werden können. Wichtig dabei ist vor allem die Tatsache, dass es sich beim ERP-System um die sensibelsten Daten im Unternehmen handelt. Gerade deswegen legen die Unternehmen großen Wert darauf, dass diese Daten sicher abgelegt sind, sodass darauf niemand unbefugt zugreifen kann oder sie abhandenkommen.

Es zeigt sich, dass (bezogen auf die IT-Sicherheit) eine performante Internetverbindung das größte Bedenken ist, wenn das ERP-System in der Cloud betrieben wird. Ähnlich wie für andere Bedenken, wie zum Beispiel dem physikalischen Standort der Daten, gibt es Maßnahmen, die im Vorfeld getroffen werden können, um diesen Bedenken entgegenzuwirken. Es zeigt sich, dass Cloud-Anbieter sich bereits Gedanken über mögliche Ängste gemacht haben und versuchen, diese mit entsprechenden Maßnahmen zu lösen. Besonders aufgrund der DSGVO müssen sich Unternehmen in Zukunft viel stärker an Richtlinien halten und auch nachweisen können, dass diese eingehalten werden. Dies führt dazu, dass die Cloud-Anbieter ebenfalls ihre IT-Sicherheitsrichtlinien überdenken müssen und daher auf ihren Homepages bereits ankündigen, dass ihre Lösungen mit der DSGVO konform sind oder werden.

Grundsätzlich bedeutet das Ergebnis dieser Arbeit, dass Bedenken hinsichtlich der IT-Sicherheit durch geeignete Maßnahmen bereits im Vorfeld minimiert werden können. Durch Konzepte, die noch weitere Bedenken im Bereich IT-Sicherheit einschließen und detaillierter betrachten, kann dadurch von den Cloud-Anbietern ein umfassendes IT-Sicherheitsmodell erstellt werden, um Bedenken ihrer potentiellen Kunden zu vermindern.

Abschließend sei nochmals erwähnt, dass IT-Sicherheit nicht alles ist. Im Zuge der Interviews stellten sich auch viele andere Bedenken heraus, die den Weg des ERP-Systems in die Cloud behindern. Eine höhere Sicherheit geht beispielsweise mit höheren Kosten einher, auch wenn die Kostensicht in dieser Arbeit vernachlässigt wurde. Es ist möglich, ein sicheres ERP-System in der Cloud zu betreiben, es kostet jedoch auch. Ein Beispiel dafür ist das Verfügbarkeitsmodell Hot Standby, das über einen zweiten Server als Sicherheit verfügt, der genau gleich aufgebaut ist. Dadurch entstehen automatisch Kosten für den zweiten Server. Die Kosten zeigen sich jedoch nicht nur in der Cloud, sondern auch beim ERP-System. Viele ERP-Systeme sind noch nicht im Stande, in der Cloud betrieben zu werden, was dazu führt, dass gegebenenfalls auch das ERP-System auf den neuesten Stand gebracht werden muss. Einen der Hauptgründe für die Blockade der Cloud lässt sich speziell in Großunternehmen finden. Hier existieren Systeme, die seit Jahren funktionieren und es wird von keiner Seite aus ein Grund für die Umstellung auf etwas Neues gesehen. So spielen auch viele andere Faktoren in Bezug auf dieses Thema eine Rolle, die sich jedoch abseits der IT-Sicherheit befinden.

ANHANG A - Interviewleitfaden

Name:

Alter:

Unternehmen:

Position im Unternehmen:

ERP-System:

Kenntnisse im Bereich Cloud und IT-Sicherheit (1- sehr gut, 5 – keine):

Fragen vorab, um vom gleichen Wissensstand ausgehen zu können:

- Was verstehen Sie unter dem Begriff ‚Cloud-Computing'?
- Was verstehen Sie unter ‚IT-Sicherheit' in Bezug auf Ihr ERP-System?

Allgemeine offene Fragen

- Wie steht Ihr Unternehmen generell zum Thema Cloud-Computing?
- Inwieweit nutzt Ihr Unternehmen bereits Cloud-Computing?
- Welche Herausforderungen hat der Einsatz von Cloud-Software mit sich gebracht?

Spezifische Fragen

- Wo betreiben Sie derzeit ihr ERP-System?
- Wo liegen derzeit die Daten ihres ERP-Systems?
- Wenn Rechenzentrum, dann (Kosten, Genehmigungen etc. außen vorlassen):
    - Haben Sie bereits in Betracht gezogen es in der Cloud zu betreiben?
    - Könnten Sie sich vorstellen Ihr ERP-System ganz oder teilweise in der Cloud zu betreiben?
    - Welche Bedenken haben Sie bei der Übersiedelung in die Cloud?
- Wenn Cloud, dann:
    - Warum hat man sich für diese Lösung entschieden?
    - Welche Bedenken gab es vor der Einführung?
    - Wie sicher denken Sie, dass Ihre Daten in der Cloud sind?
- Beunruhigt es Sie, wenn Unternehmensdaten nicht mehr im eigenen Rechenzentrum liegen? Wenn ja/nein, warum/warum nicht?

- Besteht in Ihrem Unternehmen die Sorge, dass aufgrund der Nutzung von Cloud-Lösungen die Einhaltung von Compliance-Anforderungen (z.B. im Bereich Datenschutz) gefährdet wird?
- Welche Daten würden Sie in der Cloud speichern?
- Wie beurteilen Sie die Datensicherheit bei ERP-Systemen in der Cloud?
- IT-Sicherheit betrifft auch Recovery-Szenarien der Datenbanken. Wie sehen Sie hier den Unterschied zwischen Cloud und RZ?

Abschluss

- Wie würden Sie abschließend die Zukunftsaussichten für den Einsatz von ERP- Systemen in der Cloud beurteilen?
- Gibt es etwas zum Thema ERP-Systeme in der Cloud, das Sie sagen möchten und noch nicht erwähnt wurde?

ANHANG B - Priorisierung der Bedenken

Nr.	Bedenken	IP 1	IP 2	IP 3	IP 4	IP 5	IP 6	Durchschnitt
1	Man weiß nicht wo bei der Public Cloud die Daten liegen.	2	2	1	6	8	11	**5,00**
2	Man weiß bei der Cloud nicht wie im Hintergrund alles genau funktioniert.	11	8	9	8	7	12	**9,17**
3	Die Cloud kann man selbst nicht so gut schützen wie das eigene Rechenzentrum.	5	10	10	7	6	6	**7,33**
4	Die Umstellung des aktuellen ERP-Systems in die Cloud bringt mehr Kosten/Aufwand mit sich als Nutzen.	9	9	8	3	9	9	**7,83**
5	Die Datenschutz-Grundverordnung kann mit der Cloud nicht eingehalten werden.	12	11	12	12	12	10	**11,50**
6	Die Cloud benötigt eine ausfallssichere Internetverbindung.	4	6	11	1	4	8	**5,67**
7	Die Cloud benötigt eine performante Internetverbindung.	3	5	6	2	1	3	**3,33**
8	Man muss darauf vertrauen, dass der Cloud-Anbieter das ERP-System im Katastrophenfall in annehmbarer Zeit wieder zum Laufen bringt.	1	1	7	4	5	4	**3,67**
9	Es ist wesentlich wahrscheinlicher, dass ein Hacker die Cloud angreift als das Rechenzentrum eines Unternehmens.	7	7	3	5	10	5	**6,17**
10	Der Anbieter der Cloud kann die Daten jederzeit mitlesen.	8	3	2	10	3	1	**4,50**
11	Mitarbeiter von Cloud Anbietern können unbefugt die Daten weitergeben/-verkaufen.	6	4	5	9	2	2	**4,67**
12	Die Vorteile der Cloud (z.B. Skalierbarkeit, Flexibilität) sind bei Großunternehmen unbrauchbar.	10	12	4	11	11	7	**9,17**

ABKÜRZUNGSVERZEICHNIS

AWS	Amazon Web Services
CRM	Customer Relationship Management
DLP	Data Loss Prevention
DSGVO	Datenschutz-Grundverordnung
ERP	Enterprise Resource Planning
IaaS	Infrastructure as a Service
IT	Informationstechnik
KMU	Klein- und Mittelunternehmen
MPLS	Multi Protocol Label Switching
NIFIS	Nationale Initiative für Informations- und Internet-Sicherheit e.V.
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
SaaS	Software as a Service
SCM	Supply Chain Management
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SQL	Structured Query Language
VM	Virtuelle Maschine
VPN	Virtual Private Network

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

LITERATURVERZEICHNIS

Abolhassan, F. (2017). Security. Die echte Herausforderung für die Digitalisierung. In F. Abolhassan (Hrsg.), *Security Einfach Machen. IT-Sicherheit als Sprungbrett für die Digitalisierung* (S. 1–11). Wiesbaden: Springer Gabler.

ACP. (2017). *ACP CS³ Storage.* Zugriff am 30.10.2017. Verfügbar unter http://www.acpcloud.rocks/shop/acp-cloud/virtual-data-center/acp-cs3-storage/

Amazon. (2017a). *AWS Direct Connect.* Zugriff am 29.10.2017. Verfügbar unter https://aws.amazon.com/de/directconnect/faqs/

Amazon. (2017b). *EU-Datenschutz.* Zugriff am 30.10.2017. Verfügbar unter https://aws.amazon.com/de/compliance/eu-data-protection/

Amazon Web Services. (2014). *EU Datenschutz Whitepaper.* Zugriff am 05.11.2017.

Amazon Web Services. (2016). *Using AWS in the context of Common Privacy & Data Protection Considerations.* Zugriff am 30.10.2017. Verfügbar unter https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Common_Privacy_and_Data_Protection_Considerations.69970a8201639b067041b43adf041c68c5a7f4f3.pdf

Backofen, D. (2017). Sicher und einfach: Security aus der Steckdose. In F. Abolhassan (Hrsg.), *Security Einfach Machen. IT-Sicherheit als Sprungbrett für die Digitalisierung* (S. 99–112). Wiesbaden: Springer Gabler.

Baun, C., Kunze, M., Nimis, J. & Tai, S. (2011). *Cloud Computing. Web-basierte dynamische IT-Services* (Informatik im Fokus, 2. Aufl.). Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg. https://doi.org/10.1007/978-3-642-18436-9

Berry, M. (o.J.). *Major Cloud Computing Vendors.* Zugriff am 18.05.2017. Verfügbar unter http://www.itmanagerdaily.com/cloud-computing-vendors/

Bräuninger, M., Haucap, J., Stepping, K. & Stühmeier, T. (2012). *Cloud Computing als Instrument für effiziente ITLösungen* (Nr. 71). HWWI policy paper.

Brisch, K. (2017). Der Beitrag des Rechts zur IT-Sicherheit. Rechtsrahmen, Anforderungen, Grenzen. In F. Abolhassan (Hrsg.), *Security Einfach Machen. IT-Sicherheit als Sprungbrett für die Digitalisierung* (S. 41–51). Wiesbaden: Springer Gabler.

Brüsemeister, T. (2008). *Qualitative Forschung. Ein Überblick* (Hagener Studientexte zur Soziologie, 2., überarbeitete Auflage). Wiesbaden: VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91182-3

Chandrasekara, T. (2016). *Dynamics NAV on Azure & Architecture.* Zugriff am 04.06.2017. Verfügbar unter http://tharangac-dynamicsnav.blogspot.com/2016/01/dynamics-nav-on-azure-architecture.html

Das europäische Parlament und der Rat der europäischen Union. (1995). Richtlinie 95/46/EG des europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Datenschutzrichtlinie 95/46/EG. *ABl. (Amtsblatt der Europäischen Union)* (L 281), 31–50. Zugriff am 10.08.2017. Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM:l14012

Denzin, N. K. (2006). *Sociological Methods. A Sourcebook*. Somerset: Taylor and Francis.

Doedt, M. (2013). *Service-Integration in Geschäftsprozessmanagementsystemen mit besonderem Fokus auf die Integration von ERP-Systemen unter Berücksichtigung des aktuellen Trends hin zum Cloud-Computing*. Dissertation, Technische Universität Dortmund. Dortmund.

Duzdar, M. (2016). *Datenschutz-Grundverordnung,* Bundeskanzleramt Österreich. Zugriff am 10.08.2017. Verfügbar unter https://www.digitales.oesterreich.gv.at/datenschutz-grundverordnung

Easttom, C. (2016). *Computer security fundamentals* (Third edition). Indianapolis, Indiana: Pearson.

Eckert, C. (2013). *IT-Sicherheit. Konzepte - Verfahren - Protokolle* (8. Aufl.). München: De Gruyter. https://doi.org/10.1524/9783486735871

Endruweit, G. (2015). *Empirische Sozialforschung. Wissenschaftstheoretische Grundlagen* (UTB Sozialwissenschaften, Bd. 4460, 1. Aufl.). Konstanz: UVK Verl.-Ges.

Furht, B. & Escalante, A. (2010). *Handbook of cloud computing* (3rd ed.). New York: Springer.

Futurezone. (2017). *User-Daten verkauft: Polizei nimmt Apple-Händler fest.* Zugriff am 02.11.2017. Verfügbar unter https://futurezone.at/digital-life/user-daten-verkauft-polizei-nimmt-apple-haendler-fest/268.757.350

Gadatsch, A. & Mangiapane, M. (2017). *IT-Sicherheit. Digitalisierung der Geschäftsprozesse und Informationssicherheit* (essentials). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-17713-3

Gartner. (2017a). *About Gartner.* Zugriff am 22.05.2017. Verfügbar unter http://www.gartner.com/technology/about.jsp

Gartner. (2017b). *Enterprise Resource Planning (ERP).* Zugriff am 09.05.2017. Verfügbar unter http://www.gartner.com/it-glossary/enterprise-resource-planning-erp

Google. (2017). *Managing Data Encryption.* Zugriff am 05.11.2017. Verfügbar unter https://cloud.google.com/storage/docs/encryption#default_behavior

Häder, M. (2015). *Empirische Sozialforschung. Eine Einführung* (3. Aufl.). Wiesbaden: Springer VS. https://doi.org/10.1007/978-3-531-19675-6

Helfferich, C. (2009). *Die Qualität qualitativer Daten. Manual für die Durchführung qualitativer Interviews* (3., überarbeitete Auflage). Wiesbaden: VS Verlag für Sozialwissenschaften / GWV Fachverlage GmbH Wiesbaden. https://doi.org/10.1007/978-3-531-91858-7

Intel Corporation. (2012). *What's Holding Back the Cloud? Intel Survey on Increasing IT Professionals' Confidence in Cloud Security.* Zugriff am 10.04.2017.

Interxion. (07.2015). *Truth and lies about latency in the cloud.* Zugriff am 29.10.2017. Verfügbar unter http://www.interxion.com/globalassets/_documents/whitepapers-and-pdfs/cloud/WP_TRUTHANDLIES_en_0715.pdf

ISO/IEC, 27000:2016(en). *Information security management systems — Overview and vocabulary:* DIN.

Jain, D. & Sharma, Y. (2016). Cloud computing with ERP - A push business towards higher efficiency. *Annual Research Journal of SCMS, Pune* (4), 140–155.

Jung-Elsen, S. (2013). Sind ERP-Systeme geeignet für die Cloud? *ERP Management* (3), 16–18. Zugriff am 02.05.2017.

Karagiannis, D. & Rieger, B. (2006). *Herausforderungen in der Wirtschaftsinformatik. Festschrift für Hermann Krallmann*. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg.

Kazim, M. & Zhu, S. Y. (2015). A survey on top security threats in cloud computing. *International Journal of Advanced Computer Science and Applications (IJACSA)* (6(3)), 109–113. Zugriff am 01.11.2017.

Klaffenbach, F., Damaschke, J.-H. & Michalski, O. (2017). *Implementing Azure solutions. Eliminate the pain point of implementation*. Birmingham: Packt Pub.

Kleemann, F., Krähnke, U. & Matuschek, I. (2013). *Interpretative Sozialforschung. Eine Einführung in die Praxis des Interpretierens* (2., korrigierte und aktualisierte Aufl.). Wiesbaden: Springer VS. https://doi.org/10.1007/978-3-531-93448-8

Lamnek, S. & Krell, C. (2010). *Qualitative Sozialforschung. Lehrbuch ; [Online-Materialien]* (Grundlagen Psychologie, 5., überarb. Aufl.). Weinheim: Beltz.

Lipsky, S. (2011). *Cloud Computing: Eine Abgrenzung zum IT Outsourcing und Systematisierung möglicher Sourcingoptionen* (Nr. 119). Arbeitspapiere des Instituts für Genossenschaftswesen der Westfälischen Wilhelms-.

Lynch, B. (2017). *Get GDPR compliant with the Microsoft Cloud.* Zugriff am 30.10.2017. Verfügbar unter https://blogs.microsoft.com/on-the-issues/2017/02/15/get-gdpr-compliant-with-the-microsoft-cloud/#sm.0010os6561a1ud6wrgc2m3gwwlkuz

Marinos, A. & Briscoe, G. (2009). Community Cloud Computing. In M. G. Jaatun, G. Zhao & C. Rong (Eds.), *Cloud computing. First international conference, CloudCom 2009, Beijing, China, December 1 - 4, 2009 ; proceedings* (Lecture notes in computer science, vol. 5931, pp. 472–484). Berlin: Springer.

Matros, R. (2012). *Der Einfluss von Cloud Computing auf IT-Dienstleister. Eine fallstudienbasierte Untersuchung kritischer Einflussgrößen* (Springer Gabler Research). Zugl.: Bayreuth, Univ., Diss., 2012. Wiesbaden: Springer Gabler.

Mayring, P. (2002). *Einführung in die qualitative Sozialforschung. Eine Anleitung zu qualitativem Denken* (Studium Paedagogik, 5., überarbeitete und neu ausgestattete Auflage). Weinheim: Beltz Verlag.

Mayring, P. (2010). *Qualitative Inhaltsanalyse. Grundlagen und Techniken* (Studium Paedagogik, 11., aktualisierte und überarb. Aufl.). Weinheim: Beltz.

Mell, P. & Grance, T. (2011) The NIST Definition of Cloud Computing. In *NIST Special Publication* (800. Aufl.). Gaithersburg,.U.S. Department of Commerce. Verfügbar unter http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Microsoft. (2017a). *Azure Storage Service Encryption für ruhende Daten.* Zugriff am 05.11.2017. Verfügbar unter https://docs.microsoft.com/de-de/azure/storage/common/storage-service-encryption

Microsoft. (2017b). *Dynamics 365.* Zugriff am 04.06.2017. Verfügbar unter https://www.microsoft.com/en-us/dynamics365/home

Neumann, L. (2017). Menschliche Faktoren in der IT-Sicherheit. In F. Abolhassan (Hrsg.), *Security Einfach Machen. IT-Sicherheit als Sprungbrett für die Digitalisierung* (S. 85–98). Wiesbaden: Springer Gabler.

NIFIS. (2016). *Sensibilität der deutschen Wirtschaft beim Datenschutz gestiegen.* Zugriff am 06.11.2017. Verfügbar unter http://www.nifis.de/veroeffentlichungen/news/article/nifis-sensibilitaet-der-deutschen-wirtschaft-beim-datenschutz-gestiegen/

North, K., Brandner, A. & Steininger, T. (2016). Die Wissenstreppe. Information – Wissen – Kompetenz. In K. North, A. Brandner & M. Steininger (Hrsg.), *Wissensmanagement für Qualitätsmanager* (essentials, S. 5–8). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-11250-9_2

Osintsev, A. (2016). *The 5 Biggest Challenges When Implementing ERP for the First Time.* Zugriff am 11.05.2017. Verfügbar unter https://www3.technologyevaluation.com/research/article/the-5-biggest-challenges-when-implementing-erp-for-the-first-time.html

Osterhage, W. W. (2014). *ERP-Kompendium. Eine Evaluierung von Enterprise Resource Planning Systemen* (Xpert.press). Berlin: Springer Vieweg. https://doi.org/10.1007/978-3-642-35885-2

Ostermann, S., Prodan, R. & Fahringer, T. (2010). Resource Management for Hybrid Grid and Cloud Computing. In N. Antonopoulos & L. Gillam (Eds.), *Cloud computing. Principles, systems and applications* (Computer Communications and Networks, pp. 179–194). London: Springer.

Österreichische Datenschutzbehörde. (2017). *Recht auf Datenschutz in der EU,* Republik Österreich. Zugriff am 10.08.2017. Verfügbar unter https://www.dsb.gv.at/recht-auf-datenschutz-in-der-eu

Plass, C., Rehmann, F. J., Zimmermann, A., Janssen, H. & Wibbing, P. (2013). *Chefsache IT. Wie Sie Cloud Computing und Social Media zum Treiber Ihres Geschäfts machen* (2. Aufl.). s.l.: Springer-Verlag.

Pols, A. & Heidkamp, P. (2016, 12. Mai). *Cloud-Monitor 2016. Eine Studie von Bitkom Research im Auftrag von KPMG – Pressekonferenz*.

Prabhu, M. & Paramesha, K. (2017). An Approach for Efficient Utilization of Public Cloud Storage and Securing Data. *International Research Journal of Engineering and Technology (IRJET), 4,* 841–844. Zugriff am 05.11.2017.

Raithel, J. (2006). *Quantitative Forschung. Ein Praxiskurs* (1. Aufl.). Wiesbaden: VS Verlag für Sozialwissenschaften/GWV Fachverlage GmbH Wiesbaden. https://doi.org/10.1007/978-3-531-90088-9

Rashid, M. A., Hossain, L. & Patrick, J. D. (2002). The Evolution of ERP Systems. In F. F.-H. Nah (Ed.), *Enterprise resource planning solutions and management* (pp. 1–16). Hershey, Pa.: IRM Press. https://doi.org/10.4018/978-1-931777-06-3.ch001

Rountree, D. & Castrillo, I. (2014). *Basics of cloud computing. Understanding the fundamentals of cloud computing in Theory and Practice* (The basics).

SAP. (2016). *Die digitale Transformation systematisch und agil umsetzen. Mit der zentralen Entwicklungs-, Erweiterungs- und Integrationsplattform für SAP®- und Non-SAP-Lösungen*.

Schiefer, G. (2012). Wer liest alle meine Daten in der Wolke? Wie Vertraulichkeit von Daten beim Cloud Computing möglich ist. *OBJEKTspektrum.* Zugriff am 05.11.2017.

Schirmer, D. & Blinkert, B. (2009). *Empirische Methoden der Sozialforschung. Grundlagen und Techniken* (Basiswissen Soziologie, Bd. 3175). Paderborn: Fink.

Schneider, R. (2017). IT-Sicherheit: Gemeinsam sind wir stärker. In F. Abolhassan (Hrsg.), *Security Einfach Machen. IT-Sicherheit als Sprungbrett für die Digitalisierung* (S. 53–64). Wiesbaden: Springer Gabler.

Schnell, M., Schulz, C., Kolbe, H. & Dunger, C. (2013). *Der Patient am Lebensende. Eine Qualitative Inhaltsanalyse* (Palliative Care und Forschung). Wiesbaden: Springer. https://doi.org/10.1007/978-3-531-19660-2

Schröder, R. & Schulte, M. (2011). *Handbuch des Technikrechts. Allgemeine Grundlagen Umweltrecht, Gentechnikrecht, Energierecht Telekommunikations- und Medienrecht Patentrecht, Computerrecht* (Enzyklopädie der Rechts- und Staatswissenschaft, 2. Aufl.). s.l.: Springer-Verlag.

Süddeutsche Zeitung. (2013). *Verkauf von Daten-CDs. Schweiz klagt mutmaßlichen Bankdaten-Dieb aus Deutschland an.* Zugriff am 02.11.2017. Verfügbar unter

http://www.sueddeutsche.de/wirtschaft/verkauf-von-daten-cds-schweiz-klagt-mutmasslichen-bankdaten-dieb-aus-deutschland-an-1.1708722

Verma, V. & Arora, D. (2014). Cloud-ERP Limitations and Benefits with Special Reference to Small & Medium Enterprises. *Vaibhav Verma Int. Journal of Engineering Research and Applications* (4), 170–174.

Weischer, C. (2007). *Sozialforschung* (UTB Soziologie, Bd. 2924). Konstanz: UVK.

Whitehouse, L. & Buffington, J. (2012). *Amazon Web Services: Enabling Cost-Efficient Disaster Recovery Leveraging Cloud Infrastructure.* Enterprise Strategy Group. Zugriff am 01.11.2017. Verfügbar unter http://d36cz9buwru1tt.cloudfront.net/ESG_WP_AWS_DR_Jan_2012.pdf

Wirtschaftskammer Österreich. (2017). *EU-Datenschutz-Grundverordnung (DSGVO). Kurzüberblick und Zeitplan.* Zugriff am 08.11.2017. Verfügbar unter https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html

Wolff, E. (2016). *Microservices. Grundlagen flexibler Softwarearchitekturen* (1., korrigierter Nachdruck). Heidelberg: dpunkt.verlag.

Wulkan, I., Condello, T. & Pogemiller, D. (2017). *Monetizing the Insider. The Growing Symbiosis of Insiders and the Dark Web* (Redowl & Intsights, Hrsg.). Zugriff am 02.11.2017.

Zhang, Q., Cheng, L. & Boutaba, R. (2010). Cloud computing. State-of-the-art and research challenges. *Journal of Internet Services and Applications, 1* (1), 7–18. https://doi.org/10.1007/s13174-010-0007-6

Zscaler. (05.2017). *Challenges and Opportunities in Enterprise Office 365 Deployments.* Zugriff am 29.10.2017. Verfügbar unter https://www.zscaler.com/resources/ebooks/office-365-deployment-survey.pdf