Patrick Müller
Vanessa Chamera
Martin Bodenstein

Datensicherung als Teil der IT- und Cybersecurity

Technische, menschliche und betrügerische Risiken erkennen und mit umfassenden Backup- und IT-Sicherheitsstrategien minimieren

Springer Gabler

Datensicherung als Teil der IT- und Cybersecurity

Patrick Müller • Vanessa Chamera •
Martin Bodenstein

Datensicherung als Teil der IT- und Cybersecurity

Technische, menschliche und betrügerische Risiken erkennen und mit umfassenden Backup- und IT-Sicherheitsstrategien minimieren

Springer Gabler

Patrick Müller
Stuttgart, Deutschland

Vanessa Chamera
Düsseldorf, Deutschland

Martin Bodenstein
Düsseldorf, Deutschland

ISBN 978-3-658-43700-8 ISBN 978-3-658-43701-5 (eBook)
https://doi.org/10.1007/978-3-658-43701-5

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

Planung/Lektorat: Vivien Bender
Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Herzlich willkommen zu diesem Buch über ein Thema, das in der heutigen digitalen Welt von entscheidender Bedeutung ist: die Datensicherung.

Zuallererst ist es wichtig zu betonen, dass wir uns in diesem Buch auf die Sicherung geschäftlicher Daten konzentrieren. Das bedeutet, dass wir uns darauf fokussieren, wie Daten regelmäßig gesichert werden können, um sie vor Verlust oder Beschädigung zu schützen. Dies ist nicht zu verwechseln mit der forensischen Datensicherung, bei der es darum geht, Daten in einem bestimmten Zustand zu erfassen, oft für rechtliche oder investigative Zwecke. Datensicherung darf ebenso nicht mit Datensicherheit verwechselt werden, welche sich mit dem Schutz von Daten vor unerlaubtem Zugriff oder Angriffen befasst.

Obwohl wir uns auf die Sicherung geschäftlicher Daten konzentrieren, können die hier vorgestellten Konzepte und Methoden durchaus auf private Geräte und Heimnetzwerke übertragen werden, um auch dort eine effektive Sicherung der Daten zu gewährleisten.

- **Datensicherung (Backup)** bezieht sich darauf, Kopien von Daten zu erstellen, die zur Wiederherstellung im Falle eines Datenverlustes verwendet werden können. Dies kann durch Hardwareausfälle, menschliche Fehler oder Katastrophen wie Brände oder Überschwemmungen verursacht werden. Das Hauptziel der Datensicherung ist es, die Integrität und Verfügbarkeit von Daten zu gewährleisten und sie bei Bedarf wiederherzustellen.

- **Datensicherheit** dagegen konzentriert sich darauf, Daten vor unerlaubtem Zugriff, Missbrauch, Diebstahl oder Angriffen zu schützen. Es geht darum, sicherzustellen, dass nur berechtigte Personen auf die Daten zugreifen und diese verwenden können. Datensicherheit umfasst Themen wie Verschlüsselung, Authentifizierung und Zugriffskontrollen.

Die moderne Gesellschaft ist von einer beispiellosen Datenflut umgeben. Wir verlassen uns auf unsere Computer, Smartphones, Tablets und Cloud-Services, um unser tägliches Leben zu organisieren, mit anderen zu kommunizieren, wichtige Dokumente aufzubewahren und Erinnerungen festzuhalten. Im Privaten wie im Geschäftlichen. Doch all diese digitalen Informationen sind nicht unverwundbar. Datenverlust kann auf vielfältige Weise auftreten, sei es durch Hardwarefehler, versehentliches oder auch bewusstes Löschen durch die Anwender:innen, Malware-Angriffe oder sogar Naturkatastrophen.

Die Konsequenzen eines Datenverlusts können dabei verheerend sein. Von persönlichen Erinnerungen und wertvollen Dokumenten bis hin zu geschäftskritischen Informationen und sensiblen Daten – der Verlust kann immense finanzielle, emotionale und praktische Auswirkungen haben. Umso wichtiger ist es, präventiv Maßnahmen zu ergreifen, um die Daten zu sichern und vor Verlust oder ungewollter Manipulation zu schützen.

Während vor wenigen Jahren die Datensicherungen hauptsächlich vorbeugend gegen mögliche Hardwaredefekte durchgeführt wurden, hat sich mittlerweile die Notwendigkeit, Daten zu sichern, durch andere Gefahrenquellen gesteigert. Organisatorische Gegebenheiten durch mehrere Anwender:innen sowie technologische Unwissenheit führen oft zu ungewollten Datenveränderungen oder -verlusten.

Die größte Gefahr der aktuellen Zeit birgt jedoch die Internetkriminalität (Cybercrime) – durch Manipulation oder Zerstörung von Systemen oder Dateien. Insbesondere die Vernetzung von verschiedenen Systemen wie Servern, Computern und Smartphones in Kombination mit zahlreichen verschiedenen Programmen und Apps bieten viele Schwachstellen, an denen Schadsoftware ins System eindringen kann. Beim sorglosen Umgang mit dem Smartphone wird dieses Eindringen zusätzlich begünstigt. Durch die niedrige Hemmschwelle, beliebige Apps von unbekannten Anbietern herunterzuladen und zu installieren, oder das Öffnen und Weiterleiten von Spaßbildern, -videos und -dateien von Smartphone zu Smartphone steigt die Gefahr durch Internetkriminalität stark.

Erschwerend kommt hinzu, dass auf den wenigsten Smartphones ein professionelles kommerzielles Virenschutz- oder Sicherheitsprogramm installiert ist. Selbst private Computer oder solche von kleinen Gesellschaften werden oftmals nur mit kostenlosen Virenschutz- oder Sicherheitsprogrammen ausgestattet. Selbst wenn ein professionelles kommerzielles Virenschutz- oder Sicherheitsprogramm installiert ist, deckt dieses lediglich die bislang bekannten Erscheinungsformen von Schadsoftware ab, sodass es keinen ausreichenden Schutz gegen neue Varianten oder Angriffe bietet.

Entsteht nun durch die Auswirkungen unerkannter Schadsoftware oder andere Ursachen ein Schaden, kann dieser dank eines ausgeklügelten Sicherungskonzepts minimiert werden. Vorab sei jedoch gesagt: Achten Sie immer auf verdächtige E-Mails oder Textnachrichten und folgen Sie keinen Links, die Ihnen eigenartig erscheinen. Verwenden Sie professionelle Schutzsoftware, halten Sie Ihre Betriebssysteme immer durch die Installation der verfügbaren Updates auf dem aktuellen Stand und seien Sie beim Browsen im Internet vorsichtig mit Ihrem Vertrauen auf das, was Ihnen angezeigt wird.

In diesem Buch möchten wir Ihnen die Grundlagen der Datensicherung vermitteln und Ihnen praktische Tipps und Strategien zur Verfügung stellen, um Ihre Daten effektiv zu schützen. Wir werden die verschiedenen Arten von Bedrohungen für Ihre Daten untersuchen und die besten Praktiken zur Vorbeugung von Datenverlust diskutieren. Wir werden Ihnen auch erklären, wie Sie eine robuste Datensicherungsstrategie entwickeln und implementieren können, die Ihre Daten vor den unterschiedlichsten Gefahren schützt. Zusätzlich bieten wir Ihnen auch einen Einblick in die relevanten Themen der Informations- und IT-Sicherheit, denn eine Datensicherung stellt die letzte Bastion dar und ist nicht die primäre Schutzmaßnahme.

Wir haben dieses Buch für Leser:innen aller Erfahrungsstufen konzipiert. Ob Sie gerade erst in die Welt der Datensicherung eintauchen oder bereits über fortgeschrittene Kenntnisse verfügen – wir hoffen, dass Sie hier wertvolle Informationen und Einsichten finden werden.

Die Datensicherung ist kein einmaliges Ereignis, sondern ein fortlaufender Prozess. Technologien entwickeln sich weiter, neue Bedrohungen entstehen und unsere Datenmengen sowie Ablageorte wachsen stetig. Daher ist es wichtig, sich kontinuierlich über neue Entwicklungen und bewährte Verfahren zu informieren und die Veränderungen im Blick zu behalten. Dieses Buch soll Ihnen dabei als verlässlicher Leitfaden dienen und Sie auf dem Weg zu einer umfassenden Datensicherungsstrategie begleiten. Wir geben Ihnen in diesem Buch auch einen Überblick über die Bordmittel der gängigsten Betriebssysteme und Plattformen, zeigen Unterschiede auf und geben Ihnen einige Tipps und Tricks zur Hand.

Des Weiteren verweisen wir auf Klick-für-Klick-Anleitungen für Windows, Windows Server oder macOS sowie auf diverse Online-Quellen mit längeren Hyperlinks. Damit Sie diese längeren Internetadressen nicht abschreiben müssen, möchten wir Ihnen die Möglichkeit bieten, diese über eine Linksammlung anzuklicken. Diese Linksammlung können Sie sich als PDF unter https://backup.patrick-mueller.de herunterladen.

Wir hoffen, dass Sie von diesem Buch profitieren, lernen wie Sie ein starkes Datensicherungs- und IT-Sicherheitsfundament einrichten können und dass es Ihnen hilft, Ihre wertvollen Informationen und Daten zu schützen.

▶ **Tipp** Gerne möchten wir Sie mit einem Augenzwinkern ermutigen, die Informationen, die Sie hier finden, nicht nur zu lesen, sondern auch anzuwenden. Denn letztendlich liegt es in Ihrer Hand, die Kontrolle über Ihre Daten zu behalten und dafür zu sorgen, dass sie sicher und geschützt sind.

Vielen Dank, dass Sie sich für dieses Buch entschieden haben. Wir wünschen Ihnen nun eine spannende Reise in die Welt der Datensicherung!

Abschließend möchten wir uns herzlich beim Springer-Verlag für die hervorragende Zusammenarbeit bedanken. Ein besonderer Dank geht dabei an Vivien Bender, die nicht nur als Ansprechpartnerin, sondern auch als Lektorin maßgeblich zum Gelingen dieses Werkes beigetragen hat. Unser Dank geht auch an msk media und insbesondere an Na-

dine Müller für die grafische Unterstützung, sowie an Gabriele Bodenstein für die prüferische Durchsicht des Manuskripts im Entwurf. Zuletzt möchten wir uns bei Christian Gräser bedanken, der uns Autoren zu diesem spannenden Thema zusammengebracht hat, um Ihnen als Leser:innen[1] die ganzheitliche Betrachtung von Datensicherung und IT-Sicherheit aufzeigen zu können.

Stuttgart, Deutschland — Patrick Müller
Düsseldorf, Deutschland — Vanessa Chamera
Düsseldorf, Deutschland — Martin Bodenstein
Oktober 2024

[1] Hinweis zur geschlechtsspezifischen Formulierung:

Im Rahmen dieses Buches haben wir uns bemüht, wo immer möglich und sinnvoll, geschlechtsspezifische Formulierungen zu verwenden oder beide Formen zu berücksichtigen, um niemanden zu übersehen oder auszuschließen. Sollten uns dennoch Stellen entgangen sein, bei denen wir nicht alle Geschlechter berücksichtigt haben, so war dies nicht unsere Absicht und bitten dies zu entschuldigen. Wir möchten betonen, dass wir stets alle Personen, unabhängig von Geschlecht oder Identität, in unsere Überlegungen und Aussagen einbeziehen.

Da der Hauptfokus dieses Buches auf Unternehmen liegt, verwenden wir unter anderem Begriffe wie „Anbieter“ oder „Dienstleister“. Bei diesen Bezeichnungen für juristische Personen verzichten wir auf eine Mehrgeschlechtlichkeit in der Formulierung. Wir danken für Ihr Verständnis und hoffen, dass der Inhalt des Buches für alle Leser:innen wertvoll und informativ ist.

Inhaltsverzeichnis

1 Einführung: Warum Daten gesichert werden müssen 1
1.1 Relevanz von Daten für Unternehmen 1
1.2 Herkunft und Nutzung neuer Datenmengen 3
1.3 Motivation für Datensicherung 6
1.4 Aufbau dieses Buches 8

2 Datenvielfalt, Verlustkosten und Aufbewahrungspflichten 11
2.1 Datenkategorien 12
2.2 Kosten durch fehlende Daten 24
2.3 Rechtliche Verpflichtungen 25

3 Ursachen für Datenverluste 27
3.1 Technische und räumliche Gefahren 29
3.2 Operative Gefahren 30
3.3 Gefahren durch technologische Unwissenheit 33
3.4 Gefahr bei mobilen Geräten 34
3.5 Internetkriminalität/Cybercrime 35

4 IT-Sicherheit als Ergänzung zur Datensicherung 45
4.1 Organisatorische Risikoaspekte der IT-Sicherheit 49
4.1.1 IT-Sicherheitsrichtlinie 49
4.1.2 Business Continuity und IT-Notfallmanagement 57
4.1.3 User Lifecycle Management 60
4.2 Technische Risikoaspekte der IT-Sicherheit 65
4.2.1 Network Security 66
4.2.2 Endpoint Security 69
4.2.3 Update- und Patchmanagement 72
4.3 Datensicherheit auf Reisen 75
4.4 Kategorien der Schutzmaßnahmen 77
4.4.1 Präventiv 79
4.4.2 Detektierend 84
4.4.3 Reaktiv 92

4.5 Zusammenhang zwischen Informationssicherheit und digitaler Forensik . . . 95
4.5.1 Bedeutung der Datensicherung für die Forensik . . . 96
4.5.2 Lessons Learned aus der forensischen Praxis . . . 99

5 Datensicherungsstrategie erstellen . . . 103
5.1 Das 3-2-1-Prinzip . . . 106
5.2 Arten von Speichermedien/Speicherorten . . . 107
5.3 Datensicherungsvarianten . . . 108
5.4 Geplante Backups und kontinuierliche Datensicherung . . . 109
5.5 Schutzmaßnahmen für Datensicherungen . . . 110
5.6 Remote-Backups und Cloud-Strategien . . . 111
5.7 Exkurs: Optimierung für die Datensicherung . . . 112
5.8 Notfallwiederherstellungsplan/Disaster-Recovery-Plan . . . 113
5.9 Leitfaden zur Erstellung der Datensicherungsstrategie . . . 114

6 Datensicherungsstrategie umsetzen . . . 119
6.1 Technischer Aufbau der Sicherungsarchitektur . . . 120
6.2 Organisatorischer Aufbau des Sicherungskonzeptes . . . 128
6.3 Abdeckung der Risiken durch Anzahl der Backup-Medien . . . 130

7 Sicherungskonzept implementieren . . . 131
7.1 Konfiguration . . . 132
7.2 Kontrolle . . . 133
7.3 Rücksicherung . . . 135
7.4 Bordmittel ausgewählter Systeme und Plattformen . . . 136
7.4.1 Windows für Desktops und Laptops . . . 136
7.4.2 Windows Server . . . 138
7.4.3 macOS als Desktop, Laptop oder Server . . . 139
7.4.4 Weitere Systeme oder Plattformen . . . 140

8 Arbeitshilfen und Vorlagen . . . 143
8.1 Orientierungshilfe Erstellung Datensicherungsstrategie . . . 145
8.2 Orientierungshilfe Aufbau IT-Sicherheitsrichtlinie . . . 148
8.3 Orientierungshilfe Aufbau Business Continuity und IT-Notfallmanagement . . . 150
8.4 Orientierungshilfe Aufbau User Lifecycle Management . . . 152
8.5 Orientierungshilfe Aufbau Network Security . . . 154
8.6 Orientierungshilfe Aufbau Endpoint Security . . . 156
8.7 Orientierungshilfe Aufbau Update- und Patchmanagement . . . 158
8.8 Orientierungshilfe Aufbau Sicherheitsrichtlinie für Auslandsreisen . . . 160
8.9 Orientierungshilfe Einführung konkreter Schutzmaßnahmen . . . 162

Literatur- und Quellenverzeichnis . . . 165

Stichwortverzeichnis . . . 169

Über die Autoren

Vanessa Chamera sammelte nach Abschluss ihres Masters in Economic Policy Consulting (M.Sc.) an der Ruhr-Universität Bochum berufliche Erfahrung anhand verschiedener Projekte in der IT-Sicherheit. Dabei spezialisierte sie sich auf die Analyse von Informationssicherheitsmaßnahmen zur Risikoprävention und die Durchführung von Compliance- und IT-Audits. Grundlage hierbei waren unter anderem die Anforderungen der ISO/IEC 27001 sowie aktuelle EU-Richtlinien und -Verordnungen (NIS2, DORA).

Im Rahmen ihrer Arbeit in der Digitalen Forensik war sie außerdem Teil digital-forensischer Untersuchungen in Folge von Cyberangriffen und half bei der Gewinnung, Analyse und Interpretation digitaler Beweismittel. Nicht zuletzt war sie verantwortlich für die operative Umsetzung und Koordination von IT-Projekten sowie die Kommunikation mit Stakeholdern.

Akademischer Hintergrund/Zertifizierungen

- M.Sc., Economic Policy Consulting, Ruhr-Universität Bochum
- B.A., Wirtschaft/Politik Ostasiens, Ruhr-Universität Bochum
- Lead Implementer and Lead Auditor ISO/IEC 27001
- Google Cloud Digital Leader

Kontaktmöglichkeiten und Informationen zum CV
LinkedIn: www.linkedin.com/in/vanessa-chamera

Martin Bodenstein verfügt über mehr als fünfzehn Jahre Berufserfahrung im Bereich IT-Service-, Security- und Projekt-Management. Mit einer mehrjährigen, internationalen Arbeitserfahrung (NATO) ist der Kern seiner Expertise die kontinuierliche Weiterentwicklung und professionelle Härtung von Information Security Maßnahmen, denen forensische Expertise und Know-how zugrunde liegen.

Die beruflichen Tätigkeitsschwerpunkte liegen im Bereich der Informationssicherheit mit Fokus auf Managementsysteme (ISMS), ISO- oder individuellen- Standards und IT-Prozessoptimierung nach ITIL bzw. COBIT 5.

Ausgeprägte Projekterfahrungen bestehen im Bereich der Implementierung, Zertifizierung sowie Auditierung von ISMS gemäß ISO/IEC 27001/22301, MaRisk, BSI C5, PCI DSS, TISAX® und KRITIS.

Ebenso dominiert die Verantwortung für die proaktive Bereitstellung von IT-Sicherheitsservices auf Basis IT-forensischer Methoden.

Akademischer Hintergrund/Zertifizierungen

- Diplom-Informatik (univ.) an der Universität der Bundeswehr München
- Master in Business Administration (MBA) an der Kempten University of Applied Science
- Certified Information Systems Security Professional (CISSP)
- Information Technology Infrastructure Library (ITIL) v3 Expert
- ISO/IEC 27001 (ISMS) und ISO/IEC 22301 (BCMS) Lead-/Zertifizierungsauditor
- Prüfverfahrens-Kompetenz für §8a (3) BSIG

Kontaktmöglichkeiten und Informationen zum CV
LinkedIn: https://www.linkedin.com/in/martin-bodenstein
Xing: https://www.xing.com/profile/martin_bodenstein

Patrick Müller hat sich im Laufe seiner Karriere intensiv mit forensischer Datenanalyse beschäftigt. Sein Studium an der renommierten Universität Mannheim legte den Grundstein für seine vertiefte Beschäftigung mit Datenbanksystemen, forensischer Informatik und Geschäftsprozessmanagement. Aufgrund seiner Funktionen in diversen Beratungs- und Industrieunternehmen konnte er maßgeblich zur Implementierung und Optimierung von Analyseverfahren beitragen.

In seiner Funktion als Dozent an der Frankfurt School of Finance & Management legt er den Schwerpunkt auf die Vermittlung von Kenntnissen in den Bereichen Forensische Datenanalyse, Audit Data Science und Visual Analytics.

Als Coach und Berater basiert seine Arbeitsethik auf Prinzipien der Genauigkeit und Integrität, die er aus der Forensik übernommen und in die Business Data Analytics integriert hat. Er verfolgt stets das Ziel, Unternehmen nicht nur vor Betrug und Schaden zu schützen, sondern ihnen auch transformative Geschäftseinblicke zu bieten. Sein Leitbild „No Data, No Party“ betont die essenzielle Rolle von Daten in der heutigen Geschäftswelt und sein unermüdliches Bestreben, diese effektiv und verantwortungsbewusst zu nutzen sowie zu schützen.

Akademischer Hintergrund

- Diplom-Wirtschaftsinformatik an der Universität Mannheim
- Dozent für Forensische Datenanalyse, Audit Data Science und Visual Analytics an der Frankfurt School of Finance and Management

Kontaktmöglichkeiten und Informationen zum CV
LinkedIn: https://www.linkedin.com/in/patrick-mueller-de
Homepage: https://www.patrick-mueller.de

Abbildungsverzeichnis

Abb. 1.1 Aufbau dieses Buches 10

Abb. 3.1 Kategorisierung der Gefahren zum Datenverlust. 28

Abb. 4.1 Organisatorische und technische Risikoaspekte der IT-Sicherheit 46
Abb. 4.2 Möglicher Leitfaden zum Aufbau einer IT-Sicherheitsrichtlinie. 51
Abb. 4.3 Prozesskreislauf im Business Continuity und IT-Notfallmanagement 59
Abb. 4.4 Drei Phasen im User Lifecycle Management 61
Abb. 4.5 Vergabe von Zugriffsrechten 63
Abb. 4.6 Kategorien der Schutzmaßnahmen 80
Abb. 4.7 Zusammenspiel detektierender Schutzmaßnahmen. 85
Abb. 4.8 Digital Forensic Information Security 98

Abb. 6.1 Zentrale Dateiablage mit weiteren Datenquellen. 121
Abb. 6.2 Sicherungsarchitektur mit zwei zentralen Dateiablagen und Back-up-Software 123
Abb. 6.3 Sicherungsarchitektur mit zwei weiteren Computern 124
Abb. 6.4 Sicherungsarchitektur mit mobilen Endgeräten und Geräten der IT-Infrastruktur 126
Abb. 6.5 Sicherungsarchitektur mit zwei Backup-Servern und jeweils drei Backup-Medien 127

Einführung: Warum Daten gesichert werden müssen

1

„Die Verantwortung für die Datensicherung ist ein unübertragbares Kernanliegen, das weder durch Outsourcing noch durch Cloud-Lösungen ersetzt werden kann."

(von den Autoren, basierend auf Erfahrungen aus gescheiterten Datensicherungen)

Zusammenfassung

Daten sind für Unternehmen von unschätzbarem Wert. Sie ermöglichen informierte Entscheidungen, personalisierte Kundeninteraktionen, effiziente Geschäftsprozesse und einen Wettbewerbsvorteil. Die Generierung neuer Daten wird durch Technologietrends wie das Internet of Things (IoT), künstliche Intelligenz (KI) und Blockchain vorangetrieben. In Büros sind Digitalisierungstrends zu beobachten, die aus vorherigen Technologiewellen stammen. Eine zuverlässige Datensicherung ist entscheidend, um Imageverluste, Kundenabwanderung und finanzielle Schäden zu vermeiden und den Wert der Daten zu erhalten.

1.1 Relevanz von Daten für Unternehmen

In der heutigen digitalen Ära sind Informationen in Form von Daten zu einer wertvollen Ressource geworden, die das Potenzial hat, den Erfolg eines Unternehmens maßgeblich zu beeinflussen. Sie kennen vermutlich den inzwischen älteren Spruch „Daten sind das Öl von Morgen".

P. Müller et al., *Datensicherung als Teil der IT- und Cybersecurity*,
https://doi.org/10.1007/978-3-658-43701-5_1

Unternehmen aller Größenordnungen sammeln und generieren kontinuierlich eine immense Menge an Daten, sei es über Kundeninteraktionen, Verkaufstransaktionen, Marketingkampagnen oder interne Prozesse. Doch warum sind diese Daten für Unternehmen so wichtig? Welche Rolle spielen sie bei der Entscheidungsfindung und wie können sie einen Wettbewerbsvorteil verschaffen?

Datenbasierte Entscheidungsfindung
Daten sind die Grundlage für eine fundierte und informierte Entscheidungsfindung in Unternehmen. Indem sie quantitative und qualitative Informationen liefern, ermöglichen sie es Führungskräften und Mitarbeitenden, ihre Strategien, Maßnahmen und Ziele auf objektiven Erkenntnissen aufzubauen. Daten ermöglichen es Unternehmen, Trends zu identifizieren, Muster zu erkennen und Vorhersagen zu treffen. Sie liefern Einblicke in Kundenverhalten, Markttrends und betriebliche Abläufe, die es Unternehmen ermöglichen, ihre Aktivitäten kontinuierlich zu optimieren und ihre Wettbewerbsfähigkeit zu steigern.

Kundenverständnis und personalisierte Erfahrungen
Daten spielen eine entscheidende Rolle bei der Gewinnung eines tiefen Verständnisses der Kundinnen und Kunden. Sie ermöglichen Unternehmen, das Kundenverhalten zu analysieren, Vorlieben zu identifizieren und personalisierte Erfahrungen anzubieten. Durch die Sammlung und Analyse von Kundendaten können Unternehmen ihre Produkte und Dienstleistungen an die Bedürfnisse und Wünsche ihrer Kundinnen und Kunden anpassen. Dies führt zu einer höheren Kundenzufriedenheit, stärkeren Kundenbeziehungen und letztendlich zu einer höheren Kundenbindung.

Effiziente Geschäftsprozesse und Kostenoptimierung
Daten spielen auch eine wichtige Rolle bei der Optimierung der Geschäftsprozesse eines Unternehmens. Durch die Analyse von Daten können Unternehmen Engpässe, ineffiziente Prozesse oder Bereiche mit hohem Kostenaufwand identifizieren. Dies ermöglicht es ihnen, gezielte Verbesserungen vorzunehmen, um die Effizienz zu steigern und Kosten zu senken. Darüber hinaus ermöglichen Daten Unternehmen, ihre Lagerbestände zu optimieren, die Lieferkette zu verwalten und Betriebsrisiken zu minimieren.

Wettbewerbsvorteil und Innovation
Daten können Unternehmen einen entscheidenden Wettbewerbsvorteil verschaffen, indem sie ihnen Einblicke in den Markt und das Verhalten ihrer Kundinnen und Kunden geben. Unternehmen, die in der Lage sind, Daten effektiv zu sammeln, zu analysieren und daraus handlungsrelevante Erkenntnisse zu gewinnen, können schneller auf Veränderungen im Markt reagieren, neue Trends erkennen und innovative Produkte und Dienstleistungen entwickeln. Durch die Nutzung von Daten als strategisches Kapital können Unternehmen ihre Positionierung am Markt stärken und sich von ihren Mitbewerbern abheben.

Fazit
Die Bedeutung von Daten für Unternehmen kann nicht unterschätzt werden. Daten sind der Treibstoff, der Unternehmen antreibt, indem sie informierte Entscheidungen, personalisierte Kundeninteraktionen, effiziente Geschäftsprozesse und einen Wettbewerbsvorteil ermöglichen. Unternehmen, die die Kraft der Daten verstehen und eine datengetriebene Kultur etablieren, sind gut positioniert, um in einer sich ständig wandelnden Geschäftswelt erfolgreich zu sein.

1.2 Herkunft und Nutzung neuer Datenmengen

In der digitalen Welt entstehen kontinuierlich neue Trends und Technologien, die die Art und Weise, wie Daten erzeugt und genutzt werden, grundlegend verändern. Dies führt nicht nur zu einer erheblichen Zunahme der erzeugten Datenmenge, sondern auch zu einem signifikanten Anstieg des Wertes dieser Daten. Daher möchten wir im Folgenden auf einige ausgewählte neue Technologien und Arbeitsmethoden eingehen.

Betrachtung ausgewählter neuer Technologien
Moderne Technologien verändern grundlegend die Art und Weise, wie Daten entstehen und genutzt werden. Sie ermöglichen eine effizientere Datensammlung und -verarbeitung, was Unternehmen neue Chancen eröffnet, aber auch neue Herausforderungen mit sich bringt. Im Folgenden werden die wichtigsten dieser aktuell neuen Technologien vorgestellt.

Internet of Things (IoT) ist eine Technologie, bei der physische Objekte mit Sensoren, Aktoren und Netzwerkverbindungen ausgestattet sind, um Daten zu sammeln und auszutauschen. Geräte wie Smart-Home-Geräte, „Wearables“, Industriemaschinen und vernetzte Fahrzeuge erzeugen kontinuierlich Daten über ihren Zustand, ihre Umgebung und ihre Interaktionen. Das IoT trägt erheblich zur stetigen Generierung neuer Daten bei.

Künstliche Intelligenz (KI) sowie maschinelles Lernen und neuronale Netzwerke, sind in der Lage, große Datenmengen zu analysieren und neue Erkenntnisse zu gewinnen. Durch den Einsatz von KI können Daten in Echtzeit verarbeitet und interpretiert werden, was zu einer kontinuierlichen Generierung von Informationen und Erkenntnissen führt.

Blockchain-Technologie wird hauptsächlich mit Kryptowährungen[1] in Verbindung gebracht, hat aber auch Auswirkungen auf die Generierung neuer Daten. Blockchain ermöglicht die sichere und transparente Speicherung und Übertragung von Daten. Durch dezentrale

[1] Eine Kryptowährung ist ein digitales Zahlungsmittel, das Kryptografie nutzt und auf der Blockchain-Technologie basiert. Sie ermöglichen dezentrale Transaktionen und sind oft schwankend im Wert. Das bekannteste Beispiel ist Bitcoin.

Netzwerke und „Smart Contracts[2]“ können neue Daten generiert werden, beispielsweise im Bereich der digitalen Identitäten, Lieferkettenverfolgung und Authentifizierung.

Augmented Reality[3] (AR) und Virtual Reality[4] (VR) eröffnen als Technologie neue Möglichkeiten für die Erzeugung und Erfassung von Daten. Durch die Integration virtueller Objekte in die reale Welt (AR) oder das Eintauchen in virtuelle Welten (VR) können Benutzer:innen Daten generieren, sei es durch Interaktionen, Aufzeichnungen oder Erfassung von Umgebungsdaten.

5G-Netzwerke bringen durch ihre Einführung höhere Geschwindigkeiten für das mobile Internet, geringere Latenzzeiten und eine größere Kapazität mit sich. Dadurch können mehr Geräte und Sensoren miteinander verbunden werden, was zu einer erhöhten Datenproduktion führt. Die schnelle Übertragung großer Datenmengen ermöglicht es Unternehmen, in Echtzeit auf Daten zuzugreifen und sie zu analysieren.

Cloud Computing[5] ermöglicht Unternehmen und Nutzer:innen den Zugriff auf theoretisch unbegrenzten Speicherplatz und Rechenleistung. Dies fördert die Generierung neuer Daten, da Unternehmen mehr Informationen speichern und verarbeiten können, ohne die Begrenzungen ihrer lokalen Infrastrukturen.

Sensoren und Wearables und deren zunehmende Verbreitung trägt zur Generierung neuer Daten bei. Diese Geräte, wie Fitness-Tracker, Smartwatches und medizinische Sensoren, erfassen kontinuierlich Informationen wie Herzfrequenz, Bewegungsmuster, Temperatur und Umgebungsbedingungen.

---

[2] Smart Contracts sind selbstausführende Verträge, dessen Vertragsbedingungen in Codeform geschrieben sind. Sie laufen auf einer Blockchain-Plattform und werden automatisch ausgeführt, wenn festgelegte Bedingungen erfüllt sind. Dadurch wird eine vertrauenswürdige, transparente und unveränderliche Vertragsabwicklung ermöglicht, ohne dass Dritte oder Vermittler benötigt werden.

[3] Augmented Reality (AR) ist eine Technologie, die digitale Informationen oder Grafiken in Echtzeit mit der physischen Welt überlagert. Nutzer:innen erleben AR typischerweise durch Smartphone-Apps oder spezielle Brillen und können so eine erweiterte Version ihrer tatsächlichen Umgebung wahrnehmen.

[4] Virtual Reality (VR) ist eine computergenerierte Simulation einer dreidimensionalen Umgebung, mit der Nutzer:innen über spezielle Ausrüstung wie VR-Headsets interagieren können. Sie ermöglicht das Eintauchen in eine virtuelle Welt und bietet oft ein 360-Grad-Bildfeld, wodurch sich die Nutzer:innen so fühlen, als wären sie tatsächlich in dieser Umgebung. Anwendungen reichen von Spielen über Bildung bis hin zu Trainingsszenarien.

[5] Cloud Computing ist ein Modell, bei dem IT-Ressourcen (wie Rechenleistung, Speicher oder Software) über das Internet bereitgestellt und skaliert werden, oft auf Basis von Bedarf und Verbrauch. Nutzer:innen können so auf Daten und Anwendungen von überall aus zugreifen, ohne diese lokal installieren oder verwalten zu müssen. Es ermöglicht Flexibilität, Kosteneffizienz und Skalierbarkeit für Unternehmen und Einzelpersonen.