Cloud-Computing und Datensicherheit

Hausarbeit im Seminarmodul
„Gesellschaftliche Strukturen im Digitalen Wandel“

Alexander Girke

Matrikelnummer: 3740164
Masterstudiengang Informatik
Universität Leipzig

Leitung: Prof. Hans-Gert Gräbe, Ken Kleemann
Leipzig, 31. März 2019

Inhaltverzeichnis

1 Einleitung

Mit dem Aufkommen des Internets ab den 90er Jahren des 20. Jahrhunderts eröffnete sich die Möglichkeit einer vorher nie dagewesenen Vernetzung. Auf einmal konnten innerhalb kürzester Zeit Berechnung und Daten zwischen geographisch weit entfernten Regionen ausgetauscht werden, was nicht zuletzt zu einer grundlegenden Transformation der Gesellschaft geführt hat. (vgl. [Böhringer, Bühler, Schlaich, Sinner 2014, S. 372]) Besonders im letzten Jahrzehnt schufen Internetgiganten wie Google oder Amazon ein globales Imperium, an dem keine Person und kein Unternehmen mehr vorbeikommt. Daten werden mitunter als das Gold der Neuzeit bezeichnet. Doch wenn Daten so wertvoll sind, wie können sie geschützt werden? Und wovor überhaupt? Probleme und Lösungen dieser Art werden mit dem Begriff Datensicherheit – manchmal auch Informationssicherheit oder IT-Sicherheit genannt – in Verbindung gebracht. Was genau Datensicherheit ist, wer davon betroffen ist und auf welchen Ebenen diese wirken kann, wird in dieser Arbeit erklärt.

Ein anderer Teil dieser Hausarbeit befasst sich mit der Entstehung des sogenannten Cloud-Computings, also der Auslagerung von Infrastruktur und Berechnungen an entsprechende Dienstleister. Nicht nur Unternehmen, sondern auch Privatpersonen profitieren von dieser Entwicklung, jedoch ist nicht immer durchschaubar in welchen Bereichen Cloud-Computing Einfluss nimmt. Genauere Definitionen und welche Möglichkeiten und Risiken dieses neue Konzept bietet, werden im Folgenden beschrieben.

Kernaufgabe dieser Arbeit soll jedoch das Aufzeigen von Überschneidungen und Wechselwirkungen zwischen diesen beiden Bereichen sein. Unterstützt das Cloud-Computing das Streben nach Datensicherheit oder wirkt es sich negativ auf jene aus? Wie ist die gesetzliche Grundlage für die Anbieter solcher Cloud-Dienste und welche Hilfestellung gibt es für Privatpersonen und Unternehmen bei dem Versuch Cloud-Computing zu nutzen? Eine mögliche Antwort liefert diese Arbeit.

2 Begriffsklärung

Bevor genauer auf die Problemlage und deren aktuelle sowie zukünftige Situation eingegangen werden kann, müssen grundlegende Begriffe definiert und erklärt werden. Des Weiteren soll gegenüber verwandten Themengebieten abgegrenzt werden.

2.1 Datensicherheit

Für die Definition von Datensicherheit muss zunächst der Daten-Begriff geklärt werden. Dem Begriff Datum, Singular von Daten, im Sinne der Informationsverarbeitung mangelt es an einer einheitlichen Definition. In [Wohltmann, Lackes, Siepermann 2009] wird von *„[z]um Zweck der Verarbeitung zusammengefasste[n] Zeichen, die aufgrund bekannter oder unterstellter Abmachungen Informationen [...] darstellen“* gesprochen, wohingegen bei [Witt 2010, S.4] von *„kontextfreie[n] Angaben, die aus interpretierten Zeichen bzw. Signalen bestehen“,* die Rede ist. Vereinfacht kann gesagt werden, dass es sich um Zeichen handelt, deren Interpretation noch ausstehend ist.

Sollen diese Daten gesichert sein, muss klar sein, welchen Schaden Daten erleiden können. In diesem Bereich werden die Begriffe Datenschutz und Datensicherheit beziehungsweise das in dieser Arbeit als Synonym verwendete IT-Sicherheit benutzt. Mit den folgenden Definitionen wird versucht, diese beiden Begriffe zu unterscheiden. Laut [Lenhard 2017, S. 3f] und damit angelehnt an die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 [EU-Richtlinie 1995] ist Datenschutz der *„Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“*. Ebenfalls nach [Lenhard 2017, S. 3f] ist Datensicherheit *„wesentlicher Bestandteil des Datenschutzes [...], der technische und organisatorische Maßnahmen beschreibt“.* Fraglich ist bei dieser Definition, ob Datensicherheit tatsächlich lediglich als Bestandteil des Datenschutzes zu verstehen oder doch eigenständiger Natur ist. Eine Antwort auf diese Frage liefert folgende Definition:

> *„Unter IT-Sicherheit verstehen wir den Schutz von Informationen und Informationssystemen gegen unbefugte Zugriffe und Manipulationen sowie die Sicherstellung der Verfügbarkeit [...] für legitime Benutzer, einschließlich aller Maßnahmen zur Verhinderung, Entdeckung oder Protokollierung von Bedrohungen [...], insbesondere während der Speicherung, der Verarbeitung und der Übertragung.“*
>
> [Kappes 2013, S. 2]

Gestützt auf diese Definition, kann gesagt werden, dass die vorherige Definition für Datensicherheit im Bezug auf das Verhältnis zu Datenschutz nur teilweise zutrifft: in

der Tat betrifft Datensicherheit unter anderem den Schutz personenbezogener Daten, allerdings gilt dies nicht ausschließlich für personenbezogene Daten, sondern auch für alle anderen Arten von Daten. In dieser Hinsicht wäre Datenschutz also eher ein Teilbereich der Datensicherheit. Auf der anderen Seite ist der Bezug des Datenschutzes auf die Person, deren Daten verarbeitet werden, eine Erweiterung zum allgemeineren Begriff Datensicherheit und insofern unter Umständen ein Überbegriff.

Im Rahmen dieser Arbeit ist eine abschließende Klärung des Verhältnisses zwischen Datenschutz und Datensicherheit nicht ausschlaggebend.

2.2 Cloud-Computing

Versucht man sich dem abstrakten Begriff Cloud-Computing anzunähern, lohnt es sich zunächst beide Teilbegriffe getrennt voneinander zu betrachten.

Computing heißt auf Deutsch *Berechnung* und bezieht sich im Allgemeinen sowohl auf digitale als auch analoge Ausführung von Algorithmen, an deren Ende ein Ergebnis existiert. In diesem Kontext ist mit *Computing* jedoch *„any goal-oriented activity requiring, benefiting from, or creating computers“* [Joint Task Force for Computing Curricula 2005] gemeint. Dabei spielt es zunächst keine Rolle, welche Art von computergestützter Berechnung betrachtet wird. Berechnungen können zum Beispiel auf einem lokalen Computer durchgeführt werden oder aber auf einen anderen Rechner ausgelagert werden.

Das englische Wort c*loud* bedeutet zu Deutsch *Wolke*, welche wiederum als *„Menge von etwas, was […] in der Luft schwebt, sich quellend, wirbelnd o. ä. in der Luft oder in einer flüssigen Substanz ausbreitet“* [Dudenredaktion o.J] beschrieben wird. Da Berechnungen nicht physisch *in der Luft schweben* können, wird klar, dass es sich beim Begriff Cloud-Computing um eine sinnbildliche Abstraktion handeln muss. Diese rührt möglicherweise von der Vorstellung, dass Daten - umgangssprachlich ausgedrückt - *irgendwo in der Luft verschwinden*. Dass dies so nicht der Fall ist, sondern Daten zwar im freien Raum aber in Form von Wellen oder über als Strom über metallische Leiter an einen dedizierten Empfänger übertragen werden (vgl. [Kroschel 1991, S. 9f]), wird durch diesen Begriff verschleiert. Genauso wie, dass die auf den Daten basierenden Berechnungen nicht in einem abstrakten Etwas in der Luft, sondern auf einem physischen Computer durchgeführt werden, der diese Daten im Allge-

meinen über das Internet erhält. In Wahrheit handelt es sich hier also nicht um einen technischen Begriff, sondern vielmehr um ein neuartiges Betriebsmodell, das später genauer erklärt werden soll und welches bereits existierende Technologien vereint und nutzt. (vgl. [Zhang, Cheng, Boutaba 2010, S. 7])

Eine allgemein anerkannte Definition, die zum Beispiel auch von der *European Network and Information Security Agency* (ENISA) verwendet wird, liefert das sogenannte *National Institute of Standards and Technology* (NIST):

> *„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.“*
>
> [Mell, Grance 2011, S. 2]

Zusammengefasst lässt sich sagen, dass beim Cloud-Computing Ressourcen wie zum Beispiel Rechenkraft oder Speicherplatz ohne größeren Aufwand gebucht und wieder freigegeben werden können. Dabei erfolgt die Abrechnung meist pro beanspruchter Zeiteinheit. Für einen Cloud-Service werden durch das NIST fünf Eigenschaften definiert:

1. **On-demand Self-Service:** Ressourcen wie zum Beispiel Rechenleistung oder Speicher können ohne Interaktion mit dem Anbieter gebucht werden;
2. **Broad Network Access:** Dienste sind über Standardschnittstellen des Internets miteinander verbunden;
3. **Resource Pooling:** Ressourcen liegen in einem Pool vor, auf den alle Kunden Zugriff haben (*Multi-Tenant Modell*), wobei der genaue Standort unbekannt ist;
4. **Rapid Elasticity:** Dienste können schnell und elastisch bereitgestellt werden;
5. **Measured Services:** Nutzung wird gemessen und überwacht. (vgl. [Mell, Grance 2011, S. 2])

Im selben Dokument werden für Cloud-Computing zudem Service- und Betriebsmodelle definiert. Bei den Servicemodellen wird unterschieden nach *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS) und *Software as a Service* (SaaS). Auf

unterster Ebene steht dabei IaaS, da hier die elementaren Bausteine wie Server, Datenbanken oder Netzwerke einer Softwaresystemarchitektur im Mittelpunkt stehen. PaaS liegt eine Ebene darüber und bietet meist, beispielsweise für Software-Entwickler, eine geeignete Abstraktionsebene, um die fertigen Softwareartefakte zur Verfügung zu stellen. Auf oberster Ebene befindet sich SaaS, welches wiederum hauptsächlich Endanwendern angeboten wird. (vgl. [Baun, Kunze, Nimis, Tai 2011, S. 31ff])

Abbildung 1: Servicemodelle, aus [Baun, Kunze, Nimis, Tai 2011, S. 30], bearbeitet.

Bei den Betriebsmodellen werden im Wesentlich die drei Arten *public*, *private* und *hybrid cloud* betrachtet, obwohl auch andere Formen wie *community cloud* oder *personal cloud* existieren. Von einer *public cloud* wird gesprochen, wenn Anbieter und Benutzer nicht Teil derselben organisatorischen Einheit, also zum Beispiel nicht im gleichen Unternehmen tätig sind. Eine *private cloud* auf der anderen Seite gehört einem Unternehmen allein. Die Mischform der beiden Modelle stellt die *hybrid cloud* dar, wobei hier im Regelbetrieb die *private cloud* verwendet, für Lastspitzen aber auf die *public cloud* ausgewichen wird. (vgl. [Baun, Kunze, Nimis, Tai 2011, S. 27ff])

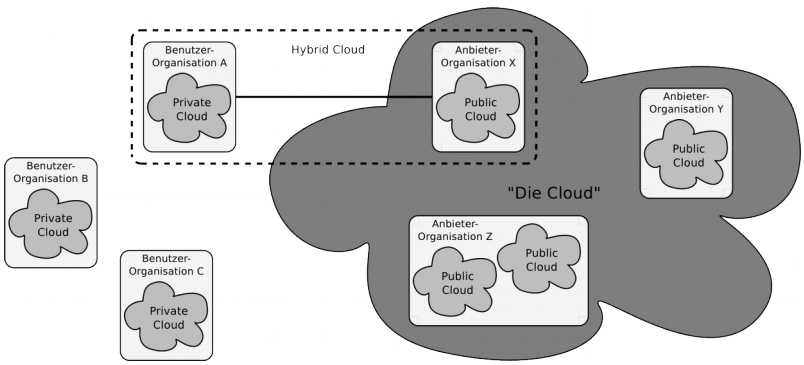

Abbildung 2: Betriebsmodelle, aus [Baun, Kunze, Nimis, Tai 2011, S. 28]

Eine Spezialform ist die sogenannte *Virtual Private Cloud* (VPC), wobei damit ein netzwerktechnisch abgegrenzter Bereich innerhalb einer *public cloud* gemeint ist. Damit wird ein Ansatz ähnlich zum bekannteren *Virtual Private Network* (VPN) – privaten Netzwerk innerhalb des eines öffentlichen Netzwerkes – verfolgt. (vgl. [Baun, Kunze, Nimis, Tai 2011, S. 27ff])

2.3 Abgrenzung

Das Thema Datenschutz – abgegrenzt von Datensicherheit wie unter 2.1 - Datensicherheit dargestellt – soll in dieser Arbeit keine Rolle spielen. Es soll also keine Unterscheidung zwischen personenbezogenen und anderen Daten gemacht werden. Auch stehen hier keine Personen im Fokus der Betrachtung. Stattdessen werden ausschließlich Eigenschaften von Daten untersucht, die es zu schützen gilt. Diese werden im Folgenden genauer definiert.

Des Weiteren soll entsprechend zu 2.2 - Cloud-Computing keine andere Form des Computing wie zum Beispiel Grid- oder Fog-Computing, sondern lediglich das Cloud-Computing betrachtet werden. Im Folgenden werden Vergleiche zu anderen Berechnungsformen gemacht, dann jedoch ausschließlich mit dem Ziel, die Eigenschaften des Cloud-Computing genauer zu erklären.

3 These und Ziel der Arbeit

Nachdem die Kernbegrifflichkeiten dieser Arbeit *Datensicherheit* und *Cloud-Computing* geklärt wurden, stellt sich die Frage inwiefern diese beiden Begriffe zusammenhängen. Deutlich geworden ist, dass Datensicherheit prinzipiell jede Art von Computing betrifft, da eine Berechnung zwingend mit Daten operiert – Daten, deren Schutz für bestimmte Akteure wichtig ist. Insofern sind Datensicherheit und Computing im Allgemeinen untrennbar miteinander verknüpft. Wie jedoch wirkt sich das Cloud-Computing auf die Datensicherheit aus? Erhöhen externe Datenhaltung und Berechnungen die Datensicherheit – oder haben sie negative Auswirkungen? Welche Bereiche der Datensicherheit sind besonders betroffen und welcher Akteur profitiert oder leidet unter diesen Auswirkungen? Und wie sieht die aktuelle Diskussionslage zu diesen Fragen aus? Die Beantwortung dieser Fragen soll Ziel dieser Arbeit sein.

Dabei soll folgende These als Arbeitsgrundlage dienen, diskutiert und am Ende auf ihren Wahrheitsgehalt überprüft werden: *Mithilfe von Cloud-Computing wird eine einfache Verbreitung datensicherheitstechnischer Standards auf internetbasierte Dienste ermöglicht, wobei jene mit einer Modularisierung dieser übergreifenden Funktionalität einhergeht.* Bevor eine Diskussion zu dieser These beginnen kann, sollen im nächsten Kapitel zunächst die einzelnen Bestandteile der These erklärt werden.

4 Diskussionsgrundlagen

Um der anschließenden Analyse und Synthese den passenden Kontext zu liefern, soll in diesem Kapitel ein Einstieg in die Konzepte und ein Überblick über die aktuelle Situation von Cloud-Computing und Datensicherheit gegeben werden.

4.1 Entwicklung der dezentralen Datenverarbeitung

Die Anfänge der auf mehrere Rechner verteilten Datenverarbeitung finden sich bereits in den späten 1950er Jahren in Form von fehleranfälligen Telefonverbindungen. Mit Entstehung des sogenannten ARPANETs in den Vereinigten Staaten von Amerika wurde die Grundlage für das heutige *World Wide Web* gelegt. (vgl. [Abbate 2000])

Einen entscheidenden Entwicklungsschub erhielt dieses amerikanische Netz, welches bisher ausschließlich für militärische und wissenschaftliche Zwecke genutzt wurde, als es 1991 für die kommerzielle Nutzung freigegeben und Verbindungen zwischen den nationalen Netzen hergestellt wurden. Bis 1993 diente das sogenannte *Internet* hauptsächlich zur Kommunikation via E-Mails, schaffte jedoch in diesem Jahr mit der Erfindung der Auszeichnungssprache HTML und dem ersten Webbrowser *Mosaic* durch den am schweizer Forschungsinstitut CERN forschenden Tim Berners-Lee den Durchbruch. (vgl. [Böhringer, Bühler, Schlaich, Sinner 2014, S. 372])

Ab Anfang der 2000er Jahre, erreichte das Internet eine neue Entwicklungsstufe, welche von Tim O‘Reilly 2005 unter dem Begriff *Web 2.0* im Buch „What is Web 2.0“ beschrieben wurde. Beschrieben wird mit diesem Begriff der Wandel eines Internets der statischen Inhalte, auf die lediglich wenige Haushalte Zugriff hatten, hin zu nutzergenerierten und -spezifischen, dynamischen Inhalten. Mit diesen Mitteln werden anschließend massenhaft Nutzerinteraktionen – erhöht durch das Aufkommen der

ersten Smartphones – verarbeitet und immer ansprechendere Services zur Verfügung gestellt. (vgl. [Behrendt, Zeppenfeld 2008, S. 5f])

Mit diesen steigenden Anforderungen an die Systeme der Anbieter solcher interaktiven Dienste, steigen auch die benötigten Ressourcen. Auch heute noch gültige Gründe für den erhöhten Bedarf sind zum Beispiel das Bedürfnis nach performanten Applikationen trotz hohen Daten- und NutzerInnenaufkommens und verkürzte Zeiten, bis das Produkt am Markt angeboten wird. (vgl. [Sehgal, Bhatt 2018, S. 3])

Ein Unternehmen, welches auf diese Anforderungen mit einer eigenen Infrastruktur und dazu passenden Schnittstellen geantwortet hat, ist *Amazon*. Als eines der größten Online-Shop-Unternehmen wurde es nötig, entsprechende Hardware zur Verfügung zu stellen. (vgl. [Strube 2010])

Mit einer hohen Anzahl an Festplatten, Servern und anderen Hardware-Komponenten steigen auch deren Ausfälle pro Tag. Entsprechend automatisiert muss der Austausch jener sein, was wiederum ein hochkomplexes System zum Management dieser Infrastruktur erfordert. Dieses System bietet Amazon seit 2006 unter dem Namen *Amazon Web Services*[1] an. Wie bei anderen Produkten dieser Art – zum Beispiel *Microsoft Azure*[2] oder *Google Cloud Platform*[3] – entsteht so eine Win-Win-Situation für AnbieterInnen und KundInnen. Aufgrund des erhöhten Hardware-Bedarfs kommt es in einem solchen Rechenzentrum zu freien Kapazitäten. Diese Kapazitäten werden weiterverkauft, wobei der/die KundIn wiederum den Vorteil hat, nicht selbst für den Betrieb dieser komplexen Infrastruktur sorgen zu müssen. (vgl. [Oppitz, Tomsu 2018])

Neben der vorangegangen Erklärung des Begriff „internetbasierter Dienst“ soll im Folgenden auch *Modularisierung* genauer beschrieben werden. Die Modularisierung – umgangssprachlich auch Baukastenprinzip genannt – hat in verschiedenartigen Bereichen wie Architektur oder Maschinenbau eine ähnliche Bedeutung. In [Hohnen, Pollmanns, Feldhusen 2013, S. 746] wird bei einem *Modul* von einer funktional vom Produkt nahezu gänzlich unabhängigen Entität gesprochen. Somit ist ein Modul immer Teil eines Ganzen. Bei Modularisierung steht laut [Hohnen, Pollmanns, Feldhu-

1 https://aws.amazon.com/
2 https://azure.microsoft.com/de-de/
3 https://cloud.google.com/

sen 2013, S. 746] vor allem die Steigerung der *Modularität* – also der vorteilhaften Strukturierung der Produktarchitektur – im Fokus.

In der Softwareentwicklung wird mitunter von sogenannten *funktionalen* und *nicht-funktionalen* Aspekten bzw. Modulen gesprochen: unter funktionalen Aspekten wird alles verstanden, was zu den Kernaufgaben eines Produktes zählt. Für Chat-Tool ist dies beispielsweise das Versenden von Nachrichten. Nicht-funktionale Aspekte sind hingegen Aufgaben, die wichtig aber nicht zwingend notwendig für die Erfüllung der Hauptaufgaben sind. Im Beispiel des Chat-Tools zählen dazu auch Performanz oder Sicherheit. Eben genannte Aspekte – auch *cross-cutting concerns* genannt – lassen sich teilweise in Module auslagern, sodass sowohl die in [Hohnen, Pollmanns, Feldhusen 2013, S. 746] geforderte vorteilhafte Strukturierung als auch die Wiederverwendbarkeit zum Tragen kommen. (vgl. [Georg, Reddy, France 2004, S. 114])

Neben den vorher genannten gehört auch die Datensicherheit zu den nicht-funktionalen Aspekten von internetbasierten Diensten.

4.2 Ebenen der Datensicherheit

Um Datensicherheit im Kontext des Cloud-Computing zu betrachten, sollen im Folgenden verschiedene Ebenen diskutiert werden, auf denen Datensicherheit wirken kann. Dabei soll im Vordergrund stehen, welche Auswirkungen die Schaffung beziehungsweise die Abwesenheit von Datensicherheit auf die einzelnen Ebenen hat.

Auf *technischer* Ebene kann Datensicherheit in sechs Bestandteile zerlegt werden: *Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Verbindlichkeit* und *Autorisation*. Kurz erklärt handelt es sich bei *Vertraulichkeit* um den Informationsschutz gegenüber dem Zugriff durch Unbefugte. Eine Verletzung der Vertraulichkeit findet beispielsweise statt, wenn in einem Unternehmen eine Gehaltsabrechnungsdatei geöffnet ist, der Bildschirm aber nicht gesperrt ist und ein beliebiger Mitarbeiter Einsicht auf diese Datei erhält. Mit *Integrität* hingegen ist der Informationsschutz gegenüber Veränderungen durch Dritte gemeint. Verletzt werden kann die Integrität beispielsweise durch Naturkatastrophen, wie Erdbeben, bei denen Daten unwiederbringlich verloren gehen. Von *Verfügbarkeit* wird gesprochen, wenn Ressourcen und Dienste einem Nutzer tatsächlich zur Verfügung stehen – gestört werden kann diese zum Beispiel durch eine sogenannten *Distributed Denial of Service* (DDoS) – Attacke, die genutzt

wird, um einen Server am Antworten zu hindern. Von *Authentizität* ist die Rede, wenn der Absender von Informationen eindeutig identifiziert werden kann. Das Vortäuschen einer anderen Identität und damit die Gefährdung der Authentizität kann beispielsweise durch Abfangen und Missbrauch von sogenannten Identitäts-Token erreicht werden. Bei *Verbindlichkeit* geht es um die Möglichkeit, den Informationsinhalt und -absender nachweisbar zu machen, was nicht möglich ist, wenn zum Beispiel auf die Verwendung einer digitalen Signatur verzichtet wird. Die *Autorisation* betrifft die Beschränkung des Ressourcenzugriffs auf ausgewählte, authentifizierte Benutzer, wobei beispielsweise im Gebrauch eines Laptops die standardmäßige Benutzung des Administrator-Nutzers ein Bedrohung für die Autorisation darstellt. (vgl. [Kappes 2013, S. 2f])

Für die Erreichung jedes einzelnen dieser Bestandteile existieren bestimmte *datensicherheitstechnische Standards*, wie in der These dieser Arbeit angedeutet. Eine wichtige Quelle für diese Standards ist das Bundesamt für Sicherheit in der Informationstechnik (BSI). Es kann beispielsweise eine Zertifizierung für jede der momentan existierenden 350 Richtlinien durch das BSI ausgestellt werden, mithilfe derer nachgewiesen werden kann, dass ein System alle Konformitätsprüfungen zu einer bestimmten Richtlinie bestanden hat. (vgl. [BSI 2019])

Auf der *individuellen* Ebene betrachtet hat Datensicherheit mehrere Schwierigkeiten. Während es zwar ausreichend Produkte zur Wahrung des Schutzes persönlicher oder zur einer Privatperson gehörender Daten gibt, sind diese mitunter nur mit einigem Aufwand einzusetzen. Dieser Aufwand wird jedoch nicht von allen EndnutzerInnen betrieben. (vgl. [Kappes 2013, S. 340]) Dabei gibt es viele Angebote, die auch Privatanwender einen sicheren Umgang mit ihren Daten ermöglichen wollen. Einige davon sind durch das Bundesministerium des Innern gefördert, wie zum Beispiel *Deutschland sicher im Netz*[4], der *Aktionsbund Digitale Sicherheit*[5] oder die *Digitale Nachbarschaft*[6], um nur einige zu nennen. Diese Plattformen bieten eine Übersicht zu existierenden Projekten, allgemeine Informationen oder auch Weiterbildungsmöglichkeiten an. Natürlich helfen diese Angebote nur weiter, wenn sich eine Privatperson aktiv damit beschäftigt, was möglicherweise erst der Fall ist, wenn die Auswir-

4 https://www.sicher-im-netz.de/dsin-f%C3%BCr-verbraucher
5 https://aktionsbund.org/
6 https://www.digitale-nachbarschaft.de/

kungen von fehlender Datensicherheit klar sind. Auch hier zählen die bereits im vorherigen Absatz zur technischen Ebene von Datensicherheit genannten Gefahren wie Datenverlust oder Identitätsdiebstahl dazu. Spätestens wenn zum Beispiel Zugangsdaten für das Bankkonto an eine unbefugte Person gelangen lässt sich der Schaden auch finanziell beziffern. Einfache Schutzmaßnahmen wie zum Beispiel die Erstellung von Backups oder das Verschlüsseln von Festplatten werden durch obige Plattformen empfohlen.

Nicht nur Privatpersonen, sondern auch staatliche oder wirtschaftliche Institutionen können von unvollständiger Datensicherheit betroffen sein. Deshalb empfiehlt das BSI die Verankerung von IT-Sicherheitsprozessen, die sich an der IT-Sicherheitsstrategie der Institution orientieren. Für die Umsetzung werden sowohl ein IT-Sicherheitskonzept als auch eine IT-Sicherheitsorganisation empfohlen. Bei ersterem werden Phasen des IT-Sicherheitsprozesses definiert, wie zum Beispiel die Risikoerkennung, die Erstellung eines Umsetzungsplanes und die Überwachung der Umsetzung. Bei letzterem handelt es sich um Angaben zur Einbettung der Datensicherheit in die Organisation. Hierfür sollen Gremien geschaffen und Verantwortliche festgelegt werden. Empfohlen wird ein IT-Sicherheitsbeauftragter, der außerhalb der eigentlichen IT-Organisation steht. Informationen und Hilfestellung zur Implementierung dieser Strukturen werden ebenfalls von verschiedenen staatlichen Ämtern oder Initiativen wie zum Beispiel *IT-Sicherheit in der Wirtschaft*[7] vom Bundeswirtschaftsministerium zur Verfügung gestellt. Für diese Maßnahmen werden vom BSI Zertifizierungen ausgestellt, die beispielsweise gegenüber GeschäftspartnerInnen oder KundInnen eine ausreichende Sicherheit nachweisen. (vgl. [Kappes 2013, S. 336])

Dies betrifft auch Anbieter von IT-Produkten wie zum Beispiel Cloud-Computing-Diensten. Auch dafür gibt es entsprechende Hilfestellungen wie zum Beispiel das Technologieprogramm *Sichere Internet-Dienste – Sicheres Cloud Computing für Mittelstand und öffentlichen Sektor (Trusted Cloud)*[8], welches ebenfalls vom Bundeswirtschaftsministerium in Leben gerufen wurde. (vgl. [DuD 2012])

Zuletzt bleibt die Frage, ob und wenn ja, welche gesamtgesellschaftlichen Auswirkungen die Datensicherheit hat. Ein Begriff, der mit Veränderungen im digitalen Zeitalter verknüpft ist, ist der der *Digitalen Transformation*. Definiert wird dieser Begriff zum

7 https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Navigation/DE/Home/home.html
8 https://www.trusted-cloud.de/

Beispiel als *„erhebliche Veränderungen des Alltagslebens, der Wirtschaft und der Gesellschaft durch die Verwendung digitaler Technologien und Techniken sowie deren Auswirkungen.“* [Pousttchi 2017] Der darin enthaltene Wandel der Gesellschaft wird manchmal als Wandel zu einer *Digitalgesellschaft* bezeichnet. Mit der in der Definition angesprochenen Verwendung digitaler Technologien stellt sich die Frage nach dem Stellungswert der Datensicherheit in einer Gesellschaft. Wie in den vorigen Absätzen beschrieben, ist Datensicherheit ein Aspekt, der alle Akteure betrifft, die digitale Technologien verwenden. Für Privatpersonen und Unternehmen wurde bereits aufgezeigt, welche Risiken eine Vernachlässigung der Datensicherheit birgt. Auch entsprechende Angebote zur Hilfestellung wurden angeschnitten, viele davon initiiert durch Bundesministerien. Die entsprechende Handhabe dieser Ministerien beruht auf gesetzlichen Grundlagen, die im Folgenden als ein möglicher Maßstab der gesellschaftlichen Bedeutung verstanden werden. Die historische Entwicklung begann im Jahr 1991 mit dem *Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik* [BSIG 1991]. Das BSI untersteht dabei dem Bundesministerium des Innern und erhält unter Anderem die Aufgaben, zur Entwicklung der IT-Sicherheit in Deutschland beizutragen, Unternehmen bei der Umsetzung zu unterstützen und zu beraten und informationstechnische Systeme und Komponenten einer Zulassungsprüfung zu unterziehen. (vgl. [§ 3 Abs. 1 BSIG 1991]) Seine Ablösung erfuhr dieses Gesetz durch das *Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes* [BSIG 2009]. Darin werden die Aufgaben des BSI wie folgt erweitert: mit diesem Gesetz wird das BSI zur zentrale Meldestelle für Sicherheitslücken, ist zuständig für die Verarbeitung sämtlicher (Protokoll-)Daten des Bundes, fungiert als zentrale Warnstelle für sowohl die Hersteller von informationstechnischen Systemen und Komponenten als auch der Öffentlichkeit und setzt IT-Sicherheitsstandards für die gesamte Bundesverwaltung. (vgl. [§ 3 Abs. 1 BSIG 2009])

Die letzte größere Erweiterung erfuhr dieses Gesetz durch das *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme* (IT-Sicherheitsgesetz). Darin enthalten waren neben Änderungen anderer Gesetze wie zum Beispiel dem Atomgesetz oder dem Energiewirtschaftsgesetz auch die Erweiterung des BSIG. Besonders §acht erweiterte den bisherigen Aufgabenbereich um die Zielgruppe der Betreiber sogenannter kritischer Infrastrukturen. Dazu zählen unter anderem die Betreiber von Wasser- oder Stromversorgungsanlagen, zusammengefasst mit der Abkürzung KRI-

TIS. Das BSI wird damit zur zentrale Koordinationsstelle für KRITIS, für die zusätzlich eine Meldepflicht bei Sicherheitslücken besteht. Außerdem kann das BSI mit dieser Gesetzeserweiterung die Hersteller von informationstechnischen Systemen oder Komponenten in einem solchen Falle zur Mithilfe verpflichten. (vgl. [§8a - §8c BSIG 2009])

Selbstverständlich sind diese gesetzlichen Grundlagen nur ein Teil der gesellschaftlichen Veränderungen im Bezug auf Datensicherheit, jedoch hilft es den Stellenwert der Datensicherheit zu verdeutlichen.

5 Analyse

In den vorangegangen Kapiteln wurden die Grundlagen für die nun folgende Diskussion der Fragestellung dieser Arbeit gelegt. Auf verschiedenen Ebenen wurden sowohl Auswirkungen der Datensicherheit (technisch, individuell, institutionell, gesellschaftlich) und Formen des Cloud-Computing (IaaS, PaaS, SaaS) betrachtet. Welche Positionen zur Vereinbarkeit und gegenseitigen Wechselwirkung zwischen diesen beiden Bereichen existieren und die Darstellung dieser, soll Inhalt dieses Kapitels sein.

Vorerst wird noch einmal die Relevanz der beiden Teilbereiche Cloud-Computing und Datensicherheit verdeutlicht werden. Wie schon in den Jahren 2016 und 2017 belegen diese beiden Themen auch 2018 Platz eins und zwei bei einer jährlichen Erhebungen[9] des *Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien* (BITKOM). Sahen 2016 noch 58% Cloud-Computing und 59% IT-Sicherheit als wichtigsten Trend an (vgl. [Krösmann 2016]), so steigerten sich die Zahlen auf entsprechend 60% beziehungsweise 69% (vgl. [Krösmann 2017]). Im Jahr 2018 blieben die Aussagen verhältnismäßig stabil bei 61% für Cloud-Computing und 67% für IT-Sicherheit. (vgl. [Streim 2018])

9 Hinweise zur Methodik: Die Daten werden halbjährlich während der Konjunkturumfrage „Bitkom-Branchenbarometer“ durch die Bitkom Research erhoben. Dabei werden Unternehmen der Informationstechnik- und Telekommunikationsbranche (ITK) gefragt, was aus Sicht des Unternehmens die maßgeblichen Trends sind, die den deutschen ITK-Markt im jeweiligen Jahr prägen werden. (vgl. [Streim 2018])

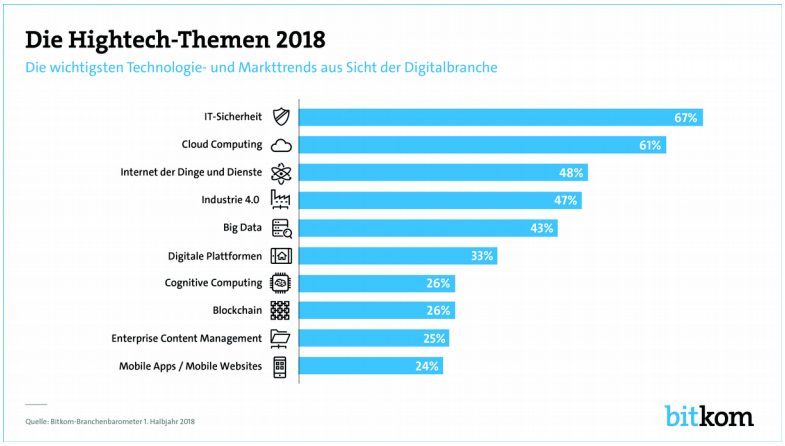

Abbildung 3: Hightech-Themen 2018, aus [Streim 2018]

Auf Grundlage dieser Zahlen ist es naheliegend, die beiden Themen auch in Verbindung miteinander zu betrachten. Für die Analyse der Frage, welche Auswirkungen Cloud-Computing auf die einzelnen Ebenen der Datensicherheit hat, werden im Folgenden soweit zu einer Ebene gehörig die Aussagen von [Baun, Kunze, Nimis, Tai 2011], [Oppitz, Tomsu 2018], [Adelmeyer, Petrick, Teuteberg 2018], [BSI 2016] und [Laue, Stiemerling 2010] dargestellt.

Im Bezug auf die technische Ebene sind sich [Oppitz, Tomsu 2018], [BSI 2016] und [Laue, Stiemerling 2010] einig: die größte Problematik bei der Interaktion mit Cloud-Computing-Diensten liegt bei der Authentizität der Kommunikationspartners. In [Oppitz, Tomsu 2018] werden vor allem unsichere Übertragungswege als Schwierigkeit genannt. Eine dort als *good* bezeichnete Nachricht, muss zusätzlich zur Authentizität auch Integrität und Vertraulichkeit gewährleisten, was nur innerhalb eines dort *trust zone* genannten Bereichs der Fall ist. Auch wird die Frage nach der Zugehörigkeit der Cloud zu dieser *trust zone* gestellt, bleibt aber vorerst unbeantwortet. Später wird allerdings auf starke Verschlüsselungsmöglichkeiten für Transport (TLS) und Verbindungen (IPsec und VPNs) hingewiesen. (vgl. [Oppitz, Tomsu 2018, S. 377 & S. S. 396])

In [BSI 2016] wird das Ausspähen von Nachrichten und der Diebstahl der Identität als Risiko benannt. Zusätzlich werden die Gefahr des Daten- und Kontrollverlustes sowie Einschränkungen der Verfügbarkeit angeführt. (vgl. [BSI 2016, S. 8]). [Laue, Stiemerling 2010] führt außerdem die Schwierigkeit im Umgang mit Zugriffsrechten an, sowohl was die Granularität als auch die Flexibilität angeht. (vgl. [Laue, Stiemerling 2010, S. 693f]).

Anders als die drei zuvor genannten Quellen, machen [Baun, Kunze, Nimis, Tai 2011] und [Adelmeyer, Petrick, Teuteberg 2018] die Schwierigkeiten eher an den unterschiedlichen Betriebs- und Servicemodellen fest. Laut [Baun, Kunze, Nimis, Tai 2011] bietet IaaS zwar die größte Flexibilität, aber erfordert auch größere Aufwände für die Datensicherheit bei NutzerInnen. SaaS hingegen schiebt die Verantwortung für die Datensicherheit zu AnbieterInnen, schränkt aber auch die Flexibilität ein. Gleichzeitig wird argumentiert, dass die verschlüsselte Kommunikation mit den Servern des Cloud-Anbieters regulierbar und das Speichern von verschlüsselten Daten in der Cloud im Vergleich zur unverschlüsselten Ablage dieser Daten auf einem lokalen Rechner sicherer sei. Grundlage dafür seien die Auditing-Prozesse – also das Aufzeichnen jeder Interaktion mit einer Ressource –, die eine Einhaltung strenger Vorgaben ermöglichen. (vgl. [Baun, Kunze, Nimis, Tai 2011, S. 85f])

In [Adelmeyer, Petrick, Teuteberg 2018] wird zusätzlich zur hohen Infrastrukturabstraktion bei SaaS das unter 2.2 Cloud-Computing beschriebene *resource pooling* als Gefahr für die Datensicherheit benannt. (vgl. [Adelmeyer, Petrick, Teuteberg 2018, S. 7]) Eine teilweise passende Übersicht über Chancen und Risiken des Cloud-Computing findet sich in [Baun, Kunze, Nimis, Tai 2011]. Diese ist nicht vollständig, deckt jedoch die meisten Aspekten der technischen Datensicherheit ab:

Tabelle 8.1 Risiken und Chancen des Cloud Computing (Auswahl)

	Risiken	Chancen
1	Verfügbarkeit der Dienste	Nutzung mehrerer Cloud-Anbieter zur Sicherstellung der Dienste-Kontinuität
2	Lock-In der Daten	Standardisierung der Schnittstellen (API)
3	Vertraulichkeit und Nachvollziehbarkeit der Daten	Einsatz von Datenverschlüsselung, virtuellen Netzwerken (VLAN) und Firewalls. Einhaltung nationaler Gesetze durch geographische Datenhaltung
4	Engpässe bzgl. Datentransfer	Versand von Festplatten durch Dritte (z. B. FedEx, UPS)[a]
5	Schlechte Vorhersagbarkeit der Leistungsfähigkeit (Performance)	Bessere Unterstützung virtueller Maschinen. Einsatz von Flash-Speicher
6	Skalierbarer persistenter Speicherplatz	Entwicklung skalierbarer Speicherplatz-Technologien
7	Fehler in großen, verteilten Systemen	Entwicklung von Debuggern für verteilte Maschinen
8	Schnelles Skalieren	Entwicklung automatischer Skalierungswerkzeuge, basierend auf Machine Learning. Ressourcen- und kostenbewusstes Nutzer- und Anbieterverhalten
9	Reputation und Haftpflicht	Einsatz von Dienstleistungen Dritter, wie z. B. für vertrauenswürdige Emails
10	Software Lizenzen	Nutzungsbezogene Lizenzen (Pay-for-use). Verkauf von Software und Diensten im Paket

Abbildung 4: Risiken und Chancen des Cloud Computing, aus [Baun, Kunze, Nimis, Tai 2011, S. 127]

Allen gemeinsam ist die Handlungsempfehlung für Institutionen in Gegenwart dieser Bedrohungen: das Risikomanagement muss bereits vor der Migration in die Cloud ausgearbeitet sein. In [Adelmeyer, Petrick, Teuteberg 2018] wird ein eigenes Frame-

work angelehnt an ISO 27005 beschrieben. Mithilfe der Risikoidentifikation, -analyse, -bewertung und -behandlung wird eine Antwort auf die vorher beschriebenen Probleme angeboten. (vgl. [Adelmeyer, Petrick, Teuteberg 2018, S. 20f])

Auch das [BSI 2016] schlägt die Entwicklung einer Cloud-Strategie vor, die sowohl Risikoanalyse als auch Kosten-Nutzen-Abschätzung berücksichtigt. Für etwaige Probleme bei der Interaktion mit Cloud-AnbieterInnen wird die Überprüfung verschiedener Zertifizierungen wie zum Beispiel dem *Cloud Computing Compliance Controls Catalogue* (C5) und die Vereinbarung von sogenannten *Service Level Agreements* (SLAs) – Vereinbarung zur Einhaltung der versprochenen Dienste – vorgeschlagen. (vgl. [BSI 2016, S. 11f & S. 18f]).

Ebenfalls auf SLAs verweisen [Baun, Kunze, Nimis, Tai 2011], wobei hier zusätzlich der sogenannte *Vendor-Lock-In* – die Abhängigkeit zu einem/einer bestimmten Cloud-AnbieterIn – als mögliches Risiko eingestuft wird. Abhilfe schafft demnach die Verwendung von standardisierten Verfahren sowie plattformunabhängige Software-Entwicklung. (vgl. [Baun, Kunze, Nimis, Tai 2011, S. 87])

Die Autorisierung als spezifischer Aspekt der Datensicherheit, der vor allem in größeren Institutionen Bedeutung erfährt, wird verstärkt in [Laue, Stiemerling 2010] betrachtet. Es werden die drei Lösungsansätze *Single-Credential, Single-Sign-On* und *die Zentrale Verwaltung von Benutzerrollen* vorgestellt, welche wiederum als Lösung von Problemen genutzt werden, die in klassischen Rechenzentren unter Umständen so nicht auftauchen. (vgl. [Laue, Stiemerling 2010, S. 696f])

Auf die Risiken und Möglichkeiten der privaten Nutzung von Cloud-Computing-Diensten und die Auswirkungen dieser auf die Gesellschaft wird in kaum einer der Quellen weiter eingegangen. Einzig in [Oppitz, Tomsu 2018] wird dem Einfluss des Cloud-Computings auf diese Ebenen im Allgemeinen ein Kapitel gewidmet. Gleich in der Einleitung des Kapitel *Changes in Society and Politics* wird auf die Relevanz des Cloud-Computing bei der Entwicklung einer *global community* verwiesen. Besonders die Beziehung zwischen Staat und Unternehmen beziehungsweise Unternehmen und BürgerInnen sei von diesem Wandel in der Hinsicht betroffen, dass es Aufgabe der Legislative sei, BürgerInnen und Unternehmen vor Missbrauch und Schaden im digitalen Bereich zu schützen. (vgl. [Oppitz, Tomsu 2018, S. 411]) Dass besonders im Bereich der Privatheit und Sicherheit im Internet vermehrt Spannungen entstehen,

kritisiere auch der Erfinder des Internets, Tim Berners-Lee. Er bemängele, dass „we‘ve lost the control of our personal data“ [Oppitz, Tomsu 2018, S. 412], was in selbigem Buch aufgegriffen wird. Demzufolge liege die Verantwortung für die Privatheit und Sicherheit sowie Identität des Kunden mittlerweile sowohl bei AnbieterInnen eines Cloud-Services als auch bei der jeweiligen Staatsregierung. (vgl. [Oppitz, Tomsu 2018, S. 422])

6 Synthese

Im abschließenden Teil dieser Arbeit wird auf Grundlage der unter 5 Analyse vorgestellten Positionen die These dieser Arbeit beantwortet. Beginnend bei der privaten und gesellschaftlichen Ebene geht aus [Oppitz, Tomsu 2018] klar hervor, welche Auswirkungen internetbasierte Dienste beispielsweise auf die globale Vernetzung aller Gesellschaften oder die Entwicklung dieser haben. Daraus ergibt sich auch die Notwendigkeit nach einem entsprechenden Schutz der dort verarbeiteten Daten, der wiederum aufgrund der Komplexität dieser Prozesse nicht alleine durch den Nutzer sichergestellt werden kann. In die Pflicht genommen werden deshalb Cloud-AnbieterInnen, die notfalls durch entsprechende Gesetze zur Sicherstellung eines ausreichenden Schutzes verpflichtet werden müssen. Da immer häufiger Unternehmen, die zum Beispiel KundInnendaten verarbeiten, auf Cloud-Lösungen setzen, treten auch diese Unternehmen die Verantwortung für die Datensicherheit teilweise an den/die Cloud-AnbieterIn ab und müssen sich auf bestimmte Versprechen, die beispielsweise in SLAs festgehalten werden, verlassen können. Sollte eine Einhaltung nicht erfolgen, können empfindliche Vertragsstrafen drohen, weshalb es naheliegend ist, dass die Cloud-Anbieter der Erfüllung dieser Vereinbarungen so gut wie möglich nachkommen werden. (vgl. [Baun, Kunze, Nimis, Tai 2011, S. 74f])

Auf dieser Grundlage muss die Frage nach den technischen und institutionellen Möglichkeiten dieser Anforderungen beantwortet werden. Für die Vertraulichkeit bietet, wie in [Baun, Kunze, Nimis, Tai 2011] argumentiert, eine Verschlüsselung auch auf Rechnern eines Cloud-Rechenzentrums einen ausreichenden Schutz vor Einsicht durch Unbefugte. Die Befürchtung, Cloud-AnbieterInnen können auf alle Daten der im Rechenzentrum befindlichen Rechner zugreifen, trifft also höchstens zu, wenn diese Daten nicht ausreichend stark verschlüsselt sind. Selbst riesige Unternehmen wie Amazon können verschlüsselte Daten nicht ohne enorme Anstrengungen entsch-

lüsseln und Verfahren wie das von [Oppitz, Tomsu 2018] beschriebene TLS und VPNs sorgen für Sicherheit durch eine verschlüsselte Datenübertragung auf netzwerktechnisch abgesicherten Wegen. Bei der Integrität der Daten gilt im Bereich der böswilligen Veränderung dieser Daten das gleiche wie für die Vertraulichkeit. Unter dem Aspekt der Verlustmöglichkeit von Daten durch beispielsweise Naturkatastrophen kann angenommen werden, dass die Integrität in Rechenzentren großer Cloud-AnbieterInnen deutlich eher gewährleistet werden kann. AnbieterInnen wie zum Beispiel AWS nutzen Replikation zwischen den Rechenzentren einer Region, wobei diese Rechenzentren über Notfallstromversorgung und geographische Entfernung mit hoher Wahrscheinlichkeit nicht gleichzeitig von Naturkatastrophen betroffen sind. (vgl. [AWS 2019])

Durch exakt diese Eigenschaften wird auch die Verfügbarkeit der Services sichergestellt. Fällt ein Dienst aus, kann in wenigen Sekunden ein Duplikat des bisherigen Dienstes bereitgestellt werden. Mithilfe von zum Beispiel bereits in PaaS-Produkte integrierten Mechanismen lassen sich außerdem wirksam und ohne zusätzlichen Aufwand beim Verwender dieser Produkte Angriffe, wie zum Beispiel die unter 4.2 Ebenen der Datensicherheit erwähnten DDoS-Attackten unterbinden. Auch der laut [Oppitz, Tomsu 2018], [BSI 2016] und [Laue, Stiemerling 2010] anfälligste Aspekt der Datensicherheit Authentizität wird beim Cloud-Computing häufig bereits durch den Anbieter solcher Dienste angegangen. Im Einhergang mit Autorisierungsmechanismen ist es möglich feingranular beispielsweise die Rechte zum Einsehen oder Verändern von kritischen Diensten einzuschränken, sodass lediglich wenige Personen Zugriff haben. Diese wenigen Personen können dann erhöhte Authentifizierungsaufwände auf sich nehmen – als Beispiel sei hier die *Multi-Factor Authentication* (MFA) genannt – die das Eindringen in geschützte Bereiche nahezu unmöglich machen. Unterstützt wird dies durch das von [Baun, Kunze, Nimis, Tai 2011] genannte Auditing, welches gleichzeitig die Forderung nach Verbindlichkeit durchgeführter Änderungen herstellt.

Für all die soeben genannten Aspekte der Datensicherheit und die dazugehörigen Lösungen bieten Cloud-Anbieter entsprechende Produkte entweder bereits integriert oder gegen zusätzliches Entgelt an. Am Beispiel AWS ist erkennbar, dass die Produkte modularisiert angeboten werden. Um nur einige Beispiele zu nennen: AWS VPC[10] bietet Vertraulichkeit durch abgeschirmte Netzwerkverbindungen, AWS Identity

10 https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

Access Management[11] stellt ohne Aufpreis eine hochkonfigurierbare Autorisierunglösung dar und AWS CloudTrail[12] zeichnet jede Veränderung am AWS Konto und jedes Infrastrukturänderung auf und bietet so ein vollständiges Auditing-Tool, mithilfe dessen die Verbindlichkeit gewährleistet werden kann. Diese Modularisierung und Auslagerung von Mechanismen zur Herstellung von Datensicherheit kann also mit wenig Aufwand in Systeme eines Unternehmens eingebunden werden. Insofern trägt das Cloud-Computing tatsächlich zur einfachen Verbreitung und modularisierten Verwendung des *cross-cutting concerns* Datensicherheit bei internetbasierten Dienste bei, womit die These dieser Arbeit als zutreffend gelten kann.

7 Fazit

In dieser Arbeit wurden die beiden Trend-Themen Cloud-Computing und Datensicherheit intensiv beleuchtet und auf ihre Vereinbarkeit geprüft. Nachdem die Begriffe zunächst auf Grundlage verschiedener Quellen definiert wurden, folgte die Aufstellung der These, dass das Cloud-Computing durch Modularisierung zur einfachen Verbreitung von Datensicherheit auf internetbasierte Dienste dient. Anschließend wurde die Entwicklung der dezentralen Datenverarbeitung und die damit einhergehende Entstehung des heutigen Internets beschrieben. Auch der Begriff des Moduls beziehungsweise der Modularisierung wurde genauer erklärt. Um Datensicherheit im Folgenden wohldefiniert verwenden zu können, wurde diese auf vier verschiedenen Ebenen (technisch, individuell, institutionell, gesellschaftlich) betrachtet. Neben den technischen Aspekten des Datenschutzes (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Verbindlichkeit und Autorisation) wurden außerdem die Auswirkungen fehlender Datensicherheit auf Privatpersonen und die Schwierigkeiten beim Verwenden entsprechender Hilfsmittel dargestellt. Wie herausgearbeitet wurde, sehen sich auch Institutionen wie Unternehmen oder Bundesämter Risiken beim Herstellen von Datensicherheit ausgesetzt, weshalb Empfehlungen und Zertifizierungsmechanismen, welche zum Beispiel vom Bundesamt für Sicherheit in der Informationstechnik vorgegeben werden, vorgestellt wurden. Zuletzt wurde auch die Rolle von Datensicherheit für die gesamte Gesellschaft angeschnitten, wobei vor allem Bezug auf die entsprechenden Gesetze genommen wurde. Mit diesen unterschiedlichen Perspektiven wurden als nächstes Werke verschiedener Autoren analysiert und auf deren Aus-

11 https://aws.amazon.com/de/iam/
12 https://aws.amazon.com/de/cloudtrail/

sagen im Bezug auf Cloud-Computing überprüft. Wie sich herausstellte, identifizierten alle AutorInnen unterschiedliche Risiken im Umgang mit Cloud-Computing, waren sich jedoch darin einig, dass ein gut geplantes Risikomanagement der Schlüssel zum Erfolg beim Verwenden von Cloud-Computing-Diensten darstellt. Zum Schluss wurden diese Argumentationen durch den Autor dieser Arbeit zur Beantwortung der Fragestellung ebenjener verwendet und eine begründete Aussage zu den Vorteilen des Cloud-Computings im Bezug auf Datensicherheit getroffen. Als Resultat steht der Beweis, dass durch verschiedene Produkte, die modularisiert in internetbasierte Systeme eingebunden werden können, eine Erfüllung der technischen Voraussetzungen für Datensicherheit vereinfacht wird, wodurch die These dieser Arbeit bestätigt wurde.

Nicht eingehender betrachtet wurde der zuvor abgegrenzte Begriff des Datenschutzes, der durch den starken Bezug auf persönliche Daten die Datensicherheit als Grundlage voraussetzt. Auch lag der Fokus dieser Arbeit nicht auf der Debatte über das Misstrauen, dass besonders amerikanischen Cloud-Anbietern aufgrund der amerikanischen Gesetzeslage oder Vorfällen wie den Zugriff auf private Daten durch die amerikanische National Security Agency entgegengebracht wird. Spannend wäre allerdings genau diese Frage nach der Einhaltung und Überprüfung der durch Cloud-Anbietern versprochenen Dienstleistungen. Die zwischen Cloud-Anbieter definierten SLAs mögen ein wichtiger Baustein sein, doch wie kann die Einhaltung dieser Verträge überprüft werden? Wie kann sichergestellt werden, dass angepriesene Verfahren und Automatismen intern tatsächlich wie versprochen umgesetzt werden? Diese Fragen bleiben leider unbeantwortet.

Fest steht jedoch, dass mithilfe von Cloud-Computing gut bekannte Standards im Aufbau und Betrieb von Infrastruktur für Software-Systeme gegen Geld verfügbar gemacht werden und so ein großer Teil der Probleme, die zum Beispiel jedes Unternehmen sonst auf eigene Weise lösen müsste, externalisiert werden und so ein stärkerer Fokus auf das Kerngeschäft dieser Unternehmen möglich ist.

8 Abkürzungsverzeichnis

BITKOM	Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
C5	Cloud Computing Compliance Controls Catalogue
DDoS	Distributed Denial of Service
ENISA	European Network and Information Security Agency
IaaS	Infrastructure as a Service
KRITIS	Kritische Infrastrukturen
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
SaaS	Software as a Service
SLA	Service Level Agreement
VPC	Virtual Private Cloud
VPN	Virtual Private Network

9 Abbildungsverzeichnis

10 Rechtsquellenverzeichnis

[BSIG 1991] BSI-Errichtungsgesetz vom 17. Dezember 1990 (BGBl. I S. 2834), zuletzt geändert durch Artikel 11 der Verordnung vom 25. November 2003 (BGBl. I S. 2304).

[BSIG 2009] BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885).

11 Literatur- / Quellenverzeichnis

[Abbate 2000] Abbate, Janet (2000): Inventing the Internet, Cambridge, London: MIT Press, 2000.

[Adelmeyer, Petrick, Teuteberg 2018] Adelmeyer, Michael; Petrick, Christopher; Teuteberg, Frank (2018): IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen, in: Essentials, Wiesbaden: Springer Fachmedien, 2018.

[AWS 2019] Amazon Web Services (2019): Rechenzentren, in: https://aws.amazon.com/de/compliance/data-center/data-centers/, abgerufen 13.03.2019.

[Baun, Kunze, Nimis, Tai 2011] Baun, Christian; Kunze, Marcel; Nimis, Jens; Tai, Stefan (2011): Cloud Computing - Web-basierte dynamische IT-Services, 2. Auflage, Berlin, Heidelberg: Springer-Verlag, 2011.

[Behrendt, Zeppenfeld 2008] Behrendt, Jens; Zeppenfeld, Klaus (2008): Web 2.0, in: Informatik im Fokus, Berlin, Heidelberg: Springer, 2008.

[BSI 2016] Bundesamt für Sicherheit in der Informationstechnik (2016): Sichere Nutzung von Cloud-Diensten, in: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf?__blob=publicationFile&v=8, abgerufen 13.03.2019.

[BSI 2019] Bundesamt für Sicherheit in der Informationstechnik (2019): Technische Richtlinien, in: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html, abgerufen 13.03.2019.

[Böhringer, Bühler, Schlaich, Sinner 2014] Böhringer, Joachim; Bühler, Peter; Schlaich, Patrick; Sinner, Dominik (2014): Internet, in: Kompendium der Mediengestaltung, X.media.press. Berlin, Heidelberg: Springer Vieweg, 2014.

[Dudenredaktion o.J.] Dudenredaktion (o. J.): „Wolke“ auf Duden online, in: https://www.duden.de/node/657917/revisions/1995278/view, abgerufen 13.03.2019.

[Georg, Reddy, France 2004] Geri Georg, Raghu Reddy, Robert France (2004): Specifying Cross-Cutting Requirement Concerns, in: T. Baar, A. Strohmeier, A.

Moreira, S.J. Mellor (Eds.): «UML» 2004 — The Unified Modeling Language. Modeling Languages and Applications, UML 2004, Lecture Notes in Computer Science, vol 3273, S. 113-127, Berlin, Heidelberg: Springer, 2004.

[Hohnen, Pollmanns, Feldhusen 2013]
Thomas Hohnen, Judith Pollmanns, Jörg Feldhusen (2013): Cost-Effects of Product Modularity – An Approach to Describe Manufacturing Costs as a Function of Modularity, in: M. Abramovici, R. Stark (Eds.): Smart Product Engineering, S. 745-754, Berlin, Heidelberg: Springer, 2013.

[Joint Task Force for Computing Curricula 2005]
Joint Task Force for Computing Curricula (2005): Computing Curricula 2005 – The Overview Report, in: https://web.archive.org/web/20160821201314/http://www.acm.org/education/curric_vols/CC2005-March06Final.pdf, abgerufen 13.03.2019.

[Kappes 2013]
Kappes, Martin (2013): Netzwerk- und Datensicherheit - Eine praktische Einführung, 2. Auflage, Wiesbaden: Springer Vieweg, 2013.

[Krösmann 2016] Krösmann, Christoph (2016): Sicherheit für IT-Unternehmen das Thema des Jahres, in: https://www.bitkom.org/Presse/Presseinformation/Sicherheit-fuer-IT-Unternehmen-das-Thema-des-Jahres.html, abgerufen 13.03.2019.

[Krösmann 2017] Krösmann, Christoph (2017): IT-Sicherheit, Cloud Computing und Internet of Things sind Top-Themen des Jahres in der Digitalwirtschaft, in: https://www.bitkom.org/Presse/Presseinformation/IT-Sicherheit-Cloud-Computing-und-Internet-of-Things-sind-Top-Themen-des-Jahres-in-der-Digitalwirtschaft.html, abgerufen 13.03.2019.

[Kroschel 1991]
Kroschel, Kristian (1991): Datenübertragung, Berlin, Heidelberg: Springer, 1991.

[Laue, Stiemerling 2010]
Laue, Philip; Stiemerling, Oliver (2010): Identitäts- und Zugriffsmanagement für Cloud Computing Anwendungen, in: Datenschutz und Datensicherheit – DuD (2010), Volume 34, Issue 10, S. 692-697, Wiesbaden: Springer Fachmedien, 2010.

[Mell, Grance 2011]
Mell, Peter; Grance, Tim (2011): The NIST Definition of Cloud Computing, in:

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, abgerufen 13.03.2019.

[Oppitz, Tomsu 2018] Oppitz, Marcus; Tomsu, Peter (2018): Inventing the Cloud Century: How Cloudiness Keeps Changing Our Life, Economy and Technology, Cham: Springer International Publishing AG, 2018.

[DuD 2012] DuD (2012): BMWi: „Kompetenzzentrum Trusted Cloud“ für Cloud Computing-Forschungsprogramm, in: Datenschutz und Datensicherheit – DuD (2012), Volume 36, Issue 2, S. 140-140, Wiesbaden: Springer Fachmedien, 2012.

[Pousttchi 2017] Pousttchi, Key (2017): Digitale Transformation, in: Enzyklopädie der Wirtschaftsinformatik http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/Informatik—Grundlagen/digitalisierung/digitale-transformation, abgerufen 13.03.2019.

[Sehgal, Bhatt 2018] Sehgal, Naresh Kumar; Bhatt, Pramod Chandra P. (2018): Cloud Computing - Concepts and Practices, Cham: Springer International Publishing AG, part of Springer Nature, 2018.

[Streim 2018] Streim, Andreas (2018): Blockchain wird zu einem Top-Thema in der Digitalwirtschaft, in: https://www.bitkom.org/Presse/Presseinformation/Blockchain-wird-zu-einem-Top-Thema-in-der-Digitalwirtschaft.html, abgerufen 13.03.2019.

[Strube 2010] Strube, Philipp (2010): Amazons Web Services im Überblick: Das Cloud-Computing-Universum, in: https://t3n.de/magazin/amazons-web-services-uberblick-cloud-computing-universum-224005/, abgerufen 13.03.2019.

[Witt 2010] Witt, Bernhard (2010): Datenschutz kompakt und verständlich: Eine praxisorientierte Einführung, Wiesbaden: Vieweg+Teubner (Springer Fachmedien), 2010.

[Wohltmann, Lackes, Siepermann 2009] Wohltmann, Hans-Werner; Lackes, Richard; Siepermann, Markus (2009): Daten, in: Gabler Wirtschaftslexikon https://wirtschaftslexikon.gabler.de/definition/daten-30636/version-133420, abgerufen 13.03.2019.

[Zhang, Cheng, Boutaba 2010] Zhang, Qi; Cheng, Lu; Boutaba, Raouf (2010): Cloud computing: state-of-the-art and research challenges, in: Journal of Internet Services

and Applications 1, S. 7–18, Waterloo, Canada: The Brazilian Computer Society, 2010.