IT kompakt

Daniel Christian Leeser

Digitalisierung in KMU kompakt

Compliance und IT-Security

Springer Vieweg

IT kompakt

Die Bücher der Reihe „IT kompakt“ zu wichtigen Konzepten und Technologien der IT:

- ermöglichen einen raschen Einstieg,
- bieten einen fundierten Überblick,
- eignen sich für Selbststudium und Lehre,
- sind praxisorientiert, aktuell und immer ihren Preis wert.

Weitere Titel in der Reihe http://www.springer.com/series/8297

Daniel Christian Leeser

Digitalisierung in KMU kompakt

Compliance und IT-Security

Springer Vieweg

Daniel Christian Leeser
Kassel, Deutschland

ISSN 2195-3651 ISSN 2195-366X (electronic)
IT kompakt
ISBN 978-3-662-59737-8 ISBN 978-3-662-59738-5 (eBook)
https://doi.org/10.1007/978-3-662-59738-5

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg
© Springer-Verlag GmbH Deutschland, ein Teil von Springer Nature 2020
Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.
Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.
Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Über die letzten Jahre hinweg konnte ich in meiner Tätigkeit als IT-Systemingenieur sowie durch ein eigenes Gewerbe viele KMU bei der Einführung und Administration neuer IT-Hardware, Software oder auch der Einführung von Produkten des Cloud-Computings unterstützen. Dabei konnte ich nicht zuletzt durch die vielen verschiedenen Eindrücke in verschiedenen Unternehmen vieles über den Umgang von KMU mit dem Geschäftsfaktor IT lernen. Über die Jahre hinweg und nicht zuletzt auch durch mein berufsbegleitendes Studium der Wirtschaftsinformatik sowie durch eigenes Gewerbe ist der Wunsch entstanden, ein Buch darüber zu schreiben, welche Potenziale für KMU in der Digitalisierung liegen und worin deren Anforderungen und auch Ängste liegen. Die genauen Beweggründe werde ich Ihnen auf den kommenden Seiten erläutern.

Mein Ziel mit diesem Buch ist es, die Thematik Digitalisierung in Bezug auf IT-Security und IT-Compliance im Bereich von Geschäfts- und Produktionsprozessen greifbarer zu machen, Ängste durch Informationen im Sinne von Beispielen zu ersetzen und zu motivieren, die kommenden spannenden Jahre mit positiver Energie für das jeweilige Unternehmen zu beschreiten. Es handelt sich dabei um eine Einführung in die Thematik, auch für Themenfremde, mit dem Hauptaugenmerk auf Verständnis und Heranführung an die Bereiche IT-Compliance und IT-Security. Dabei werden die Teilbereiche weitestgehend oberflächlich, im Rahmen von Digitalisierung in KMU, behandelt, um eine Abschreckung durch weitere Fachbegriffe und damit verbundenen, komplexen

Thematiken zu vermeiden. Deshalb handelt es sich bei dieser Ausarbeitung um eine Verknüpfung aus Praxis und Theorie. Dies wird gestützt anhand von Beispielen aus der Praxis, persönlichen Erfahrungswerten und durch Studien sowie Umfragen. Die Umsetzung in der Praxis ist im individuellen Fall verschieden. Daher sollten Schritte in der Praxis nur nach Beratung durch und in Zusammenarbeit mit entsprechenden Experten/Consultants stattfinden. Diese Ausarbeitung versteht sich daher als Bericht über den wahrgenommenen Stand in der Praxis, gestützt durch Studien und Umfragen, und zur Erweiterung des individuellen Know-hows, nicht aber als Umsetzungsleitfaden. Daher kann diese Ausarbeitung etwa in Verhandlungssituationen dabei helfen, besser argumentieren zu können und dazu beitragen, in Digitalisierungsprojekten besser verstehen zu können, welche Schritte aufgrund welcher Notwendigkeit entstehen.

Ich möchte diese Gelegenheit auch nutzen, um den vielen Gesprächspartnern in den Unternehmen, für die ich tätig war, für ihre offenen und ehrlichen Antworten zu danken. Außerdem möchte ich meinen Freunden und vor allem meiner Familie für das aufgebrachte Verständnis in den Zeiten danken, in denen ich mich der Wirtschaftsinformatik und der Ausarbeitung dieses Buches gewidmet habe.

Dank gebührt auch meinem Arbeitgeber, der Hermanns HTI-Bau GmbH u. Co. KG, für die Unterstützung und die offenen und fördernden Gespräche, insbesondere mit meinem Vorgesetzten Christian Becker.

Ein besonderer Dank geht an Hendrik Klöters, Sebastian Rode, Dr. Philipp Bitzer und Dr. René Wegener. Ohne Euch würden mir heute viele wertvolle Erfahrungen und Erlebnisse fehlen. Danke, dass Ihr mich so offen aufgenommen habt und mich auf meinem Weg unterstützt, motiviert und mir neue spannende Perspektiven aufzeigt!

Vielen Dank auch an Frau Sophia Leonhard und Herrn Martin Börger vom Verlag Springer Vieweg für die professionelle redaktionelle Unterstützung.

Kassel, im Juni 2019 Daniel Christian Leeser

Inhaltsverzeichnis

1 Einführung und Motivation 1
1.1 Feststellung der Ausgangssituation 7
1.2 Zielsetzung 11
1.3 Vorgehensweise 12
1.4 IT – kein reiner Kostenfaktor 14
Literatur 19

2 Definitionen, Erläuterungen und Abgrenzung 21
2.1 Definition und Abgrenzung des Begriffs KMU 22
2.2 Definition der Entscheidungsträger in KMU 26
2.3 Digitalisierung von Geschäfts- und Produktionsprozessen 30
2.4 IT-Compliance 48
2.5 IT-Security 51
Literatur 59

3 Lokale Herausforderungen durch Digitalisierung 63
3.1 Lokale IT-Infrastruktur 64
3.2 Anforderungen und Probleme aus Sicht von KMU . . . 67
3.3 Anforderungen an IT-Security in lokaler IT-Infrastruktur abbilden 73
3.4 Umsetzung von Compliance-Maßnahmen 95
3.5 Abgrenzung zu Cloudsystemen 99
Literatur 108

4 Cloud-Computing als Herausforderung für KMU . . . 113
4.1 Anforderungen und Probleme aus Sicht von KMU 113
4.2 IT-Security abbilden – Möglichkeiten und Anforderungen 116
4.3 Umsetzung von Compliance-Maßnahmen 122
4.4 Abgrenzung zu On-Premises IT-Infrastruktur 126
Literatur 133

5 Entscheidungsfaktoren und Fazit 135
5.1 Diskussion der Aussagen aus den Kap. 3 und 4 136
5.2 Entscheidungsfaktoren und Handlungsmöglichkeiten 145
5.3 Fazit und Zukunftsausblick 187
Literatur 194

Einführung und Motivation

1

Ich beginne dieses Buch vielleicht etwas unüblich, und zwar stelle ich Ihnen und mir die rhetorische Frage „*Warum wurde dieses Buch geschrieben?*“

In den vergangenen Jahren konnte ich in meiner Funktion als IT-Systemingenieur sowie durch eigenes Gewerbe Einblicke in viele kleine und mittlere Unternehmen gewinnen. Ich konnte deren Sorgen und Ängste in Bezug auf IT erkennen, aber auch Potenziale und positive Effekte durch die fortschreitende Digitalisierung aktivieren und feststellen, wie durchaus auch die Produktivität des jeweiligen Unternehmens mit der Einführung von beispielsweise Cloudprodukten stieg. Dennoch musste ich auch häufig feststellen, dass gängige Anforderungen wie zum Beispiel jene der Datenschutz-Grundverordnung (EU-DSGVO) oder auch weitere IT-Compliance-Anforderungen, die beispielsweise im Zuge der Zusammenarbeit mit Zulieferern und Endkunden entstanden, und damit in der Folge auch die IT-Sicherheit eher auf die leichte Schulter genommen wurden. Denn die technische Umsetzung einiger dieser Anforderungen im Bereich der IT fiel anschließend in meinen Aufgabenbereich. Vielmehr wurden diese Punkte stiefmütterlich betrachtet und die Digitalisierung in den häufigsten Fällen abgelehnt, mit der Begründung, dass sie IT-Sicherheit und IT-Compliance sogar gefährde, da Anforderungen nicht umgesetzt werden könnten. De facto wurde also angeführt, dass eben diese Punkte, welche selten bereits

© Springer-Verlag GmbH Deutschland, ein Teil von Springer Nature 2020 D. C. Leeser, *Digitalisierung in KMU kompakt*, IT kompakt, https://doi.org/10.1007/978-3-662-59738-5_1

richtig implementiert waren, die Digitalisierung zum Angstfaktor machen würden. Da hier ein Widerspruch besteht und KMU je nach Definition über 99 % der deutschen Unternehmen ausmachen (siehe Abschn. 2.1), ist es mir ein persönliches Anliegen, Starthilfe durch Informationen und Beispiele zu geben und KMU einen Weg aufzuzeigen, wie Digitalisierung ermöglicht werden und sich vom Angstfaktor zum Potenzialträger entwickeln kann.

In dieser Ausarbeitung finden Sie deshalb verschiedene Definitionen und eine grobe Übersicht über beispielhafte Handlungsmöglichkeiten sowie Erfahrungswerte und Beispiele. Zusammenfassend formuliert, eine Verknüpfung von theoretischen Inhalten mit praktischen Erfahrungen. Die Theorieinhalte, Erfahrungswerte und Praxisbeispiele sind dabei aus meiner Tätigkeit als IT-Systemingenieur in der IT-Administration und der Einführung von IT-Produkten sowie meinem berufsbegleitenden Studium der Wirtschaftsinformatik und dem Austausch mit vielen Geschäftsführern von KMU und im Rahmen meines eigenen Gewerbes entstanden. Bitte bedenken Sie, dass dieses Werk nicht den Anspruch auf Vollständigkeit erhebt, denn viele der zentralen Punkte in diesem Feld sind einer ständigen Evolution unterworfen. Vor allem im Themenbereich dieser Ausarbeitung gibt es regelmäßige Änderungen. In diesem Buch wird beispielhaft aufgezeigt, wie IT bei der Umsetzung von Compliance unterstützen kann und welche Anforderungen es durch IT-Compliance geben könnte. Die Inhalte sind jedoch nicht zur Umsetzung gedacht. Wie Sie bereits dem Vorwort entnehmen konnten, sollte ein IT-Projekt immer mit entsprechenden Experten durchgeführt werden, da die Anforderungen im individuellen Fall grundlegend verschieden sein können und jeweils entsprechende andere Lösungen/Prozesse etabliert werden müssen.

Mir ist es daher wichtig, dass Ihnen bewusst ist, dass es sich hierbei um Erfahrungswerte und Beispiele aus der Praxis handelt, also um reine Informationen zur Erweiterung Ihres Know-hows und zur Erleichterung des Verständnisses der IT, insbesondere im Bereich von Digitalisierungsprojekten. Bei der Umsetzung von Projekten wurden immer entsprechende Experten wie Datenschutzberater, Datenschutzbeauftragte sowie themenbezogen Consultants hinzugezogen. Deshalb möchte ich Ihnen mit dieser

Ausarbeitung einen Einblick in die Praxis geben und Ihnen aufzeigen, wo und wann Sie Experten hinzuziehen sollten und wie man die Dinge auch aus anderen Blickwinkeln angehen kann. Doch muss Ihnen auch bewusst sein, dass Ihnen diese Informationen nur helfen können, wenn Sie selbst anfangen zusammen mit Experten, ‚umzusetzen', und Ihnen bewusst ist, dass es keine Universallösung für Digitalisierung sowie IT-Security und IT-Compliance gibt und diese Ausarbeitung auch keine solche darstellt, sondern immer der individuelle Fall betrachtet werden muss. Somit soll auch darauf aufmerksam gemacht werden, dass Digitalisierung, auch unabhängig von IT-Security und IT-Compliance, regelmäßigen Investitionen bedarf, dies wird jedoch im Laufe der Ausarbeitung nochmals aufgegriffen.

Mein erklärtes Ziel ist es, nicht die Digitalisierung aufzuzwingen, sondern Wege aufzuzeigen, wie diese Ihrem Unternehmen helfen kann. Des Weiteren möchte ich Ihnen Definitionen verschiedener Technologien und gängiger Begriffe aufzeigen, damit Sie im IT-Urwald den Durchblick behalten können und auch in einem möglichen Digitalisierungsprojekt verstehen, welche Tätigkeiten die Projektbeteiligten verrichten und wieso einige Punkte durchaus Investitionen erfordern. Daraus resultierend wünsche ich mir, dass es Ihnen gelingt, zusammen mit der Beratung und Umsetzung durch Experten eine Digitalisierungsstrategie für Ihre Firma auszuarbeiten, die sie langfristig konkurrenzfähiger macht und die IT-Compliance und IT-Security einhält, ohne dass diese Punkte einen Angstfaktor darstellen.

Wie bereits eingehend angesprochen, machen KMU in Deutschland je nach Quelle über 99 % der gesamten deutschen Unternehmen aus (siehe Abschn. 2.1). Damit Sie diese Zahlen besser einordnen können, erfolgt im Definitionsbereich dieses Werkes ebenfalls eine Abgrenzung des Begriffs KMU. Letztlich habe ich mir beim Verfassen dieser Ausarbeitung und bereits davor immer wieder die Frage gestellt: „*Wie können KMU in Deutschland weiterhin auch gegen internationale Konkurrenz bestehen, die durch die Digitalisierung verstärkt zunehmen wird?*". Damit diese Frage beantwortet werden kann, lade ich Sie zunächst auf eine kleine Reise in die Hintergründe der IT-gestützten Wirtschaft ein.

Etwa ab den 1980er-Jahren hat IT erstmals dazu beigetragen, dass die Ökonomie weltweit entscheidend verändert wurde. Deren ökonomische Prozesse sowie die Art des Handels wurden massiv beschleunigt. Zum einen liegt dies an der Einführung des Personal Computer, kurz: PC und zum anderen ist es später in der Folge des Zugangs zum Internet erstmals möglich geworden, auch im Ausland Waren zu beziehen, die es dort womöglich günstiger gibt als im eigenen Land. Vielleicht haben auch Sie mit Ihrem Unternehmen bereits einen eigenen Onlineshop als zusätzlichen Absatzort in Nutzung oder nutzen die vielen verfügbaren Plattformen im Internet, um Ihren Absatzmarkt auszubauen.

In diesem Zusammenhang ist klar zu erkennen, dass diese Entwicklung für den Konsumenten sein Gutes haben mag, für die Unternehmen jedoch zu verstärkten Konkurrenzsituationen führen kann. Vergleicht man die aktuelle Entwicklung mit der der letzten Jahrzehnte, so ist festzustellen, dass es eine klare Trendwende zu geben scheint. Egal wo Sie hinsehen, lesen Sie von ‚Digitalisierung', ‚Industrie 4.0', der ‚Cloud' oder auch von neuen ‚disruptiven Geschäftsmodellen'. Doch was bedeutet das eigentlich für Sie? Da ich aus erster Hand weiß, wie sehr eine Entscheidungsfindung durch nicht abschätzbare Faktoren negativ beeinflusst werden kann, werden auch diese Begriffe in dieser Ausarbeitung verständlich definiert.

Eine grundlegende Form der Digitalisierung werden Sie bereits in Ihrem Unternehmen vorliegen haben. So haben Sie in Ihrem Unternehmen mit großer Wahrscheinlichkeit bereits einen Server, einige Computerarbeitsplätze sowie Drucker und Scanner und vermutlich auch ein System zur Verwaltung der Kunden- und Warendaten. All dies gehört in gewisser Weise bereits zur Digitalisierung, da es sich hierbei um ‚digitales Arbeiten' handelt.

Für Sie als Unternehmen bedeutet dies, dass Sie nur konkurrenzfähig sind und es auch bleiben können, wenn Sie bereits auf digitale Datenverarbeitung setzen. Insgesamt ist also feststellbar, dass Unternehmen am Markt zwangsläufig auf IT angewiesen sind, um mit der Konkurrenz im In- und Ausland mithalten zu können. Dabei kommt es sowohl auf die Sicht in Richtung des Absatzmarktes als auch auf die interne Unternehmenssicht und die Zusammenarbeit mit Lieferanten und Geschäftspartnern an.

Das heißt, es kommt darauf an, wie Ihre internen Prozesse hinsichtlich den klassischen Funktionen Beschaffung, Produktion sowie Absatz und somit auch Ihrer internen Organisation gestaltet sind.

Für ein kosteneffizientes Beschaffen, Produzieren und Absetzen eines Betriebs bedarf es meist unter anderem der Planung mithilfe von Supply-Chain-Management-Tools (SCM), Customer-Relationship-Management-Tools (CRM), Enterprise-Resource-Planing-Tools (ERP) und vielem mehr. Eine Umfrage des Statistischen Bundesamtes aus dem Jahr 2017 zeigt jedoch, dass beispielsweise CRM-Software noch nicht durchdringend in allen Wirtschaftszweigen angekommen ist. So nutzen nur rund 54 Prozent aller Gewerbe in Deutschland eine solche Lösung (vgl. Statista 2019).

Bevor Sie sich die Frage stellen, was diese Begriffe bedeuten, möchte ich sie kurz erklären, aber auch betonen, dass sie das Thema dieser Ausarbeitung nur am Rande begleiten. Supply-Chain-Management ermöglicht prinzipiell das Managen sowie Organisieren der Lieferkette und somit auch das Optimieren dieser Prozesse. Ein Customer-Relationship-Management hingegen bietet Ihnen als Unternehmen unter anderem die Möglichkeit, Kundendaten zu verwalten, zu erkennen, welche Produkte ein Kunde häufig kauft, und somit auch abschätzen zu können, welche Produkte der Kunde in Zukunft vielleicht kaufen könnte, sowie viele weitere Möglichkeiten in Bezug auf die Verwaltung von Kundendaten und Kundenkommunikation. Das Enterprise-Resource-Planing hingegen ermöglicht Ihnen beispielsweise die Planung Ihrer Ressourcen im Unternehmen. Je nach Anforderungszweck kann dies Arbeitskraft oder auch die Verfügbarkeit von Waren oder Dienstleistungen sein. Alle Tools bieten Ihnen in ihren jeweiligen Bereichen die Chance, durch Optimierungen Zeit, Geld und Ressourcen einzusparen und erfolgreicher im Sinne des Unternehmens zu wirtschaften.

Diese Tools sind, wie bereits angesprochen, in Ihrem Unternehmen vielleicht schon vorhanden, dennoch kommen durch fortschreitende Digitalisierung neue produktivitätssteigernde Tools hinzu, die ich Ihnen nicht vorenthalten möchte. Big Data und Business-Intelligence-Methoden erweitern die bereits angesprochenen

Tools dabei um Möglichkeiten der Informationserfassung und -verarbeitung, die ein Mensch im entsprechenden Zeitraum nicht erfassen und auswerten könnte. Doch mit Industrie 4.0 und mit Cloud-Computing stehen Unternehmen bereits vor der nächsten Herausforderung in Bezug auf die Digitalisierung und Anwendung von IT. Damit Firmen auch weiterhin erfolgreich am Markt teilnehmen können, müssen diese sich mit den Themen der Digitalisierung befassen (vgl. Schmiech 2018, S. 25). Dazu zählen etwa Internet of Things (IoT), künstliche Intelligenz (KI) und Cloud-Computing.

Ich kann mir vorstellen, dass bei Ihnen bereits nach dieser kurzen Einführung die ein oder andere Fragestellung entstanden ist. Dies ist jedoch kein Grund, abgeschreckt zu sein. Auf den nachfolgenden Seiten werden die Begriffe zunächst definiert und anschließend gegenübergestellt, welche Herausforderungen und Probleme bei einem reinen lokalen Betrieb von IT (‚On-Premises') und bei einer Cloud-Infrastruktur auftreten können. In Kap. 5 werden die Ergebnisse diskutiert, beispielhafte Handlungsmöglichkeiten und grobe Entscheidungsfaktoren abgeschätzt sowie ein Fazit gezogen.

Mir ist wichtig, dass ich Sie ermutigen kann, die richtigen Experten für Ihr Digitalisierungsprojekt zu gewinnen und Ihnen in diesem Zusammenhang die Angst vor den Faktoren IT-Compliance und IT-Security nehmen kann. Des Weiteren ist es mir wichtig, dass Sie IT nach dem Lesen dieser Ausarbeitung nicht mehr nur als Kostenfaktor ansehen, der sich nicht zu rentieren scheint, sondern als Teil der Geschäftsstrategie.

Ich möchte Ihnen in diesem Zusammenhang gerne einen Merksatz mitgeben, der sich aus der Praxis ergeben hat, über die Jahre hinweg zu meiner grundsätzlichen Einstellung geworden ist, und der sich in so gut wie allen Fällen immer wieder bestätigt hat. Die Aussage ist aus meiner Sicht selbsterklärend.

> „Wer jetzt 10 € sparen kann, indem er selbst und ohne Hintergrundwissen sowie externe Hilfe aktiv wird, zahlt im Nachhinein meist 1000 € mehr."

1.1 Feststellung der Ausgangssituation

Dass Digitalisierung gerade auch für mittelständische Unternehmen an Bedeutung gewinnt, zeigt sich vor allem daran, dass diese Digitalisierung zunehmend mehr in ihrer Geschäftsstrategie verankern. Laut einer Studie der Deutsche Telekom AG haben im Jahr 2016 noch 27 Prozent und im Jahr 2017 bereits knapp 42 Prozent der befragten mittelständischen Unternehmen die angesprochene Verankerung vorgenommen (vgl. Deutsche Telekom AG 2017, S. 4).

Des Weiteren ist laut einer repräsentativen Umfrage des Bundesministeriums für Wirtschaft und Energie (BMWi) die durchschnittliche Digitalisierung in KMU im Jahr 2017 auf 52 Prozent gestiegen; 19 Prozent sind demnach bereits hoch digitalisiert (vgl. Bundesministerium für Wirtschaft und Energie (BMWi) und Kantar TNS 2017, S. 10). Es wurden dabei unter anderem die Nutzung von Cloud-Computing, Big Data und die Verwendung von mobilen Endgeräten sowie von mobilem und stationärem Internet als treibende Kräfte hinter der Digitalisierung angenommen (vgl. Bundesministerium für Wirtschaft und Energie (BMWi) und Kantar TNS 2017, S. 10).

Die statistischen Werte decken sich dabei mit den Erfahrungen, die ich in KMU sammeln durfte. Mir ist dabei jedoch aufgefallen, dass sich zumeist der Dienstleistungssektor stärker für Digitalisierung interessiert und die Umsetzung von Projekten beispielsweise in Richtung Cloud-Computing plant. Aber auch Themen wie die Nutzung von VPN-Verbindungen oder die zunehmende Zentralisierung von Diensten auf Terminalservern, um Zugriffe auf die eigenen Server beispielsweise aus dem Home-Office oder von einem externen Einsatzort zu erhalten, spielen weiterhin eine wichtige Rolle. In allen Fällen spielt jedoch immer wieder IT-Compliance und IT-Sicherheit eine wichtige und entscheidende Rolle dabei, wie Teilschritte dieser Digitalisierungsstrategien umgesetzt werden.

So sind unter anderem Datenschutz- und IT-Sicherheitsfaktoren entscheidende Faktoren bei der Durchführung der Migration der lokalen Daten in die sogenannte Cloud. Die Bitkom Research GmbH gibt im Rahmen des ‚Cloud-Monitor 2018' an, dass 97

Prozent der befragten Unternehmen die Konformität mit der seit dem 25.05.2018 gültigen Datenschutz-Grundverordnung als wichtigstes Kriterium sehen (vgl. Bitkom Research GmbH und KPMG AG 2018, S. 7).

Dazu führt eine Studie der Hochschule für Wirtschaft und Recht Berlin an, dass die Zahl derer, die Bedenken hinsichtlich des Datenschutzes hatten, steigt. Nach 60 Prozent im Jahr 2015 hatten im Jahr 2017 bereits 91,3 Prozent entsprechende Bedenken (vgl. Hochschule für Wirtschaft und Recht Berlin und forcont business technology GmbH 2017, S. 6). Laut einer Studie der etventure GmbH zu Digitalisierung in Großunternehmen geben 48 Prozent Sicherheitsanforderungen als blockierend an (vgl. etventure GmbH 2018, S. 6). Daraus lässt sich ableiten, dass auch KMU Probleme mit Sicherheitsanforderungen haben, vor allem, da diesen nicht dieselben finanziellen und personellen Mittel zur Verfügung stehen wie einem Großunternehmen.

Dies deckt sich auch mit der angesprochenen Praxiserfahrung. Häufig stehen wenige personelle Ressourcen mit aktuellem IT-Fachwissen zur Beurteilung von IT-Belangen zur Verfügung. Das häufigste Kriterium gegen die Nutzung von Cloud-Computing und das Auslagern von Daten ist laut einer Umfrage der Bundesdruckerei, die, nach Definition dieser Ausarbeitung (siehe Abschn. 2.1), zu über 50 Prozent unter KMU durchgeführt wurde, das Behalten der Hoheit über die eigene IT (vgl. Bundesdruckerei GmbH und Kantar Emnid 2017, S. 5).

Im Widerspruch zum Behalten der Hoheit über die eigene lokale IT steht jedoch auch, dass lokale Compliance- und Sicherheits-Anforderungen ebenso eingehalten werden müssen. Dazu sind Informationen und Maßnahmen unter anderem in den Veröffentlichungen zur Umsetzung des IT-Grundschutzes des Bundesministeriums für Sicherheit in der Informationstechnik (BSI) dargelegt (vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI) o. J.)

Aus der Praxis ist bekannt, dass vor allem Kleinunternehmen Schwierigkeiten haben, sich an diese Anforderungen zu halten. Größtenteils beschäftigen diese sich wieder verstärkt seit dem Inkrafttreten der Datenschutz-Grundverordnung (EU-DSGVO) mit der Thematik IT-Compliance und IT-Security. Die Entstehung

von Schwierigkeiten kann durch die Studie zur IT-Sicherheit in KMU des BSI aus dem Jahr 2011 bekräftigt werden. Sie gibt in ihrem Fazit zwar an, dass die Unternehmen generell sinnvoll aufgestellt seien, jedoch deutliche Defizite im Bereich der geschäftskritischen IT-Sicherheit aufweisen. Es wird angeführt, dass die entsprechenden Unternehmen sich selbst hinsichtlich ihrer Handlungsmöglichkeiten bei Sicherheitsvorfällen überschätzen und deshalb im Vorfeld keine Dokumentation oder Maßnahmen ergreifen würden (vgl. Bundesamt für Sicherheit in der Informationstechnik 2011, S. 98–99). Das auch im Jahr 2017 noch Herausforderungen hinsichtlich der IT-Sicherheit im Mittelstand, zu dem auch KMU zählen, bestanden, zeigt die repräsentative Studie ‚Studienbericht zur Security Bilanz Deutschland 2017' der techconsult GmbH. Demnach schätzen sich öffentliche und mittelständische Unternehmen branchenübergreifend seit dem Jahr 2014 immer schlechter bezüglich ihrer Sicherheit ein, wohingegen die allgemeine wahrgenommene Gefährdung stetig steige (vgl. techconsult GmbH 2017, S. 6). Festzustellen ist außerdem, dass gerade kleine Unternehmen auf lokaler Ebene verschiedene Risiken in Kauf nehmen. Im Jahr 2017 haben demnach, laut WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, nur 20 Prozent der kleinen und 48 Prozent der größeren Unternehmen mit bis zu 499 Mitarbeitern angegeben jemals eine IT-Sicherheitsanalyse durchgeführt zu haben (vgl. WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH 2017, S. 4).

In Anbetracht der Herausforderungen, die KMU, in der wahrgenommenen Praxis, hinsichtlich der Digitalisierung und insbesondere der Nutzung von Cloud-Diensten sehen, widerspricht diese allgemeine Grundhaltung der IT-Sicherheit. Wie die bereits angeführte Studie des BSI verdeutlicht hat, haben KMU auf lokaler Ebene den Eindruck, dass sie Anforderungen an IT-Sicherheit und geschäftskritische Vorfälle in ihrer eigenen IT am Unternehmensstandort jederzeit problemlos lösen können, stellen jedoch oft an die Cloud Anforderungen, die sie lokal häufig unzureichend abbilden. Die entsprechenden KMU scheinen dabei außer Acht zu lassen, welche Sicherheitsrisiken auch bei dem Betreiben einer lokalen und selbstverwalteten IT-Infrastruktur entstehen können

und welchen Einfluss der Faktor Mensch dabei hat. Bekräftigt wird dies auch durch die Ergebnisse des Cyber-Security Reports 2017 – Teil 2 des Beratungsunternehmens Deloitte, in dessen Rahmen Aussagen von Führungskräften aus mittelständischen und großen Unternehmen in Deutschland ausgewertet wurden. Demnach sehen 75 Prozent der Befragten im leichtfertigen Datenumgang von Mitarbeitern ein höheres Sicherheitsrisiko als in Hacker-Angriffen. Letztere wurden nur mit 50 Prozent als mögliches Sicherheitsrisiko angeführt (vgl. Deloitte Global 2017, S. 14). Im Widerspruch dazu steht, dass nur 46 Prozent der befragten Unternehmen in der bereits benannten Umfrage der Bundesdruckerei ihr Personal regelmäßig zu IT-Sicherheit schulen (vgl. Bundesdruckerei GmbH und Kantar Emnid 2017, S. 5).

Wie Sie nach dem Lesen dieses Unterkapitels feststellen können, gibt es viele Teilbereiche, die Einfluss auf IT-Compliance und IT-Security haben können. Ich möchte abermals betonen, dass Sie sich von diesen Informationen nicht beängstigen lassen sollten. Vielmehr möchte ich Sie bitten, diese Informationen beim Lesen der nächsten Kapitel im Hinterkopf zu behalten.

In den nachfolgenden Kapiteln werden die hier zusammengefassten Informationen noch einmal aufgegriffen und vor allem auch in Bezug auf Ihren praktischen Zusammenhang und mögliche resultierende Anwendungsfälle in der Praxis betrachtet. So viel möchte ich bereits vorwegnehmen: In der Praxis war es häufig so, dass nicht immer der Einsatz von neuer Technik zielführend war. Vielmehr half es in einigen Fällen schon, die Probleme mit den Zuständigen im Unternehmen zu besprechen und durch betriebliche Regelungen sowie deren anschließende technische Umsetzung festzulegen, was letztlich aber das Hinzuziehen eines Experten für die jeweiligen Thematiken bedurfte. Zur Umsetzung von Compliance und in der Folge auch von IT-Compliance und IT-Security empfiehlt sich die Rücksprache mit Experten zur Einführung von Referenzmodellen zur Umsetzung der Corporate Governance im Unternehmen. Dies wird in der Definition der IT-Compliance (Abschn. 2.4) noch einmal kurz angeschnitten, da diese Thematik den kompakten Inhalt dieses Buches übersteigen würde und die gewünschte Heranführung an die Thematik damit zu umfangreich werden würde.

1.2 Zielsetzung

Wie ich Ihnen bereits in der Einführung in das Thema erläutert habe, ist es mein Ziel, Ihnen die Potenziale von Digitalisierung aufzuzeigen. Da Digitalisierung in meiner Erfahrung jedoch fälschlicherweise immer häufiger als das Transferieren aller Daten in die Cloud verstanden wird, möchte ich Ihnen auch einige Möglichkeiten zeigen, wie Digitalisierung ohne die Nutzung der Cloud stattfinden kann.

Damit dies geschehen kann, wird, wie bereits angekündigt, eine Abgrenzung von lokaler Ebene und reiner ‚Cloud-Computing'-Ebene vorgenommen. Dabei wurde viel Wert daraufgelegt, dass auch Argumente der Gegner und Befürworter jeweils beider Seiten zusammentragen werden und diese objektiv darlegt werden. Mit großer Wahrscheinlichkeit werden auch Sie sich in dem ein oder anderen Argument wiederfinden. Ein kleiner Hinweis an dieser Stelle: Auch ich zählte mich einst zu den Gegnern von Cloud-Computing und fortschreitender Digitalisierung.

Die Bedenken werden auch deshalb angeführt, weil ein Entscheidungsträger seine Entscheidung für oder gegen etwas nicht fundiert begründen kann, wenn er nicht die Argumente beider Seiten kennt. Daher ist es mir ein großes Anliegen, Ihr Know-how in diesem Bereich bereichern zu können. Es sollte Ihnen dennoch selbst ein Anliegen sein, sich im Bereich Digitalisierung und generell IT weiterzubilden. Es ist nachvollziehbar, dass diese Aufgabe auf den ersten Blick groß zu sein scheint. Um Ihnen die Wahl der geeigneten Fortbildung oder auch Informationsveranstaltung etwas zu erleichtern, finden Sie aus diesem Grund in Kap. 5 einen Fragenkatalog, der Ihnen dabei helfen kann, Ihr eigenes Know-how einzuordnen.

Weiterbildung sollte auch im generellen Bereich der IT erfolgen, weil IT-Compliance- und IT-Security-Anforderungen auch dann bestehen, wenn Sie nicht planen sollten, eine umfassende Digitalisierungsmaßnahme zu ergreifen. Zumeist ist es aufgrund von finanziellen und personellen Aufwendungen oftmals schwer für ein KMU, entsprechende Anforderungen umzusetzen. Damit Sie dennoch die Wichtigkeit verstehen und einen groben Über-

blick darüber haben, wen Sie in einem solchen Fall mit der Umsetzung der Anforderungen beauftragen können, bedarf es eines gewissen Grundwissens.

Wie Sie der Einführung bereits entnehmen konnten, ist Cloud-Computing eine der treibenden Kräfte der Digitalisierung. Aus diesem Grund soll daran dargelegt werden, an welchen Stellen Cloud-Computing Sicherheitsvorteile und IT-Compliance-Vorteile, je nach Einsatzzweck, im Vergleich zur reinen lokalen IT-Ebene bieten könnte. Es soll jedoch auch aufgezeigt werden welche Nachteile entstehen könnten. Bedenken Sie aber bitte, dass es niemals eine 100-prozentige Sicherheit geben kann und Ihnen dies auch niemals jemand zusagen kann und wird.

Im Vergleich zur Nutzung einer lokalen Lösung bietet sich in der Cloud unter anderem der Vorteil, dass Sicherheitskriterien für alle Teilnehmer geschaffen werden. Der Anbieter hat also vereinfacht dargestellt nur einmalig den Aufwand, Sicherheitsmaßnahmen zu ergreifen, und kann diese dann auf alle Teilnehmer der Cloud anwenden. Zu diesen Sicherheitsmerkmalen zählen unter anderem Dienste, die je nach Anbieter sofort nutzbar sind, und solche, die gesondert hinzugebucht werden können. Dazu zählen generell unter anderem die Zwei-Faktor-Authentifizierung und der identitätsgestützte Zugriff auf Dateien. Letztlich obliegt die Umsetzung der Konfiguration und Sicherstellung der Funktion der Sicherheitsmerkmale jedoch den Kunden.

Dennoch möchte ich an dieser Stelle betonen, dass es aus meiner Sicht nicht absehbar ist, dass jegliche Anwendungsform in naher Zukunft in die Cloud transferiert wird. Es ist in erster Instanz auch nicht zielführend, und Digitalisierung bedeutet für ein Unternehmen auch nicht zwangsläufig, dass Sie alle Daten auf irgendein Cloudsystem verlagern sollen. Dazu aber im Verlaufe der Ausarbeitung mehr.

1.3 Vorgehensweise

Damit Sie einen besseren Überblick über die Thematik erhalten, ist dieses Buch thematisch aufeinander aufbauend gegliedert. Dennoch können Sie jederzeit zu den einzelnen Kapiteln oder