

# IT-Management

## Das umfassende Handbuch

» Hier geht's  
direkt  
zum Buch

# DIE LESEPROBE

# Kapitel 1

## IT-Management

*Was bedeutet es überhaupt, eine IT-Umgebung zu verwalten und zu »managen«?*

Kein Unternehmen kann heutzutage auf die Nutzung von modernen *Informations-technologien* (kurz IT) verzichten. Die Nutzung der richtigen IT-Werkzeuge wirkt sich unmittelbar auf den Unternehmenserfolg aus und hilft, konkurrenzfähig zu sein und zu bleiben. Unabhängig von der Unternehmensgröße sind Entscheidung rund um die Einführung und Nutzung von IT-Lösungen erforderlich. Einzig der Umfang und die damit einhergehende Komplexität der Lösungen sind je nach Unternehmensgröße und Branche unterschiedlich.

Schon als Kleinunternehmen benötigen Sie ein Mindestmaß an IT-Lösungen, um mit Kunden in Kontakt zu treten, Rechnungen auszustellen und Ihre Buchhaltung im Blick zu haben. Es erscheint nicht viel, aber schon diese wenigen Bausteine wollen gut gewählt sein. Je größer Ihr Unternehmen ist, desto mehr müssen Sie Aufgaben rund um die Beschaffung und den Betrieb der IT delegieren. Die Anforderungen an IT-Verwaltungs- und Kontrollaufgaben nehmen zu und erfordern somit ein durchdachtes und planvolles IT-Management.

In der IT gibt es kein *One Size fits all*. Dies gilt für die Wahl der IT-Komponenten ebenso wie für alle Planungs- und Umsetzungsarbeiten. Aus diesem Grund ist es unmöglich, Ihnen in einem Handbuch die eine Empfehlung zu geben, wie Sie in Ihrem Unternehmen mit dem Thema IT-Management umgehen sollen.

Die eigentliche Frage, die es zu beantworten gilt: Was ist IT-Management?

Mit dieser Frage beschäftigen sich zahlreiche Publikationen am Markt, die sich dem Thema oftmals sehr theoretisch nähern und wenig Praxisbezug mitbringen. Dieses Handbuch zeigt Ihnen die Sichtweise auf das Thema aus den Blickwinkeln der Autorinnen und Autoren.

---

### Deutsch, Englisch, Denglisch

In diesem Buch werden Ihnen neue und bereits bekannte Begriffe begegnen. Wir haben beim Verfassen der Texte darauf Wert gelegt, dass die Inhalte verständlich und die Texte lesbar bleiben.

Eine durchgehende Übersetzung englischer Fachbegriffe ins Deutsche ist nicht immer praktikabel. Dies gilt insbesondere für etablierte Begriffe, wie z. B. *Modern Workplace* oder *Digital Workplace*. Aus diesem Grund finden Sie eine Mischung englischer und deutscher Fachbegriffe und manchmal auch eine denglische Bezeichnung, wie den Enterprise-Architekten.

Wichtig war es uns, eine entsprechende Konsistenz in den Kapiteln zu gewährleisten.

Die eigentliche Kunst beim IT-Management ist, die richtigen Entscheidungen zum richtigen Zeitpunkt zu treffen.

In diesem einleitenden Kapitel möchten wir Ihnen das Thema IT-Management anhand von Begriffen und Beispielen aus dem realen IT-Leben näherbringen. Oftmals wird immer nur von der *IT* gesprochen. Daher widmen wir uns zuerst der Frage, was ist die *IT* überhaupt?

## 1.1 Was ist IT?

*Informationstechnik (kurz IT) ist ein Oberbegriff für die elektronische Datenverarbeitung und die hierzu verwendete Hard- und Software-Infrastruktur.*

(<https://de.wikipedia.org/wiki/Informationstechnik>)

Um sich dem Thema IT-Management zu nähern, müssen wir zuerst ein gemeinsames Verständnis haben, was wir unter IT verstehen und welche Bausteine dazu zählen. Wie die einleitende Beschreibung zum Begriff *Informationstechnik* auf Wikipedia richtig feststellt, handelt es sich um einen Oberbegriff für die elektronische Datenverarbeitung mit den benötigten Hard- und Softwarekomponenten.

Neben der rein technischen Definition verstehen wir unter der Bezeichnung IT auch die damit einhergehenden Dienstleistungen zur Bereitstellung und zum Betrieb dieser Komponenten. Je nach Unternehmensgröße und -art ergeben sich hieraus unterschiedliche Organisationsstrukturen. Eine allgemeingültige Abgrenzung der Zuständigkeiten einer IT-Abteilung, die für alle Unternehmen einheitlich gilt, ist nicht möglich.

In diesem Buch geht es weniger um die technische Definition der Informationstechnik oder Informationstechnologie, sondern vielmehr um die Herausforderungen und Aufgaben, die sich eine IT-Abteilung zu stellen hat.

### 1.1.1 Definition der »IT«

Wenn man sich über die *IT* eines Unternehmens unterhält, wird diese je nach Unternehmensgröße und Gesprächspartner ganz unterschiedlich wahrgenommen.

- 
- ▶ Kleinere und mittelständische Unternehmen (KMU) verfügen oftmals über keine oder nur eine sehr kleine IT-Abteilung.

Wenn keine eigene IT-Abteilung vorhanden ist, erfolgt die Betreuung der IT-Systemlandschaft im Idealfall vollständig durch einen externen Dienstleister. Oftmals ist aber zumindest ein kleines IT-Team vorhanden, das sich im Regelfall um die täglich anfallenden Aufgaben kümmert und die unterschiedlichen externen Dienstleister koordiniert, um neue Lösungen zu implementieren oder schwer lösbarer technische Probleme zu bewältigen. In beiden Fällen wird selten über Weiterentwicklung, Innovationen oder den Austausch von Komponenten im Rahmen eines geplanten Lebenszyklus (*Lifecycle*) nachgedacht. Solange der tägliche Betrieb störungsfrei läuft, sind alle zufrieden.

- ▶ In größeren Unternehmen, insbesondere mit mehreren Standorten, ist meist eine entsprechend große IT-Abteilung vorhanden, die sich in mehrere IT-Fachteams aufgliedert, die aus den Fachleuten, den *Subject Matter Experts*, bestehen. Diese Fachteams stellen nicht nur den täglichen Betrieb sicher, sondern machen sich auch Gedanken über die technologische Weiterentwicklung der von ihnen betreuten Komponenten innerhalb der *IT-Plattformen* oder *IT-Infrastrukturen*.

Meine Frage an Sie:

*Wie wird die »IT« in Ihrem Unternehmen definiert?*

Aus der Antwort auf diese Frage ergibt sich, welchen Beitrag Sie und Ihr Team zum Erfolg des Unternehmens beitragen können.

### 1.1.2 Beitrag der IT zum Unternehmen

*Informationstechnologie* (IT) ist ein wesentlicher Faktor im Unternehmensmanagement – das ist unstrittig. Die Frage ist eher: Welche Aufgaben kommen konkret auf Sie zu, und wie können Sie priorisieren, was zu tun ist?

Auch die Antwort auf diese Frage kann ich Ihnen nicht abnehmen, denn sie hängt von der Ausrichtung und der Strategie Ihres Unternehmens ab. (Dazu kommen wir in Kapitel 2.) Als Anregung helfen Ihnen vielleicht folgende Punkte:

- ▶ **Kommunikation**

Ohne eine funktionierende Kommunikation kommt Ihr Unternehmen zum Stillstand. Mitarbeitende müssen schnell, unkompliziert und vor allem sicher Informationen austauschen können. Nur so kann gewährleistet werden, dass alle Beteiligten die richtigen Informationen zur richtigen Zeit zur Verfügung haben, um Entscheidungen rasch und fundiert fällen zu können.

► **Datensicherheit**

Der Austausch von Daten wirft unmittelbar Fragen zur Sicherheit auf. Im IT-Management obliegt es Ihnen, die Sicherheit der Umgebung zu gewährleisten, indem Sie beispielsweise regelmäßige Updates für Soft- und Hardware durchführen oder Maßnahmen gegen ungewollten Datenabfluss implementieren. Eine sichere IT-Umgebung ist ein zentraler Bestandteil eines erfolgreichen Unternehmens.

► **Fundierte Geschäftsentscheidungen**

Nicht der Informationsaustausch allein sorgt für bessere Entscheidungen, sondern auch die Datenanalyse. Moderne Werkzeuge erleichtern den Mitarbeitenden, Trends und Muster in Geschäftsdaten zu finden und so Einblicke in das Verhalten Ihrer Kunden und den Markt zu erlangen. Helfen Sie den Geschäftsbereichen, diese Erkenntnisse optimal zu nutzen, um Strategien zu entwickeln und Geschäftsprozesse zu optimieren. Die IT stellt die Werkzeuge und die Dateninfrastruktur bereit, um datenbasierte Entscheidungen zu treffen.

► **Routineaufgaben automatisieren**

Handarbeit ist out: Unternehmen achten inzwischen sehr darauf, dass möglichst viele Routineaufgaben automatisiert werden. Und wer ist dann dafür verantwortlich, dass die Systeme funktionieren? Richtig, Sie!

Wenn die IT stillsteht, funktioniert plötzlich nichts mehr. Sie müssen daher dafür Sorge tragen, dass die Mitarbeitenden nicht nur moderne Hilfsmittel nutzen können, sondern dass auch alles zuverlässig funktioniert. IT-Mitarbeitende sind zu wertvoll, um Standardaufgaben manuell durchführen zu lassen.

► **IT-Sicherheit und Compliance** (Diese Punkte stellen wir Ihnen in Kapitel 7 vor.)

Kurz gesagt: Ihre Aufgabe ist es, Daten vor Bedrohungen zu schützen und dafür zu sorgen, dass alle gesetzlichen Anforderungen und internen Unternehmensvorgaben erfüllt werden. IT-Sicherheitsmaßnahmen gilt es nicht nur einzuführen, sondern auch regelmäßig zu evaluieren und zu überarbeiten. Wenn Sie Ihre IT-Sicherheit und Compliance im Griff haben, fördert das das Vertrauen Ihrer Kunden und Geschäftspartner in das Unternehmen und bewahrt es vor rechtlichen Problemen.

Was davon trifft auf Ihr Unternehmen und Ihren Aufgabenbereich zu? Welche zusätzlichen Aufgaben fallen außerdem noch in Ihren Bereich, wofür tragen Sie Verantwortung?

Wenn Sie sagen können, was IT für Ihr Unternehmen bedeutet, können Sie im nächsten Schritt schauen, welche technischen Grundlagen es dafür geben muss. Auch dabei können wir nicht ins Detail gehen – das wäre auch absurd, denn es geht ja darum, was konkret und individuell Ihre IT unterstützt –, aber grob sollten Sie mit folgenden Komponenten vertraut sein.

### 1.1.3 Komponenten der IT

Um Ihre Geschäftsprozesse zu unterstützen, ist eine robuste IT-Infrastruktur unerlässlich. Auch diese sieht in jedem Unternehmen anders aus, und wir werden in Kapitel 15 noch genauer auf den Betrieb eingehen. Grob besteht »die Technik« aber aus den nachfolgend erläuterten Bestandteilen.

#### Server- und Netzwerk-Infrastruktur

Sie brauchen leistungsstarke Server, um Ihre Daten zu speichern und zu verarbeiten. Um maximale Verfügbarkeit und hohe Leistungsfähigkeit sicherzustellen, sollten diese Server regelmäßig gewartet und auf den neuesten Stand (Hardware und Software) gebracht werden. Ebenso benötigt man zuverlässige Netzwerklösungen, die eine schnelle und stabile Verbindung zwischen den verschiedenen IT-Komponenten ermöglichen.

Ein gut konfiguriertes Netzwerk sorgt dafür, dass Ihre Mitarbeitenden effizient arbeiten können und jederzeit auf notwendige Ressourcen zugreifen können. Investieren Sie daher in qualitativ hochwertige Hardware, um Ausfallzeiten zu minimieren und die Produktivität zu steigern.

Moderne Kommunikationswerkzeuge sind entscheidend für die Unterstützung der Unternehmenskommunikation. E-Mail-Server und -Clients bieten eine schnelle und sichere Möglichkeit zum Nachrichtenaustausch. Ergänzend sollten Kollaborationsplattformen wie Microsoft Teams oder Slack genutzt werden, um die Echtzeit-Zusammenarbeit zu fördern. Diese Tools bieten Funktionen wie Chat, Videokonferenzen und Dateifreigabe, die die Teamarbeit erheblich erleichtern.

#### Software für Geschäftsabläufe

Ein weiterer wesentlicher Bestandteil der IT sind leistungsstarke Softwarelösungen zur Unterstützung Ihrer Geschäftsabläufe. *Enterprise-Resource-Planning-(ERP-)Systeme* ermöglichen die Integration und Steuerung verschiedener Geschäftsfelder wie Finanzen, Personalwesen und Produktion.

*Customer-Relationship-Management-(CRM-)Systeme* helfen Ihnen beim Aufbau und der Pflege von Kundenbeziehungen. Diese Softwarelösungen bieten Einblicke in Ihre Unternehmensprozesse und unterstützen fundierte Entscheidungsfindungen.

#### IT-Sicherheit und Compliance

Um IT-Sicherheit zu gewährleisten, sind umfassende Sicherheitsmaßnahmen erforderlich. Firewalls und Antivirensoftware bewahren Ihr Netzwerk und Ihre Geräte vor äußeren Bedrohungen. Wenn Sie sensible Informationen verwalten, müssen Sie Verschlüsselungstechnologien einsetzen. Regelmäßige Updates und Patches sind notwendig, um Sicherheitslücken zu schließen und das System stets aktuell zu halten.

Weiterhin sollten Sie Ihre Mitarbeitenden in IT-Sicherheitsfragen schulen, um ihr Bewusstsein für mögliche Gefahren zu erhöhen. Grundsätzlich sollten Sie eine durchdachte Sicherheitsstrategie entwickeln, die Ihr Unternehmen vor Cyberangriffen und Datenverlust schützt.

Eng mit der IT-Sicherheit verbunden ist die *Compliance*. Darunter fallen alle Vorgaben und Regeln, die Ihr Unternehmen einhalten muss. Für Sie als IT-Verantwortlicher spielt dies eine große Rolle, denn fast alle Vorgaben betreffen in irgendeiner Form Ihre Arbeit: Denken Sie nur an die Datenschutzregeln der DSGVO oder die Bestimmungen des KRITIS-Gesetzes.

### **Backup und Restore**

Der Betrieb einer IT-Infrastruktur ist ohne Backup- und Wiederherstellungslösungen undenkbar. Die regelmäßige Sicherung Ihrer Daten sorgt dafür, dass diese im Fall eines Verlusts oder einer Datenkorruption rasch wiederhergestellt werden können. Cloudbasierte Backup-Systeme bieten dabei zusätzliche Sicherheit und Flexibilität. Achten Sie darauf, dass Sie Ihre Backup-Strategie regelmäßig überprüfen und testen. Eine verlässliche Backup-Lösung reduziert das Risiko von Datenverlust und Ausfallzeiten erheblich. Investieren Sie daher in technisch robuste und redundante Backup-Lösungen, um die Kontinuität des Geschäftsbetriebs Ihres Unternehmens zu sichern.

### **Virtualisierung**

Der Einsatz von Virtualisierungstechnologien steigert die Effizienz Ihrer IT-Infrastruktur. Indem Sie Server- und Desktop-Systeme virtualisieren, können Sie die kostenintensiv beschafften Hardware-Ressourcen optimal ausnutzen und die IT-Infrastruktur flexibler gestalten. Virtualisierung bietet die Möglichkeit, mehrere virtuelle Maschinen auf einem einzelnen physischen Server zu betreiben, was die Verwaltung erleichtert und Kosten reduziert. Ergänzend dazu erweitern Cloud-Dienste wie *Infrastructure as a Service* (IaaS) und *Software as a Service* (SaaS) diese Flexibilität und Skalierbarkeit. Setzen Sie auf Virtualisierung und Cloud-Dienste, um Ihre IT-Infrastruktur zukunftssicher zu gestalten. Der Einsatz von cloudbasierten virtuellen Desktop-Systemen ermöglicht es Ihren Mitarbeitenden, von überall sicher zu arbeiten.

### **Hardware für die Belegschaft**

Als IT-Verantwortlicher gestalten Sie die Grundlage für reibungsloses Arbeiten – und das beginnt bei der richtigen Ausstattung. Ihre mobilen Kolleginnen brauchen mehr als nur irgendeinen Laptop: Sie brauchen leistungsstarke Geräte mit genügend Rechenpower und Speicher, um auch anspruchsvolle Anwendungen mühelos zu bewältigen. Ebenso entscheidend ist eine schnelle, stabile Internetverbindung – denn ohne sie wird der Zugriff auf Unternehmensressourcen oder die Teilnahme an Videokonferenzen schnell zur Geduldsprobe. Achten Sie bei der Auswahl mobiler Geräte auf

zwei Dinge: Sie sollten leicht genug sein, um unterwegs nicht zur Last zu fallen, und gleichzeitig robust genug, um den Alltag zu überstehen. Investieren Sie in hochwertige Hardware – das zahlt sich aus. Denn gut ausgestattete Mitarbeitende arbeiten effizienter, flexibler und motivierter.

### Sicherheit unterwegs

Auch hier spielt die Sicherheit der IT-Systeme eine große Rolle. Während Sie im Büro noch recht gut einschränken können, was mit den Daten passiert, ist dies beim mobilen Arbeiten deutlich schwieriger. Mobile Geräte sind besonders anfällig für Diebstahl, Zerstörung und Verlust, weshalb es entscheidend ist, Sicherheitsmaßnahmen wie Verschlüsselung und die Möglichkeit zur Fernlöschung zu implementieren. Diese Maßnahmen sorgen dafür, dass Ihre Daten selbst bei Verlust oder Diebstahl geschützt bleiben. Darüber hinaus sollten Sie sichere VPN-Verbindungen nutzen, um den Zugang zum Unternehmensnetzwerk abzusichern. Es ist ebenfalls wichtig, Mitarbeiter im sicheren Umgang mit mobilen Geräten zu schulen (Sperrbildschirm, Token, Sichtschutz etc.).

Welche spezifische Kombination der IT-Komponenten Sie in Ihrem Unternehmen wiederfinden, hängt von der Größe, Branche und den besonderen Bedürfnissen Ihres Unternehmens ab.

Oftmals ist es eine reine Interpretationsfrage, wo der Aufgabenbereich des IT-Teams anfängt und bis wohin die Fachbereiche zuständig sind. Der Klassiker ist die Frage nach dem VBA-Makro, das plötzlich nicht mehr tut, was es soll: Der Buchhalter beschwert sich bei der IT, dass die Berechnungen in seiner Excel-Tabelle nicht stimmen. Ist das nun ein Problem mit einer »IT-Komponente« und damit ein Problem für Sie? Wohl eher nicht, wobei die Grenzen in unterschiedlichen Unternehmen und Organisationen sehr fließend sind.

In Produktionsbetrieben ist dieses Problem aber noch wesentlich größer und führt häufig zu einer Aufteilung der IT-Verantwortlichkeiten, was sowohl technische als auch organisatorische Herausforderungen mit sich bringt. Der folgende Abschnitt basiert auf Erfahrungen aus der chemischen Industrie.

#### 1.1.4 IT in Produktionsbereichen – Schatten-IT und Kompetenzgerangel

In Unternehmen des produzierenden Gewerbes kommt es immer wieder zu Kompetenzgerangeln um die Frage, was IT überhaupt ist. Gehören die IT-Komponenten in den Produktionsbereichen dazu?

In der Produktion wird dem »allgemeinen« IT-Team die Kompetenz für eine sichere und stabile Implementierung von Komponenten abgesprochen. Das kann beispielsweise Labor- und Messsysteme betreffen oder die Steuergeräte von Maschinen, ob-

wohl diese Dinge auch »nur« Computer sind. Diese Infrastrukturen basieren im Regelfall auf industriefähigen IT-Komponenten, die in bestehenden Industrieanlagen schleichend von betreuenden Prozesstechnik-Abteilungen eingeführt wurden. Solche Implementierungen hatten stets die Funktionalität im Fokus und wurden nicht mit einem strategischen IT-Blick angeschafft.

### Sicherheitsrisiko durch Schatten-IT

Die schleichende Einführung von IT-Komponenten in den Produktionsbereichen stellt häufig die größte *Schatten-IT* (mehr dazu in Abschnitt 6.1) im Unternehmen dar. Und damit ist sie automatisch ein kritisches Betriebsrisiko.

Zu Beginn meiner beruflichen Karriere als Mess- und Regelmechaniker erfolgten Messung und Steuerung von Industrieanlagen weitgehend auf Basis analoger Messverfahren und klassischer elektrischer Schaltungen. Die Einführung der *Prozessleittechnik (PLT)* führte zu einer Erleichterung im täglichen Betrieb der Komponenten und zu einem Wechsel von schalterbasierter Messwarten-Technik hin zu bildschirmbasierter Steuerung.

Diese Nähe zum Produktionsbetrieb führt in vielen Unternehmen dazu, dass die Produktions-IT durch die PLT-Abteilung und nicht durch die IT-Abteilung des Unternehmens betreut und betrieben wird. Beide Abteilungen verfügen hinsichtlich ihrer Aufgabengebiete über das notwendige Fachwissen, aber Probleme entstehen durch historisch gewachsene Kommunikationsgrenzen zwischen den Abteilungen. In der Praxis führt so etwas zu unsicheren IT-Implementierungen in der Produktion und wird noch verschlimmert, wenn persönliche Streitereien und unklare Aufgabenverteilungen hinzukommen.

### Wer ist zuständig?

In einem Unternehmen der chemischen Industrie kam es wegen eines Streits über die Zuständigkeit für die *Labor-Management-Systeme (LMS)* des ganzen Konzerns zu einer persönlichen Fehde zwischen CIO und CTO. Dies hatte zur Folge, dass über einen längeren Zeitraum hinweg keine Entscheidung über die Einführung eines neuen LMS getroffen wurde.

Zwischenzeitlich wurde nicht nur das vorhandene LMS nicht mehr vom Hersteller unterstützt, sondern auch die Hardware selbst, die für das LMS genutzt wurde, erreichte ihr Lebensende. Die gesamte LMS-Umgebung war somit nicht mehr unter Support und entsprach daher auch nicht mehr den selbst definierten Compliance-Anforderungen. Von den Auswirkungen auf die ISO-27001-Zertifizierung ganz zu schweigen.

Unklare Zuständigkeiten bzw. Kämpfe um Zuständigkeiten haben also eine direkte Auswirkung auf Ihre IT-Umgebung und damit auf die IT-Sicherheit. Im Organigramm

sehen Sie das daran, dass die Zuständigkeiten für die IT zwischen dem *Chief Information Officer* (CIO) und dem *Chief Technology Officer* (CTO) aufgeteilt und dadurch unklar sind. Diese Unklarheit kann zu Konflikten und ineffizienten Entscheidungsprozessen führen.

Der CIO fokussiert sich auf IT-Strategie und Verwaltung der IT-Infrastruktur, während der CTO technologische Innovationen und die Entwicklung neuer Produkte und Dienstleistungen im Blick hat (im nächsten Abschnitt werden die Rollen genauer vorgestellt). Ohne eine klare Abgrenzung der Verantwortlichkeiten kann es zu Überschneidungen und Missverständnissen kommen, was die Umsetzung von IT-Projekten verzögert und die Effizienz des Unternehmens beeinträchtigt. Daher ist eine eindeutige Definition der Rollen und Verantwortlichkeiten unerlässlich.

Ein weiteres Problem, das durch unklare Verantwortlichkeiten entstehen kann, ist die fehlende Abstimmung zwischen den Abteilungen. Wenn der CIO und der CTO unterschiedliche Prioritäten und Ziele verfolgen, entstehen widersprüchliche Anweisungen und Strategien. Dies schafft bei den Mitarbeitern Verwirrung und erschwert die Zusammenarbeit, gerade auch bei auftretenden Störungen oder Unterbrechungen. Eine mangelnde Koordination führt zudem dazu, dass wichtige Projekte nicht termingerecht abgeschlossen werden oder Ressourcen ineffizient eingesetzt werden. Deshalb ist eine enge Kooperation und kontinuierliche Kommunikation zwischen dem CIO und CTO unerlässlich, um solche Herausforderungen zu meistern. Regelmäßige Meetings und klare Kommunikationskanäle können dabei unterstützen, die Zusammenarbeit zu optimieren.

Und schließlich beeinträchtigen unklare Zuständigkeiten die IT-Sicherheit und Compliance. Wenn die Verantwortlichkeiten nicht eindeutig festgelegt sind, entstehen möglicherweise Sicherheitslücken. Der CIO könnte sich stärker auf die Erfüllung der Compliance-Vorschriften konzentrieren, während der CTO den Fokus auf technische Sicherheitsmaßnahmen legt. Fehlen jedoch klare Zuständigkeitsbereiche, könnten wesentliche Sicherheitsmaßnahmen übersehen werden. Dies birgt das Risiko von Cyberangriffen und Datenverlusten. Achten Sie daher auf eine klar definierte Verteilung der Verantwortung in Bezug auf IT-Sicherheit und Compliance.

## 1.2 Die Teams und Rollen in der IT

Es ist komplett unrealistisch, dass eine komplexe IT-Infrastruktur von einer unstrukturierten Mitarbeiterschar oder gar nur von einer einzigen Person verwaltet wird. Stattdessen sind Teamplayer gefragt, die gezielt ihre Aufgaben erledigen und damit ihre Rollen ausfüllen.

Wie diese Teams aufgebaut sind und welche Rollen besetzt werden, hängt vollkommen vom Aufbau des Unternehmens ab. Zudem wird es so sein, dass die Trennung

gerade in kleineren Unternehmen nicht messerscharf ist und Sie als IT-Manager auch mal ein Projekt leiten und vielleicht sogar im 1st-Level-Support aushelfen müssen, falls Not am Mann ist. Dennoch sollen Ihnen die nächsten Abschnitte eine Idee geben, wie sich Ihr Aufgabenbereich personell strukturieren lässt.

### 1.2.1 Die Rollen in der IT

Es ist sehr unwahrscheinlich, dass Sie alle folgenden Rollen in Ihrem Unternehmen genauso wiederfinden. Trotzdem sollten Sie diese Begriffe kennen und zumindest grob wissen, wie sich ihre Aufgabenbereiche unterscheiden und wer wofür verantwortlich ist.

- ▶ **CEO (Chief Executive Officer)/Geschäftsführung:** Die Person in der Geschäftsführung leitet das Unternehmen. Sie legt die strategische Ausrichtung fest und trifft die wichtigsten Entscheidungen.
- ▶ **CIO (Chief Information Officer)/IT-Leitung:** Die IT-Leitung ist verantwortlich für die gesamte IT-Strategie des Unternehmens.
- ▶ **CTO (Chief Technology Officer)/technische Leitung:** Die technische Leitung konzentriert sich auf die technologische Entwicklung und Innovation innerhalb des Unternehmens.
- ▶ **CISO (Chief Information Security Officer)/Sicherheitsleitung:** Der CISO ist für die Sicherheit des Unternehmens verantwortlich, sowohl physisch als auch digital. Innerhalb der IT ist er für die Informationssicherheit zuständig.
- ▶ **IT-Direktor:** Der IT-Direktor leitet die IT-Abteilung und ist verantwortlich für die Umsetzung der IT-Strategie. Er koordiniert die verschiedenen IT-Bereiche.
- ▶ **IT-Manager:** Das IT-Management ist für die tägliche Verwaltung der IT-Abteilung verantwortlich und überwacht die IT-Projekte, das Personal und die Budgets. Es stellt sicher, dass die IT-Systeme den Anforderungen des Unternehmens entsprechen. Das ist die Ebene, auf die wir uns in diesem Buch (zumeist) beziehen.
- ▶ **IT-Projektmanager/IT-Projektleitung:** Die IT-Projektleitung leitet spezifische IT-Projekte und sorgt für deren erfolgreiche Durchführung. Dazu gehören die Planung, Umsetzung und Überwachung der Projektziele, Zeitpläne und Budgets.
- ▶ **IT Operations Manager/IT-Betriebsleitung:** Die IT-Betriebsleitung ist für den Betrieb der IT-Systeme und -Infrastruktur verantwortlich. Sie sorgt dafür, dass die Systeme reibungslos funktionieren und dass Probleme schnell behoben werden.
- ▶ **IT Service Manager/IT-Dienstleitung:** Die IT-Dienstleitung überwacht die Bereitstellung von IT-Diensten und -Support für die Nutzer im Unternehmen. Sie stellt sicher, dass alle IT-Dienste den Erwartungen entsprechen und kontinuierlich verbessert werden. Sie ist die Ansprechpartnerin für alle IT-Bedürfnisse und sorgt für optimalen Service.

- ▶ **IT Systems Administrator/Systemadministration:** Die Systemadministration verwaltet die IT-Infrastruktur, einschließlich Servern, Netzwerken und Datenbanken. Sie sorgt für die Sicherstellung der Verfügbarkeit und Leistung der IT-Systeme.
- ▶ **Network Administrator/Netzwerkadministration:** Die Netzwerkadministration ist für die Verwaltung und Wartung der Netzwerkinfrastruktur verantwortlich.
- ▶ **Cyber Security Analyst/IT-Sicherheitsanalyse:** Die IT-Sicherheitsanalyse ist für die Analyse und Überwachung der Sicherheitssysteme verantwortlich. Sie identifiziert Sicherheitsrisiken und entwickelt Strategien zur Bedrohungsabwehr.
- ▶ **Database Administrator (DBA)/Datenbankadministration:** Die Datenbankadministration verwaltet die Datenbankumgebungen innerhalb des Unternehmens.
- ▶ **Software Developer/Softwareentwicklung:** Die Softwareentwicklung entwickelt und implementiert Softwarelösungen, die den Geschäftsanforderungen des Unternehmens entsprechen.
- ▶ **Business-Analyst:** Business-Analysten arbeiten zwischen den IT- und Geschäftsteams, um sicherzustellen, dass die IT-Lösungen den Geschäftsanforderungen entsprechen und die Unternehmensziele unterstützen. Sie müssen gute Übersetzer sein und zwischen zwei Welten vermitteln
- ▶ **Helpdesk Technician/IT-Support:** Der IT-Support bietet technischen Support für Endbenutzer und hilft bei der Lösung von IT-Problemen. Er ist der Helfer in der Not, der schnelle Lösungen für IT-Fragen bietet.

### Rollen mit KI-Bezug

In Unternehmen, in denen die KI einen zentralen Bestandteil der Wertschöpfungskette ausmacht, gibt es oft zusätzliche Führungsrollen, wie z. B.:

- ▶ **CAIO (Chief AI Officer)/KI-Leitung:** Die KI-Leitung ist verantwortlich für die strategische Planung, Entwicklung und Implementierung von KI-Initiativen im gesamten Unternehmen.
- ▶ **CDAO (Chief Data & AI Officer):** Diese Rolle ist verantwortlich für die Kombination der Daten- und KI-Strategie.

Dem Erfindungsgeist sind hinsichtlich der Rollenbezeichnungen keine Grenzen gesetzt.

### 1.2.2 IT-Teams

Ob in Ihrem Unternehmen nur ein einziges IT-Team existiert, das sich um alle IT-Themen kümmert, oder ob die unterschiedlichen IT-Themen auf verschiedene Fach-Teams verteilt sind: Es geht immer um die Sicherstellung des Tagesbetriebs, die Umsetzung von Projekten und die Unterstützung bei technischen Problemen.

### **Wer ist für die Produktion zuständig?**

Wenn Ihr Unternehmen im produzierenden Gewerbe tätig ist, stellt gerade das Thema IT-Sicherheit eine besondere Herausforderung dar. Die Betrachtung der Sicherheit in der Infrastruktur für die Bürokommunikation unterscheidet sich von der für den Produktionsbetrieb.

Es gibt in jedem Unternehmen unterschiedliche Sichtweisen zur Zuständigkeit und unterschiedliche Zuordnungen der Rollen. Grob lässt sich aber die nachfolgend dargestellte Aufteilung festhalten.

#### **Betrieb**

Der sichere Betrieb einer IT-Infrastruktur erfordert ein Team, das aus Personen ganz unterschiedlicher Fachbereiche zusammengesetzt ist. Je nach Größe Ihres Unternehmens besteht auch der Bedarf an mehreren IT-Teams. In diesem Fall richten sich die Teams nach den notwendigen Fachthemen, wie z. B. Rechenzentrum, Server, Netzwerk, Virtualisierung, Backup, Datenbanken, E-Mail usw. Sie sind somit verantwortlich für den sogenannten Backend- und Basisbetrieb der IT-Infrastruktur.

Die tägliche Arbeit im Basisbetrieb wird über eine IT-Servicemanagement-Lösung gesteuert, die im Idealfall auch Funktionen für (teil-)automatisierte Workflows für nicht alltägliche Aufgaben bietet. Prüfen Sie, ob sich täglich wiederholende Aufgaben automatisieren lassen. Diese Art der Automatisierung erfordert in den meisten Fällen eine von der ITSM-Lösung separat betriebene Lösung. Im Rahmen der ITSM-Lösung werden einerseits interne Betriebsthemen bearbeitet, aber es wird auch an Problemlösungen gearbeitet, die das IT-Supportteam aufgenommen hat.

Diese Teams nehmen im Gegensatz zu Projektteams eine permanente Rolle im Unternehmen ein. Die Mitglieder der Teams können sowohl interne wie externe Personen sein. Ebenso ist es möglich, dass die Betreuung einzelner Fachthemen vollständig durch externe Dienstleister erbracht wird.

#### **Projekte**

Projektteams werden immer dann gebildet, wenn besondere Probleme in einem definierten Zeitrahmen gelöst werden müssen, neue IT-Lösungen eingeführt oder bestehende Komponenten oder Applikationen migriert werden müssen (siehe dazu auch Kapitel 10, »IT-Projektmanagement«).

Je nach Projektaufgabe setzen sich diese Teams aus internen und externen Mitarbeitern zusammen. Externe Personen werden in das Projektteam eingebunden, wenn die benötigte Expertise im eigenen Unternehmen nicht vorhanden ist oder etwas ganz Neues angegangen wird. Hierbei kann sowohl technologisches Fachwissen im Projekt als auch das Projektmanagement an sich ergänzt werden. Sollten für ein Pro-

jezt keine internen Ressourcen zur Verfügung stehen, kann ein Projektteam auch vollständig durch externe Personen gebildet werden.

Projektteams folgen in ihrer Arbeit den etablierten Methodiken des Projektmanagements. Hierbei agieren sie eigenständig oder sind im Rahmen eines umfassenden Programms als Teilprojekt in ein übergeordnetes Programm-Management eingebunden.

## Support

Support-Teams sind Teil der Frontend-Dienste und die erste Anlaufstelle für Endanwender. Die erste Support-Ebene, der *1st-Level-Support*, nimmt Fehlermeldungen oder IT-Wünsche der Anwender entgegen. Technische Probleme können auf Basis einer Wissensdatenbank bekannter Probleme und Handlungsanweisungen schnell und kompetent beantwortet werden. Support-Teams bestehen in der Regel nicht aus Spezialisten, sondern vielmehr aus Generalisten, die sich schnell einen Überblick über die technische Problemlage des Anwenders verschaffen können. Jeder Vorgang wird in einer IT-Servicemanagement-Lösung in einem Vorgang erfasst und bearbeitet.

Sollte sich ein Problem nicht unmittelbar durch den 1st-Level-Support lösen lassen, so wird der Vorgang an eine weitere Support-Ebene weitergegeben. Diese weiteren Support-Ebenen gliedern sich in den *2nd-* und *3rd-Level-Support*. In diesen beiden Ebenen arbeiten IT-Spezialisten mit dem entsprechenden Fachwissen für das jeweilige Themengebiet. Nicht jedes Unternehmen verfügt über mehrere Support-Ebenen.

### Ticketbearbeitung – Theorie und Wirklichkeit

In der Theorie erfasst und bearbeitet eine ITSM-Lösung nicht nur IT-Vorgänge. Sie ist zudem eine Wissensdatenbank, um wiederkehrende Probleme nicht immer von Grund auf neu lösen zu müssen. Dies bringt aber zwei Probleme mit sich:

- ▶ Eine Wissensdatenbank muss zuerst einmal gefüllt und gepflegt werden. Hierzu ist es in einem ersten Schritt ausreichend, ausführliche Lösungsbeschreibungen zu erfassen und einen Vorgang aussagekräftig zu verschlagworten.
- ▶ Das zweite und wesentlich größere Problem ist die Nutzung der Wissensdatenbank. In vielen Unternehmen erfolgt durch den 1st-Level Support kein Lösungsversuch. Stattdessen werden gemeldete Probleme nur erfasst und basierend auf einem Schlagwort umgehend an den 2nd- oder 3rd-Level-Support weitergeleitet. Währenddessen ist der 1st-Level-Support in anderen Firmen deutlich aktiver und kümmert sich selbstständig um bekannte Incidents.

Die letzte Support-Ebene, manchmal gerne auch *Last-Level-Support* gezeichnet, wird meist von den Teams des IT-Betriebs erbracht, da es um Applikations- und unmittelbare Serverprobleme geht.

Ebenso wie die IT-Teams für den Betrieb der IT spielen auch die Support-Teams eine permanente Rolle im Unternehmen. Die Team-Mitglieder des IT-Supports können interne und externe Mitarbeiter sein.

Besonders der 1st-Level-Support wird oftmals an externe Dienstleister ausgelagert. Dies ist von besonderem Interesse, wenn ein Unternehmen global tätig ist und Support-Verfügbarkeit rund um die Uhr in allen Zeitzonen gewährleisten möchte.

### 1.2.3 Wissensaufbau und Weiterentwicklung: das Wissensmanagement

Der Wissensaufbau und die Weiterentwicklung eines IT-Teams sollten von Ihnen mit Nachdruck vorangetrieben werden, damit die Teammitglieder über die erforderlichen Fähigkeiten und Kenntnisse verfügen, um ihre Aufgaben zu erledigen.

- ▶ **Richten Sie ein zentrales Wissensmanagement ein, und sorgen Sie dafür, dass alle Prozesse und Systeme dokumentiert sind:** Es sollte keine »Wissenssilos« geben, und wenn sogar Passwörter oder andere wichtige Informationen nur im Kopf einer Person existieren, läuft etwas sehr schief! Wissen und Infos müssen geteilt werden und für alle zugänglich sein, die damit arbeiten.
- ▶ **Investieren Sie in fortlaufende Schulungen und Zertifizierungen:** Wenn der interne Austausch nicht reicht, muss Fachwissen von außen importiert werden. Halten Sie Ihr IT-Team auf dem neuesten Stand, indem Sie Weiterbildungen und Zertifizierungen ermöglichen (aber mit Maß: siehe Abschnitt 3.8).
- ▶ **Implementieren Sie Mentoring-Programme:** Setzen Sie erfahrene Teammitglieder als Mentoren ein, um neue Leute zu unterstützen. Dies hilft, Wissen zu teilen und die berufliche Entwicklung zu fördern.
- ▶ **Schaffen Sie eine Kultur des Lernens und der kontinuierlichen Verbesserung:** Fördern Sie eine Arbeitsumgebung, in der Lernen und Weiterentwicklung aktiv unterstützt werden, um die Effizienz und Produktivität Ihres Teams zu steigern.
- ▶ **Sorgen Sie für eine gesunde Fehlerkultur:** Fehler werden immer passieren, aber zumindest kann man aus ihnen lernen. Das geht aber nur, wenn sich alle trauen, Fehler offen anzusprechen, zu diskutieren und auszutauschen.

### 1.2.4 Fehlerkultur

Eine etablierte und unternehmensweit gelebte Fehlerkultur ist der Schlüssel zu einem sicheren und sich stetig verbessernden IT-Betrieb, denn Fehler sind menschlich und können nie vollständig ausgeschlossen werden. Eine gute Fehlerkultur erkennt dies an und sieht Fehler nicht als Versagen, sondern als Chance zum Lernen und auch zur Verbesserung.

Das trägt dazu bei, dass es weniger Furcht vor dem Scheitern gibt. In vielen Unternehmen vermeiden Mitarbeiter Risiken und bremsen Innovationen aus, weil sie Fehler fürchten. Eine Kultur, die Fehler als Chance zum Lernen betrachtet, kann helfen, diese Furcht zu überwinden und eine Atmosphäre zu schaffen, in der Mitarbeiter Risiken wagen und neue Ideen ausprobieren.

Ein weiterer Vorteil einer guten Fehlerkultur ist, dass sie die Kommunikation und Kooperation im Team stärken kann. Wenn Fehler ohne Furcht vor Konsequenzen offen angesprochen werden können, steigert dies die Ehrlichkeit und das Vertrauen im Team. Dies kann zu einer effektiveren Teamarbeit und schließlich zu besseren Leistungen führen.

Schließlich ist in der IT-Abteilung eine gute Fehlerkultur besonders wichtig. Aufgrund der Komplexität und des sich ständig ändernden Charakters der Technologie sind Fehler in der IT unvermeidlich. Eine Kultur, die Fehler als Gelegenheit zum Lernen und zur Verbesserung ansieht, trägt dazu bei, dass die IT-Abteilung effektiver und effizienter arbeitet und besser auf die sich ändernden Anforderungen und Herausforderungen reagieren kann.

Eine gute Fehlerkultur kann sich in verschiedenen Praktiken und Verhaltensweisen manifestieren. Hier sind einige Beispiele, auf die Sie achten sollten:

1. **Transparente Kommunikation:** Eine konstruktive Fehlerkultur zeichnet sich dadurch aus, dass offen über Fehler gesprochen wird. Mitarbeitende werden ermutigt, ihre Fehler zuzugeben, ohne Angst vor negativen Folgen haben zu müssen. Dies stärkt das Vertrauen und die Zusammenarbeit innerhalb Ihres Teams.
2. **Lernorientierung:** Fehler werden als Chancen zum Lernen betrachtet. Anstatt sie zu sanktionieren, analysiert man, was schiefgelaufen ist und wie solche Fehler künftig vermieden werden können. Dies unterstützt kontinuierliche Verbesserung und fördert Innovation in Ihrem Team.
3. **Fehlervermeidung:** Eine gute Fehlerkultur heißt auch, dass proaktive Maßnahmen ergreifen werden, um Fehler zu vermeiden. Dies kann durch regelmäßige Schulungen, klare Prozesse und Richtlinien sowie durch den Einsatz von Technologie zur Fehlererkennung und -vermeidung erreicht werden. Hier spielt die Automation ebenfalls eine wichtige Rolle.
4. **Fehleranalyse:** Wenn Fehler auftreten, werden sie gründlich analysiert (z. B. per RCA – Root Cause Analysis), um die wirkliche Ursache zu ermitteln. Dies hilft dabei, ähnliche Fehler bzw. Fehlerquellen in der Zukunft zu vermeiden, und verbessert die Qualität der Arbeit.
5. **Fehlerberichterstattung:** Ermutigen Sie Ihre IT-Teammitglieder, Fehler zu melden, wenn sie sie bemerken. Dies ermöglicht es Ihnen, schnell auf Probleme zu reagieren und sie zu beheben, bevor sie zu größeren Problemen werden.

### 1.3 IT-Lebenszyklus (Lifecycle)

Die Einführung von IT-Komponenten besteht nicht nur aus dem Erwerb und der Inbetriebnahme. Jeder Baustein, der für den Betrieb der IT-Landschaft in Ihrem Unternehmen benötigt wird, bedarf einer Planung von Anschaffung, Implementierung, Betrieb, Wartung und Migration (oder Ablösung) zu einer neueren Version. Darauf werden wir noch in Abschnitt 15.4 genauer eingehen.

Jeder dieser Bausteine hat andere Anforderungen an das Lifecycle-Intervall, auf die Sie in Ihrer IT-Plattformstrategie und Investitionsplanung Rücksicht nehmen müssen. Nur so können Sie sicherstellen, dass Sie auf veränderte Bedürfnisse der Fachabteilungen des Unternehmens und auf Technologieentwicklungen reagieren können. Sich auf ein »es wird schon gut gehen« zurückzuziehen, ist grob fahrlässig.

Der Lebenszyklus von Hard- und Softwarekomponenten und die damit einhergehende Aktualisierung oder der Wechsel zu einer neuen Version oder einem neuen Produkt hat direkte Auswirkungen auf die Cyber-Sicherheit des Unternehmens.

### 1.4 Was ist IT-Management?

In den vorherigen Abschnitten haben Sie die Komponenten der IT, die Teams und Rollen und den Beitrag, den die IT zum Unternehmenserfolg beiträgt, kennengelernt. Der Betrieb der IT-Infrastruktur erfolgt nicht zum Selbstzweck der IT-Abteilung selbst, sondern immer im Hinblick auf die Bedürfnisse und Anforderungen des Unternehmens. Dies erfordert eine durchdachte und planvolle Verwaltung, das *IT-Management*.

Die IT im Unternehmen gibt es nicht geschenkt. Die Hauptaufgabe des IT-Managements ist die Umsetzung der definierten IT-Strategie, in enger Zusammenarbeit mit den Fachabteilungen. Die IT ist Dienstleister im eigenen Unternehmen. Sie betreibt die notwendige IT-Infrastruktur, erbringt die benötigten Dienstleistungen und treibt die Weiterentwicklung durch die Implementierung von Innovationen an – und dies unter Berücksichtigung koordinierter Zeitpläne und abgestimmter Prioritäten.

Diese wenigen Sätze verdeutlichen auch schon die Herausforderungen, die Ihnen im IT-Management begegnen. Sie müssen den Bedürfnissen und Wünschen unterschiedlicher Personengruppen im Unternehmen gerecht werden. Dies gelingt nicht immer. Ein wichtiger Teil des IT-Managements ist daher das Erwartungshaltungsmanagement. Sie müssen die Erwartungen der beteiligten Personen und Abteilungen verstehen, um diese mit dem notwendigen Realismus der IT-Möglichkeiten in die richtige Richtung zu steuern.

### 1.4.1 Aufgabenbereiche im IT-Management

Die Anforderungen, die an die IT herangetragen werden, entstammen nicht nur aus den Fachabteilungen selbst, sondern basieren ebenfalls auf den Zielen des Unternehmens. Die Fachabteilungen werden bei der Erbringung von IT-Dienstleistungen als Kunde, also als Leistungsempfänger, eingestuft. Die Gesamtorganisation des Unternehmens ist die übergeordnete Einheit, aus der unternehmensweit gültige Anforderungen an die IT herangetragen werden.

- ▶ Die Aufgaben im IT-Management sind vielfältig und haben alle das Ziel, die IT-Infrastruktur eines Unternehmens sowohl effizient als auch sicher zu gestalten. Ein zentraler Bereich ist das *IT-Strategiemanagement*, das langfristige IT-Ziele plant und umsetzt. Dabei ist es wichtig, die IT-Strategie mit den Geschäftsstrategien des Unternehmens abzustimmen. Ebenso bedeutend ist das IT-Projektmanagement, das für die Planung, Durchführung und Überwachung von IT-Projekten verantwortlich ist. Diese Projekte können von der Einführung neuer Software bis hin zur Implementierung neuer IT-Systeme reichen. Für den Einstieg sollten Sie sich zunächst grundlegend mit dem Projektmanagement vertraut machen – lesen Sie dazu etwa die Einführung in Kapitel 10.
- ▶ Ein weiteres Aufgabengebiet umfasst das *IT-Servicemanagement*. Dabei geht es darum, IT-Dienstleistungen bereitzustellen und zu verwalten, die den Geschäftsanforderungen gerecht werden. Dies beinhaltet auch die Leitung von IT-Support-Teams (intern & extern), die technische Unterstützung bieten. Ein effektives IT-Servicemanagement stellt sicher, dass alle IT-Dienste störungsfrei funktionieren und die Mitarbeitenden produktiv arbeiten können. Neueinsteiger sollten sich mit etablierten IT-Servicemanagement-Frameworks und Best Practices wie ITIL vertraut machen (siehe Kapitel 12). Diese Frameworks liefern bewährte Verfahren für die Bereitstellung und Verwaltung von IT-Diensten.
- ▶ Das *IT-Infrastrukturmanagement* befasst sich mit der Verwaltung der physischen und virtuellen IT-Ressourcen eines Unternehmens, darunter Server, Netzwerke und Speicherlösungen. Das Ziel besteht darin, eine stabile und leistungsfähige IT-Infrastruktur bereitzustellen, die den Geschäftsanforderungen entspricht. Dies schließt auch die regelmäßige Wartung und Aktualisierung aller IT-Systeme ein.

Als Neuling in der IT-Management-Rolle sollten Sie sich mit den Grundlagen der IT-Infrastruktur vertraut machen und lernen, diese effektiv zu verwalten, um Ausfallzeiten zu minimieren und die Produktivität zu maximieren. Die *CMDB (Configuration Management Database)* erfasst alle relevanten Informationen über die IT-Infrastruktur Ihres Unternehmens und kann so ein zentraler Baustein Ihres IT-Infrastrukturmanagements sein.

- ▶ Das *IT-Risikomanagement* befasst sich mit der Identifizierung und Bewertung potenzieller Risiken, die die IT-Systeme eines Unternehmens bedrohen könnten. Zu

diesen Risiken gehören Cyberangriffe, Datenverluste und Systemausfälle. Das Hauptziel besteht darin, Strategien zu entwickeln, um diese Risiken zu minimieren und die IT-Sicherheit aufrechtzuerhalten. Für den Einstieg sollten Sie sich mit den grundlegenden Prinzipien des Risikomanagements vertraut machen und erlernen, wie Risiken identifiziert, dokumentiert und bewertet werden. Daran schließt dann das Erarbeiten von Strategien zur Risikobehandlung an.

- ▶ Das *IT-Compliance-Management* beinhaltet die Einhaltung von gesetzlichen und regulatorischen Vorgaben im IT-Bereich. Es umfasst die Einführung von Richtlinien und Prozessen, um sicherzustellen, dass alle IT-Aktivitäten gesetzeskonform sind. Ein IT-Compliance-Management schützt das Unternehmen vor rechtlichen Problemen und stärkt das Vertrauen von Kunden und Geschäftspartnern. Als Neulinge sollten Sie sich intensiv mit den relevanten gesetzlichen und regulatorischen Anforderungen auseinandersetzen und lernen, wie diese praktisch umgesetzt werden. Dies ist wesentlich, um die IT-Compliance sicherzustellen.
- ▶ Das *IT-Budgetmanagement* beinhaltet die Planung und Verwaltung finanzieller Mittel für IT-Projekte und -Dienste. Das primäre Ziel besteht darin, IT-Ausgaben zu optimieren und sicherzustellen, dass alle IT-Investitionen den größtmöglichen Nutzen für das Unternehmen bringen. Dies umfasst auch die Überwachung der IT-Ausgaben und die Erstellung von Budgetberichten. Für den Einstieg sollten Sie sich mit den grundlegenden Konzepten des Budgetmanagements vertraut machen und lernen, wie man IT-Budgets effizient plant und verwaltet. Häufig werden die Planung und Verwaltung von IT-Budgets als mühselig empfunden, aber ohne sie geht es einfach nicht (siehe Kapitel 4).
- ▶ Das *IT-Sicherheitsmanagement* hat große Bedeutung für den Schutz von Unternehmens-IT-Systemen vor Bedrohungen (siehe Kapitel 7). Es beinhaltet die Einführung und Verwaltung von Sicherheitsmaßnahmen wie Firewalls, Antivirensoftware und Verschlüsselungstechnologien. Ein effizientes IT-Sicherheitsmanagement sichert das Unternehmen gegen Cyberangriffe und Datenverlust ab. Neulinge sollten grundlegende Kenntnisse über IT-Sicherheit erlangen und lernen, Sicherheitsmaßnahmen effektiv umzusetzen und zu verwalten. Dies ist wesentlich, um die IT-Sicherheit und Geschäftskontinuität zu wahren.

Wenn Sie gerade erst ins IT-Management einsteigen, sollten Sie sich zunächst auf die grundlegenden Aspekte konzentrieren.

- ▶ Machen Sie sich mit wesentlichen IT-Management-Frameworks und -Methoden vertraut, beispielsweise *ITIL* (<https://www.atlassian.com/de/itsm/itil>) für das IT-Servicemanagement und *PRINCE2* (<https://de.wikipedia.org/wiki/PRINCE2>) für das Projektmanagement.
- ▶ Verstehen Sie die Grundkonzepte der IT-Infrastruktur sowie der IT-Sicherheit.

Zudem ist es wichtig, die gesetzlichen und regulatorischen Anforderungen im IT-Bereich zu kennen. Indem Sie diesen Grundlagen besondere Aufmerksamkeit schenken, legen Sie eine solide Basis, die es Ihnen ermöglicht, Ihre Fähigkeiten und Ihr Wissen zu erweitern.

### 1.4.2 Von Menschen und Maschinen

Ein umfassendes IT-Fachwissen bildet nur einen Teil der notwendigen Voraussetzungen ab, um ein IT-Management erfolgreich auszufüllen. Es hilft Ihnen beim Verständnis der technischen Anforderungen, bei der Analyse der Bedürfnisse des IT-Betriebs und bei den notwendigen Planungen. Gerade im Dialog mit externen IT-Dienstleistern ist es wichtig, dass Sie sich auf Ihr Wissen verlassen können, um die Aussagen der Dienstleister richtig einschätzen und bewerten zu können.

Neben dem IT-Fachwissen gibt es aber einen weiteren wichtigen Faktor, um erfolgreich und nachhaltig eine IT-Abteilung oder ein IT-Team zu führen, die *Soft Skills* oder *soziale Kompetenz*.

#### Soft Skills

Beginnen wir mit der *Kommunikationsfähigkeit*. Stellen Sie sich vor, Sie müssen Ihrem Team einen komplexen technischen Sachverhalt erklären. Was nützen Ihnen Ihre brillanten technischen Kenntnisse, wenn Sie diese nicht verständlich vermitteln können? Ihre Fähigkeit, technische Details in einfache Worte zu fassen, hilft nicht nur Ihrem Team, sondern auch Ihrer Zusammenarbeit mit anderen Abteilungen und der Führungsebene.

Denken Sie an die letzte Teambesprechung. War sie produktiv oder chaotisch? *Zusammenarbeit im Team* ist entscheidend, und als Führungskraft im IT-Management müssen Sie nicht nur zuhören, sondern auch Kompromisse eingehen und Lösungen gemeinsam entwickeln. Erinnern Sie sich an ein Projekt, bei dem das Team mehr erreicht hat, als jeder Einzelne hätte leisten können?

Im IT-Management jonglieren Sie oft mit mehreren Projekten gleichzeitig. Da kann es leicht passieren, dass man sich überfordert fühlt und man das Gefühl hat, dass man alles gleichzeitig erledigen muss? Hier kommt Ihre Fähigkeit ins Spiel, Prioritäten zu setzen, Aufgaben zu delegieren und Deadlines im Blick zu behalten. Mit einem guten *Zeitmanagement* behalten Sie den Überblick und erhöhen Ihre Produktivität – und das ohne Stress.

*Flexibilität* ist unerlässlich, besonders in der dynamischen IT-Branche. Wenn sich neue Technologien und Arbeitsmethoden ergeben, sollten Sie bereit sein, sich rasch anzupassen. Erinnern Sie sich daran, wie plötzlich während Corona alle von zu Hause arbeiten mussten? Man musste sich um die Kinderbetreuung kümmern, während

man mit überlasteten Zulieferern um eine Ladung Laptops verhandelte. Ihre Bereitschaft, kontinuierlich zu lernen und sich weiterzuentwickeln, ermöglicht es Ihnen, in einem sich ständig verändernden Umfeld erfolgreich zu agieren.

*Probleme* wird es immer und überall geben – ständig werden Sie damit konfrontiert werden, dass irgendwas nicht so funktioniert, wie es soll, dass ungeplante Herausforderungen auftauchen und dass ganz viele Leute mit ihren Fragen zu Ihnen kommen. Dann ist Ihre Fähigkeit gefragt, schnell und effizient Lösungen zu finden. Das bedeutet, analytisch zu denken und kreativ zu sein – zwei Eigenschaften, die Ihnen helfen, Herausforderungen aus verschiedenen Perspektiven zu betrachten und innovative Ansätze zu entwickeln. Gleichzeitig müssen Sie stets entscheiden, ob »pragmatische« Lösungen ausreichen oder man besser genau den Prozessen und Vorschriften folgt.

*Führungskompetenz* ist das Herzstück Ihrer Rolle als IT-Manager. Sie müssen Ihr Team anleiten, klare Ziele vorgeben und bei Konflikten vermitteln. Und noch mehr: Sie müssen Entscheidungen treffen und Verantwortung übernehmen.

Und zum Schluss ganz wichtig: Vergessen Sie nicht die *Empathie*! Sie sollten in der Lage sein, die Bedürfnisse und Standpunkte Ihrer Mitarbeitenden zu erkennen und nachzuvollziehen. Das fördert nicht nur ein positives Arbeitsklima, sondern stärkt auch das Vertrauen im Team. Denken Sie daran, wie wichtig es ist, auf die Anforderungen Ihrer Kunden und Geschäftspartner einzugehen. Ein empathischer Führungsstil kann die Zufriedenheit und Motivation Ihrer Mitarbeitenden erheblich steigern.

Wenn Sie im IT-Management erfolgreich sein wollen, brauchen Sie sowohl technisches Know-how als auch die richtigen Soft Skills. Trotz aller technischen Hilfsmittel arbeiten Sie mit Menschen, die unterschiedliche Hintergründe und Voraussetzungen mitbringen. Ihre Fähigkeit, in diesem dynamischen Umfeld effektiv zu agieren, ist der Schlüssel zu einem harmonischen und erfolgreichen Arbeitsalltag.

### IT-Manager oder IT-Leader?

Im IT-Management gibt es zwei Schlüsselrollen, die etwas abseits der formalisierten Rollen stehen, die wir in Abschnitt 1.2.1 beschrieben haben: der IT-Manager und der IT-Leader. Beide tragen maßgeblich zum Erfolg eines Unternehmens bei, unterscheiden sich jedoch in ihren Verantwortlichkeiten und Vorgehensweisen.

- ▶ Als *IT-Manager* konzentrieren Sie sich vor allem auf die Verwaltung und den Betrieb der IT-Infrastruktur. Sie stellen sicher, dass die Systeme reibungslos funktionieren, Probleme rasch gelöst werden und IT-Ressourcen effizient eingesetzt werden. Als IT-Manager sind Sie häufig in den täglichen Betrieb involviert und gewährleisten, dass alle technischen Anforderungen erfüllt sind.
- ▶ Als *IT-Leader* hingegen nehmen Sie eine strategischere Position ein. Sie entwerfen Visionen und langfristige Strategien sowohl für die IT-Abteilung als auch für das gesamte Unternehmen. Dabei inspirieren und motivieren Sie Ihr Team, innovative

Lösungen zu entwickeln und neue Technologien einzuführen. In enger Zusammenarbeit mit anderen Führungskräften sorgen Sie dafür, dass die IT-Strategie mit den Geschäftszielen im Einklang bleibt. Der Schwerpunkt liegt dabei auf der Förderung von Innovation und dem Aufbau einer zukunftsorientierten IT-Kultur. Die Sicherstellung der technischen Anforderungen und des täglichen Betriebs obliegt Ihrem kompetenten IT-Team.

Einführend sollten Sie wissen, dass beide Rollen unterschiedliche, aber sich ergänzende Ziele haben. Der IT-Manager gewährleistet den reibungslosen Ablauf der täglichen Aktivitäten, während der IT-Leader die Richtung vorgibt und die Zukunft formt. Ein erfolgreicher IT-Manager muss detailorientiert und lösungsfokussiert sein, wohingegen ein IT-Leader visionär und inspirierend sein sollte. Beide Positionen erfordern jedoch starke Kommunikationsfähigkeiten und die Fähigkeit zur effektiven Zusammenarbeit mit diversen Stakeholdern. Wenn Sie erst in Ihre Management-Rolle einsteigen, sollten Sie die Unterschiede und Gemeinsamkeiten dieser Rollen verstehen, um Ihre Karriere effektiv zu planen und zu gestalten.

### Generalisten und Spezialisten

In der IT unterscheiden wir zwischen IT-Generalisten und IT-Spezialisten.

- ▶ *IT-Generalisten* haben umfassendes Wissen in verschiedenen IT-Bereichen. Sie können vielfältige Aufgaben übernehmen und bieten vielseitige Unterstützung bei unterschiedlichen Projekten. Diese Flexibilität macht sie besonders wertvoll für kleinere Unternehmen oder Teams, die ein breites Spektrum an IT-Aufgaben abdecken müssen.
- ▶ *IT-Spezialisten* hingegen fokussieren sich auf ein spezifisches Segment innerhalb der Informationstechnologie. Sie verfügen über umfassende Kenntnisse und Fertigkeiten in ihrem Fachbereich, sei es Netzwerksicherheit, Datenbankverwaltung oder Softwareentwicklung. Diese Spezialisten sind häufig in größeren Unternehmen gefragt, wo ihre spezialisierten Fähigkeiten notwendig sind, um komplexe Aufgaben zu bewältigen. Dank ihrer Expertise können sie innovative Lösungen entwickeln und technische Herausforderungen effizient meistern.

Für die vielfältigen Aufgaben des IT-Managements braucht es eine Mischung aus Generalisten und Spezialisten. Generalisten dienen als Verbindungsglieder zwischen unterschiedlichen IT-Feldern und sorgen dafür, dass alle Projektaspekte beachtet werden. Sie haben den Überblick. Spezialisten liefern das Fachwissen, um spezifische technische Herausforderungen zu meistern und die Qualität der IT-Dienstleistungen sicherzustellen. Manche Leute arbeiten sich gerne und rasch in neue Themen ein und können fast überall etwas beisteuern, andere vertiefen sich lieber jahrelang in eine Fragestellung und verbeißen sich so lange in ein Problem, bis sie wirklich alles verstanden haben.

Als IT-Manager müssen Sie die Stärken und Schwächen Ihres Teams verstehen, damit Sie die Kompetenzen von Generalisten und Spezialisten effektiv nutzen können. Verteilen Sie Aufgaben und Projekte so, dass alle (möglichst) glücklich sind und ihre Stärken ausspielen können.

### Angst vor Veränderung

Früher war es üblich, dass man seine gesamte berufliche Laufbahn in dem einmal erlernten Beruf von der Ausbildung bis zur Rente verbrachte. Besonders in der IT-Branche ist dieser Ansatz jedoch seit über 30 Jahren bedeutungslos. Der rasante technologische Fortschritt führt dazu, dass sich die beruflichen Anforderungen im IT-Bereich ständig ändern. Gerade diese Geschwindigkeit des Wandels macht vielen Menschen in der IT Angst (<https://granikos.eu/wie-veraendert-sich-mein-it-arbeitsplatz-in-einer-cloudbasierten-welt>). Auch die Anwender in Ihrem Unternehmen sind von der Furcht vor technologischen Veränderungen betroffen.

Die tägliche Arbeit gibt Menschen Halt und Struktur. Veränderungen am Arbeitsplatz, sei es durch neue Aufgaben und Zuständigkeiten oder durch die neue Zusammenarbeit in einem anderen Team durch eine Umstrukturierung, führen oft zu einer inneren Abwehrhaltung oder gar völligen Blockade. Ob diese Haltung eintritt, hängt im Wesentlichen von der begleitenden Kommunikation ab.

Machen Sie sich die Ängste Ihrer IT-Mitarbeiter bewusst. Adressieren Sie sie offensiv in persönlichen Gesprächen im passenden Rahmen (siehe auch Kapitel 3).

### Das Setting für persönliche Gespräche

Wie der passende Rahmen für persönliche Gespräche aussieht, müssen Sie selbst entscheiden. Die Kommunikationskultur in Ihrem Unternehmen im Allgemeinen und die Gesprächskultur in der IT im Besonderen spielen eine Rolle, wie persönliche Gespräche wahrgenommen werden.

Persönliche Gespräche werden oft als heikel wahrgenommen. Gehen Sie mit dem Anspruch eines Mitarbeiters auf die Begleitung durch eine Vertrauensperson proaktiv um. Weisen Sie schon bei der Einladung auf diese Möglichkeit hin. Es geht um eine offene Kommunikation. Versuchen Sie, im Anschreiben schon mögliche Ängste abzubauen.

Hier einige Beispiel für einen passenden Rahmen bzw. ein optimales Setting:

- ▶ **Ungestörtheit:** Sorgen Sie aktiv dafür, dass Sie während des Gesprächs nicht gestört werden (Telefon umleiten, Handy aus, Tür zu mit Hinweisschild etc.).
- ▶ **Genügend Zeit einplanen:** Quetschen Sie den Termin nicht zwischen zwei andere Termine. Genügend und ausreichend Zeit einplanen.
- ▶ **Getränke:** Bieten Sie ruhig als Eisbrecher etwas zu trinken an (Wasser, Kaffee etc.).

### 1.4.3 IT-Organisation

Der Aufbau einer IT-Organisation folgt in den meisten Fällen den Anforderungen des Unternehmens. Es gibt hierbei (wie kann es anders sein) keine einfache Empfehlung, die auf alle Unternehmen passt. Die IT-Organisation ist eingegliedert in die Gesamthierarchie des Unternehmens und stellt somit nur den für uns relevanten Teil dar. In diesem Kapitel konzentrieren wir uns auf die IT-Organisation.

Die Aufteilung unterschiedlicher IT-Themenfelder hilft Ihnen bei der Zuweisung von Zuständigkeiten und Verantwortlichkeiten. In den vergangenen Jahren sind die starren Grenzen bei bestimmten IT-Themen immer mehr verschwommen, bewusst und unbewusst. Ein Beispiel für das bewusste Verschwinden ist die das Thema der *Demokratisierung der IT*, also die Übertragung von IT-Verantwortung an Endanwender. Diesem Thema widmen wir uns in Abschnitt 1.4.7 separat. Als Beispiel für ein unbewusstes Verschwinden von Grenzen nenne ich gerne Office-Applikationen.

Diese Applikationen fallen eindeutig in den Zuständigkeitsbereich des Frontend-Teams. Kommt es aber zu Support-Anfragen zu diesen Applikationen, allen voran Outlook, fällt die Zuständigkeit oftmals an das Team der Applikationen oder Backend-Dienste. Ohne eine klare Abgrenzung der Aufgaben und Zuständigkeiten entsteht sofort ein Spannungsfeld zwischen den Teams.

Ein einfacher Aufbau kann die Aufteilung in die folgenden drei Hauptbereiche beinhalten:

#### ► **Workspace-Services**

Dieser Bereich bündelt alle Zuständigkeiten und Aufgaben, die sich auf Anwender auswirken, wie z. B. die Ausgabe und Verwaltung von Endgeräten und die Installation und Wartung von Client-Applikationen auf Endgeräten per Softwareverteilung.

Ebenso ist hier der 1st-Level-Support angesiedelt, der als erster Ansprechpunkt für Anwendende agiert und sich um die Lösung einfacher und bekannter Probleme kümmert. Applikationsbezogene Fehler werden durch den Helpdesk erfasst und anschließend an den 2nd-Level-Support der Application-Services weitergeleitet.

Die Nachverfolgung von Geräten im Rahmen von Mitarbeiterwechseln im Unternehmen oder bei Austritt aus dem Unternehmen gehört auch zu den Aufgaben der Workplace-Services.

#### ► **Application-Services**

In diesen Bereich fallen die Planung und der Betrieb der Applikationen für die Applikationsdienste, die im Unternehmen benötigt werden. Zu den allgemeinen Diensten gehören einfache Services, wie die Bereitstellung von Druck- und Dateidiensten. Die Bereitstellung von Datenbankdiensten gehört ebenfalls zu den Application-Services.

► **Backend- & Cloud-Services**

Die Backend-Services stellen mit dem Betrieb des Rechenzentrums und des Unternehmensnetzwerks das Rückgrat der IT-Infrastruktur bereit. Auch der Betrieb physischer Serverkomponenten und einer Hypervisor-Plattform werden durch die Backend-Services abgedeckt.

In einem modernen Unternehmen gehört hierzu auch die Bereitstellung von Cloud-Diensten, da die sichere Anbindung Kernbestandteil der Netzwerkinfrastruktur ist.

Sicher werden Sie beim Lesen der Beschreibungen dieser drei beispielhaften Bereiche ein Verlangen zum Widerspruch gespürt haben. Zwischen den Bereichen gibt es Überschneidungen, die eine eindeutige Abgrenzung schwerfallen lassen. Gerade bei den Applikationen und den Cloud-Diensten kommt es zu Überschneidungen.

Cloud-Dienste sind mit ihren Angeboten IaaS, PaaS und SaaS nicht leicht zu trennen – darum geht es ausführlich in Kapitel 13. Während die Infrastrukturkomponenten (IaaS) meist den Backend-Services zugeschlagen werden, ist es bei den beiden anderen Komponenten nicht mehr so leicht. Es gibt funktionale Komponenten in den PaaS- und SaaS-Angeboten, die einen Infrastrukturanteil besitzen, den die Backend-Dienste für sich beanspruchen. Als Beispiel sei hier die Netzwerkfilterung von Verbindungen zwischen Applikationen und Systemen genannt.

Eine moderne IT-Abteilung darf nicht mehr in starren Silos denken und handeln. Es wird oft und viel über die Demokratisierung der IT gesprochen. Damit ist vordergründig die Übertragung der Verantwortung für IT-Aufgaben an Endanwender gemeint. Diese Demokratisierung ist jedoch nicht auf Endanwender begrenzt, sie trifft die IT ebenso.

Nutzen Sie diese Struktur als Ausgangspunkt zur Abbildung Ihrer organisatorischen Bedürfnisse, wenn Sie sich bisher noch keine Gedanken über eine Struktur gemacht haben und kein Organigramm existiert. In der Regel wird die Organisationsstruktur an anderer Stelle in Ihrem Unternehmen definiert und festgelegt.

Die IT-Leitung des Unternehmens sollte aber in der Lage sein, die betrieblichen Bedürfnisse als Teil einer Organisationsstruktur in die Führungsgremien zu tragen. Seien Sie daher vorbereitet, und machen Sie sich alle Argumente für die von Ihnen vorgeschlagene Struktur bewusst.

---

**Umorganisation im Unternehmen**

Unternehmen sind keine starren Gebilde, sie leben. Dies ist notwendig, um die Weiterentwicklung durch interne und äußere Veränderungen voranzutreiben. Damit einher gehen regelmäßige Umstrukturierungen. Aus rein organisatorischer Sicht stellen Umstrukturierungen keine allzu große Herausforderung dar.

- ▶ Aus IT-Sicht haben *Umorganisationen* zwei Seiten. Die erste ist eine rein technische Auswirkung. In vielen Unternehmen erfolgt die Steuerung der Zugriffsberechtigung auf Applikationen und Daten auf Basis der Unternehmensstruktur, oftmals automatisiert. Solch eine automatisierte Anpassung der Berechtigungen wirkt sich oftmals durch ein erhöhtes Aufkommen an Support-Tickets aus, da z. B. Anwender von einem Tag auf den nächsten den Zugriff auf aus ihrer Sicht wichtige Daten verlieren. Eine weitere technische Auswirkung ist die manuelle Anpassung von Berechtigungen und Organisationsbezeichnungen in Applikationen, die für eine Automation nicht geeignet sind.
- ▶ Eine größere Herausforderung sind *Umstrukturierungen*, die sich direkt auf die IT-Organisation auswirken und IT-Teams verändern. In diesem Fall sind weniger die (zwischen-)menschlichen Herausforderungen im Fokus, sondern die Veränderungen hinsichtlich der individuellen Fachkenntnisse. Dies kann zu der Situation führen, dass zwar rein rechnerisch ausreichend Personen für ein IT-Thema, z. B. die Betreuung der Virtualisierungsplattform, vorhanden sind, diese jedoch nicht über den gleichen Kenntnisstand verfügen. Solche Situationen werden von Ihrem IT-Personal sehr sensibel wahrgenommen. Hier ist es notwendig, dass Umorganisationen in Ihrer IT-Abteilung nicht nur verkündet, sondern ausführlich kommuniziert werden.

Dies ist oftmals leider nicht der Fall. Aus persönlicher Erfahrung kann ich sagen, dass es kein gutes Gefühl ist, von einer beruflichen Veränderung zuerst aus dem veröffentlichten Organigramm zu erfahren und nicht in einem Gespräch mit der Team-Leitung!

In großen Unternehmen ist eine IT-Organisation komplexer und u. U. in der Organisationsstruktur verteilt aufgestellt. Eine Verteilung von IT-Themen und -Verantwortlichkeiten auf zwei oder mehr Bereiche schadet einem Unternehmen mehr, als es nützt. Das folgende Beispiel zeigt eine Unternehmensorganisation, die zwei Spannungsfelder für die IT beinhaltet.

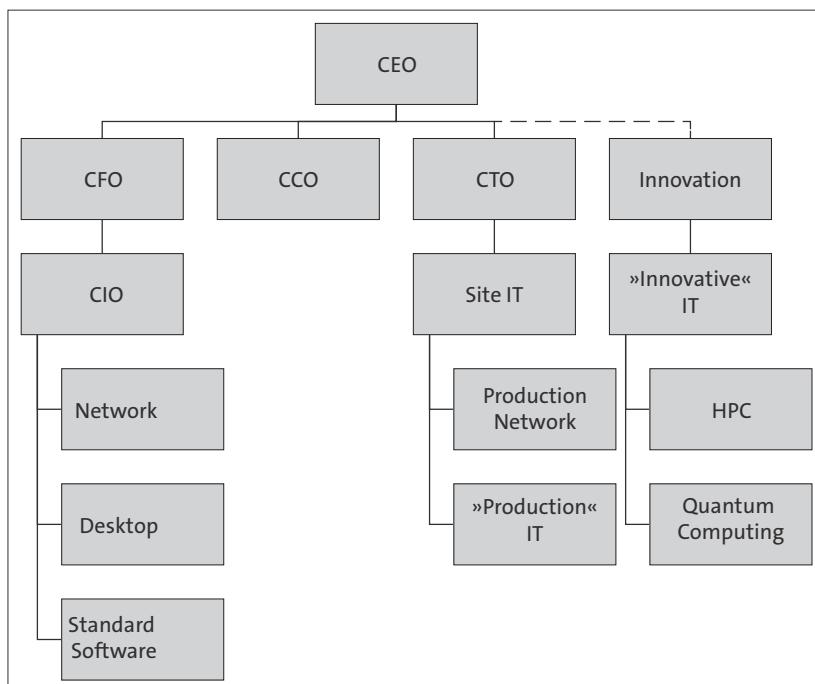
- ▶ Das erste Spannungsfeld ist die Trennung zwischen IT für die allgemeine IT, die dem CIO untersteht, und der IT für die Produktions- und Fertigungsbereiche im Unternehmen, die einem CTO untersteht. Diese beiden Rollen verfolgen innerhalb eines Unternehmens ähnliche Interessen, jedoch aus ganz unterschiedlichen Beweggründen. Diese Interessenkonflikte haben Sie bereits in Abschnitt 1.1.4 kennengelernt.
- ▶ Das zweite Spannungsfeld ist der Bereich »Innovation«. Wie der Name vermuten lässt, ist dieser Bereich die Spielwiese für kreative Innovationsgedanken, um neue Produkte oder Dienstleistungen zu entwickeln oder vorhandene zu verbessern. Aber wo ist die Verbindung zur IT? Schauen wir uns ein Beispiel an.

In der chemischen Industrie ist ein Innovationstreiber die Weiterentwicklung und Optimierung chemischer Rezepteuren und Prozesse. Diese Weiterentwicklung erfordert den Einsatz kostenintensiver IT-Komponenten, wie z. B. High-Performance-Cluster (HPC) für Berechnungen und Simulationen. Was sich unspektakulär liest, enthält zwischen den Zeilen den Sprengstoff für den internen IT-Betriebsfrieden.

- ▶ *Innovation* ist direkt dem CEO unterstellt und muss sich nicht mit anderen Bereichen abstimmen.
- ▶ *Innovation* muss sich nicht an bestehende Beschaffungs- und Genehmigungsprozesse halten, die Freigabe erfolgt einzig durch den CEO.
- ▶ *Innovation* muss sich nicht an Regeln für die IT-Sicherheit halten, insbesondere dann nicht, wenn diese der Innovation im Wege stehen.
- ▶ *Innovation* muss sich nicht verantworten, wenn sich eine Investition als Fehlinvestition herausstellt.

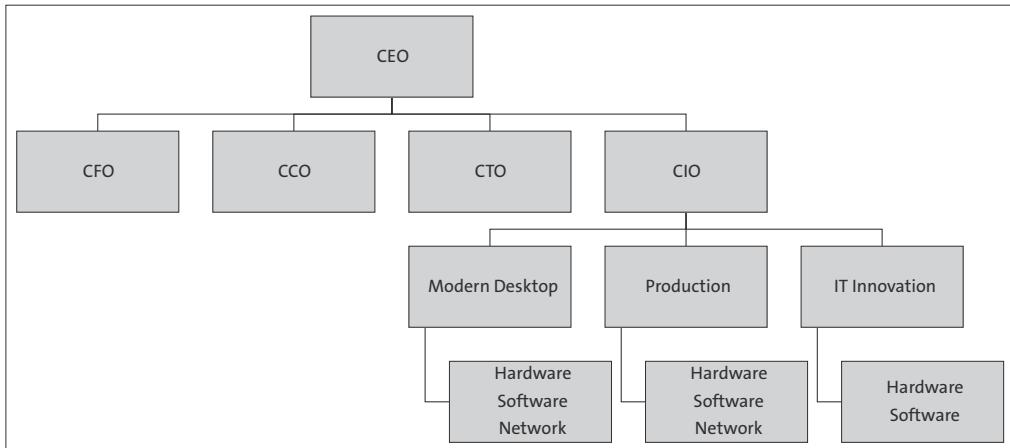
*Innovation* agiert im Unternehmen als freie Radikale. Damit sorgt der Bereich Innovation für latenter Unmut in anderen IT-Bereichen, die sich an Regeln, Bestellprozesse und rechtliche Vorgaben halten müssen.

Das Organigramm in Abbildung 1.1 verdeutlicht die Komplexität und das Spannungsfeld zwischen CIO, CTO und Innovation.



**Abbildung 1.1** Beispiel einer komplexen IT-Organisation mit getrennten IT-Verantwortlichkeiten

Eine bessere Variante stellt das Organigramm in Abbildung 1.2 vor. Hier sind alle IT-relevanten Aktivitäten gebündelt. So kann gerade im Hinblick auf die IT-Sicherheit gewährleistet werden, dass Regeln für den Schutz von und Zugriff auf Daten unternehmensweit eingehalten werden. Dies gilt auch für Innovation.



**Abbildung 1.2** Vereinfachtes Beispiel einer Organisation mit einer verantwortlichen Stelle für IT

Lassen Sie uns mit einem ausführlichen Blick auf die Frontend- und Modern-Workplace-Dienste beginnen.

### Frontend und Modern Workplace

Die Dienstleistungen der Frontend- und Modern-Workplace-Dienste sind das Gesicht der IT im Unternehmen. In diesen Bereich fallen die Bereitstellung aller IT-relevanten Arbeitsgeräte, die Zuweisung von Applikation und der Betrieb der IT-Hotline.

Dies erfolgt oft über ein internes IT-Shopsystem, über das Anwender eigenständig Hard- und Software bestellen können. Ergänzend sind in solch einem System Workflows zur Genehmigung von Waren oder Dienstleistungen ab einem bestimmten Wert hinterlegt. Dies ist wichtig, wenn mit einer Bestellung eine wiederkehrende Belastung der Kostenstelle einer Abteilung einhergeht. Hierzu gehören die monatliche Bereitstellung einer Softwarelizenz oder eines E-Mail-Postfachs, um nur zwei Beispiele zu nennen.

Die Implementierung eines digitalen Arbeitsplatzes ist im IT-Management ein wesentlicher Schritt zur Steigerung der Effizienz und Produktivität eines Unternehmens. Das ist die Aufgabe des Frontend-Services-Teams, das sich um die Gestaltung und Wartung der Benutzeroberflächen kümmert, die den Mitarbeitern den Zugang zu den digitalen Werkzeugen und Ressourcen ermöglichen. Wenn diese Dienste gut funktionieren, arbeiten alle im Unternehmen effizienter und zufriedener.

Das wird besonders bei der Infrastruktur für den Modern Workplace deutlich. Diese umfasst sämtliche digitalen Werkzeuge und Plattformen, die den Mitarbeitenden zur Verfügung stehen, um ihre Aufgaben effizient zu erfüllen. Dazu gehören Kollaborationstools, Cloud-Dienste und mobile Anwendungen.

Ein gut strukturiertes Team sorgt dafür, dass diese Komponenten reibungslos integriert und stets aktualisiert sind. Die fortlaufende Überwachung und Pflege dieser Systeme ist unerlässlich, um Ausfallzeiten zu minimieren und die Datensicherheit zu gewährleisten. Ein starkes Team kann proaktiv auf Veränderungen reagieren und neue Technologien rasch implementieren.

Zu den Aufgaben im Bereich der Betreuung von Frontend-Diensten zählen unter anderem:

- ▶ Die Entwicklung und Pflege der Benutzeroberflächen verschiedener Anwendungen und Plattformen. Diese Oberflächen müssen so gestaltet sein, dass sie benutzerfreundlich und intuitiv zu bedienen sind und den Beschäftigten ihren Arbeitsalltag erleichtern.
- ▶ Das Team übernimmt zudem die Einbindung von Drittanbieter-Tools zur Erweiterung der bestehenden Systemfunktionen.
- ▶ Darüber hinaus ist das Team dafür verantwortlich, regelmäßige Schulungen für die Mitarbeiter durchzuführen, damit alle Nutzer die zur Verfügung stehenden Werkzeuge optimal nutzen können.
- ▶ Ein weiterer Aspekt ist die kontinuierliche Analyse sowie Verbesserung der Benutzererfahrung.
- ▶ Das Team muss gewährleisten, dass sämtliche Anwendungen und Plattformen den aktuellen Sicherheitsstandards entsprechen und regelmäßig upgedatet werden. Dazu gehört auch die Implementierung von Mechanismen zur Authentifizierung und Autorisierung.
- ▶ Das Team ist dafür zuständig, die Systeme auf Sicherheitslücken zu überwachen und schnell auf Bedrohungen zu reagieren, damit Sicherheitsvorfälle frühzeitig erkannt und entsprechende Maßnahmen eingeleitet werden. Dazu gehört auch die Zusammenarbeit mit anderen Abteilungen wie der IT-Sicherheit.
- ▶ Leistungsfähige und verlässliche Endgeräte sind essenziell für den modernen digitalen Arbeitsplatz. Das Frontend-Services-Team ist verantwortlich dafür, dass sämtliche Geräte wie Laptops, Tablets und Smartphones konfiguriert und gepflegt werden. Dazu gehören die Installation und Aktualisierung von Betriebssystemen sowie die Einrichtung der Sicherheitssoftware.
- ▶ Eine effektive Geräteverwaltung sorgt für mehr Sicherheit und Effizienz der Arbeitsabläufe. Ein gut organisiertes Team kann technische Probleme beheben und Lösungen anbieten, um die Produktivität der Angestellten sicherzustellen.

Die Auswahl der passenden Betriebssysteme und ihre Pflege sind ebenfalls von großer Bedeutung. Das Team muss gewährleisten, dass alle Systeme aktuell sind und regelmäßig mit Updates versorgt werden. Dies schließt die Implementierung von Sicherheitsaktualisierungen und Patches ein, um mögliche Schwachstellen zu beheben. Zudem ist es wichtig, dass die Betriebssysteme mit den verwendeten Anwendungen und Tools kompatibel sind. Ein gut ausgebildetes Team kann sicherstellen, dass alle Systeme einwandfrei laufen und die Mitarbeiter effizient arbeiten.

Kollaborationswerkzeuge sind an einem digitalen Arbeitsplatz unverzichtbar. Ihr Frontend-Services-Team sollte sicherstellen, dass alle Kollaborationstools wie Videokonferenzsoftware, Chat-Anwendungen und Projektmanagement-Tools optimal konfiguriert und gewartet werden. Die nahtlose Integration dieser Werkzeuge in die bestehende IT-Infrastruktur ist entscheidend für eine reibungslose Zusammenarbeit. Ein gut koordiniertes Team kann gewährleisten, dass alle Mitarbeitenden die bereitgestellten Tools effizient nutzen. Laufende Schulungen und Unterstützung für die Mitarbeiter sind dabei essenziell.

Am Ende des Tages sind ein gutes Frontend-Team und eine moderne Arbeitsplatzinfrastruktur wichtig, damit ein digitaler Arbeitsplatz erfolgreich sein kann. Das Team kümmert sich um die Benutzeroberflächen, bringt neue Technologien ein und sorgt für die Sicherheit. Wenn das Team gut organisiert und kommunikativ ist, kann es die Effizienz und Produktivität eines Unternehmens stark verbessern. Wer neu im IT-Management ist, sollte verstehen, wie wichtig diese Rolle ist, und versuchen, die nötigen Fähigkeiten zu erlernen, um so ein Team effektiv zu leiten. Laufende Weiterbildungen und die Anpassung an neue Technologien sind dabei besonders wichtig.

## Applikationen

Eine Applikationsplattform bildet das Fundament Ihrer IT-Infrastruktur. Sie erlaubt die effiziente Ausführung und Verwaltung verschiedener Anwendungen. Ohne eine robuste Applikationsplattform könnten Ihre Geschäftsprozesse unterbrochen werden. Diese Plattform gewährleistet, dass Anwendungen sicher und zuverlässig betrieben werden. Sie bietet die erforderliche Flexibilität, um auf veränderte Geschäftsanforderungen reagieren zu können. Die wesentliche Rolle dieser Plattform besteht darin, den reibungslosen Betrieb Ihrer IT-Umgebung zu gewährleisten.

## Backend- und Cloud-Dienste

Die Backend-Dienste bilden das Rückgrat der IT-Infrastruktur eines Unternehmens und umfassen Server, Datenbanken sowie Anwendungen, die im Hintergrund arbeiten, um Frontend-Dienste zu unterstützen. Diese Komponenten sind entscheidend für die Datenverarbeitung, -speicherung und Anwendungsbereitstellung. Ohne eine robuste Backend-Infrastruktur könnten viele Geschäftsprozesse nicht sicher und

stabil ablaufen. Ein gut strukturiertes Backend gewährleistet eine zuverlässige und sichere IT-Umgebung.

Cloud-Dienste stellen eine flexible und skalierbare Lösung für die IT-Anforderungen eines Unternehmens dar. Sie gewähren Zugriff auf Rechenressourcen und Applikationen über das Internet, was den Bedarf an physischer Hardware verringert und eine kostengünstige Verwaltung der IT-Ressourcen ermöglicht. Darüber hinaus bieten Cloud-Dienste hohe Verfügbarkeit und Zuverlässigkeit, da sie in der Regel von renommierten und global agierenden Anbietern mit starken Sicherheitsmaßnahmen bereitgestellt werden. Die Einführung von Cloud-Diensten kann die IT-Infrastruktur eines Unternehmens erheblich verbessern, indem sie die Flexibilität und Skalierbarkeit der IT-Ressourcen erhöht.

Ein grundlegender Dienst eines Unternehmens ist die Internetanbindung, die den Zugang zum weltweiten Netzwerk bereitstellt. Eine stabile und ausfallsichere Internetverbindung ist unverzichtbar für Kommunikation und Datenaustausch. Sie ermöglicht den Zugang zu Cloud-Diensten und unterstützt tägliche Geschäftsprozesse.

*DNS* (Domain Name System) ist ein weiterer wichtiger Basisdienst der Backend-Dienste. DNS übersetzt Domainnamen in IP-Adressen, sodass Benutzer auf interne und externe Websites und Dienste zugreifen können. Ein zuverlässiger DNS-Dienst stellt sicher, dass Anfragen schnell und korrekt verarbeitet werden. Ein gut konfigurierter DNS-Dienst trägt nicht nur zur Benutzerfreundlichkeit bei, sondern ist ebenfalls ein wichtiger Baustein Ihrer IT-Sicherheit.

Zusammen bilden Backend- und Cloud-Dienste die Basisdienste in Ihrem Unternehmen, die für den reibungslosen Betrieb Ihrer IT-Infrastruktur unerlässlich sind. Sie stellen sicher, dass alle Anwendungen und Dienste zuverlässig und sicher betrieben werden können. Die Verwaltung dieser Dienste erfordert sorgfältige Planung und regelmäßige Wartung. Ein gut organisiertes IT-Management-Team trägt dazu bei, die Stabilität und Sicherheit Ihrer IT-Umgebung zu gewährleisten.

## Partnerunternehmen

Nur in den seltensten Fällen kann die IT-Abteilung eines Unternehmens alle erforderlichen Aufgaben eigenständig umsetzen. Die Anforderungen in allen Bereichen der IT erfordern Spezialkenntnisse, die einen zeitweisen oder dauernden Einsatz von externem Fachpersonal erfordern. Hierzu arbeiten Sie mit Partnerunternehmen zusammen, mit denen Sie vertragliche Bindungen eingehen.

Diese Partnerschaft bezieht sich nicht nur auf die Erbringung von Beratungsdienstleistungen, sondern bindet auch die Bereitstellung und den Betrieb von Applikationen mit ein. In gleichem Maße können Sie als Partnerunternehmen für andere Unternehmen auftreten, indem Sie entsprechende Applikationen oder Beratungsdienstleistungen erbringen.

In einer anderen Variante hat Ihr Unternehmen ein eigenes Netzwerk an externen Partnerunternehmen, die Ihre Dienstleistung oder Ihr Produktpotfolio an Kunden vertreiben. Diese Art der partnerschaftlichen Zusammenarbeit hat nicht nur Berührungspunkte mit dem Vertrieb Ihres Unternehmens, sondern ebenfalls Verbindung zu Ihrer IT-Abteilung.

#### 1.4.4 IT-Prozesse

IT-Prozesse sind strukturierte Abläufe und Aktivitäten innerhalb einer IT-Organisation, die darauf abzielen, die Effizienz, Qualität und Kontrolle von IT-Dienstleistungen und -Operationen zu gewährleisten. Diese Prozesse helfen dabei, die Anforderungen Ihres Unternehmens zu erfüllen, die technologische Infrastruktur zu verwalten, Sicherheitsstandards einzuhalten und einen reibungslosen IT-Betrieb sicherzustellen. Hier sind einige grundlegende IT-Prozesse:

##### ► Change-Management (Änderungsmanagement)

Jede Änderung an einem IT-System kann andere Teile des Systems beeinflussen, oft auf unerwünschte Weise. Um diese Gefahren zu vermeiden, gibt es das *Change-Management*, das gewährleistet, dass alle Änderungen gründlich geplant, getestet und überwacht werden. Zusätzlich wird damit sichergestellt, dass alle Änderungen den Geschäftszielen und -bedürfnissen entsprechen und dass sie den Nutzern und Stakeholdern verständlich mitgeteilt werden.

Ein wirksames Change-Management unterstützt zudem die kontinuierliche Verbesserung, indem es einen standardisierten Prozess bietet, um Feedback zu erhalten und aus jeder Änderung zu lernen. Außerdem sorgt ein CM dafür, dass die in den SLAs zugesicherten Leistungen erbracht werden und unnötige Unterbrechungen aktiv verhindert werden.

Wie Sie ein Change-Management implementieren können, zeigt Abschnitt 12.4.2.

##### ► Incident-Management (Vorfallmanagement)

Die meisten geschäftlichen Abläufe sind auf IT-Systeme angewiesen. Sollten diese Systeme ausfallen oder gestört werden, kann das Geschäft ernsthaft beeinträchtigt werden. Daher ist ein gutes *Incident-Management* wichtig, um diese Beeinträchtigungen zu reduzieren, indem es einen klar definierten Prozess für die rasche Erkennung, Untersuchung und Behebung von IT-Störungen (*Incidents*) anbietet. Es unterstützt auch die Kommunikation mit den Nutzern während eines Vorfalls und stellt sicher, dass sie kontinuierlich über den Status und die voraussichtliche Lösungsdauer informiert werden.

Durch Incident-Management können die IT-Systeme und -Prozesse kontinuierlich verbessert werden. IT-Teams können Vorfälle analysieren, um Muster und Trends zu erkennen, die auf bestehende Probleme hindeuten. Das erlaubt ihnen, proaktiv

diese Probleme zu lösen und künftige Vorfälle zu vermeiden. Außerdem ermöglicht das Incident-Management das Lernen aus Fehlern und das Austauschen von Best Practices, was zu einer besseren IT-Organisation führt.

► **Release-Management (Freigabemanagement)**

Das *Release-Management* hilft, die Softwareprodukte und -dienste qualitativ hochwertig und stabil zu halten. Es erlaubt die systematische Planung, Abstimmung und Kontrolle von Software-Releases von der Entwicklung bis zur Bereitstellung. Dies hilft, Risiken zu vermeiden, Ausfallzeiten zu verringern und sicherzustellen, dass neue Features und Verbesserungen effektiv und effizient in die Produktionsumgebung übernommen werden. Außerdem unterstützt das Release-Management die Zusammenarbeit zwischen verschiedenen Teams wie Entwicklung, Betrieb und Qualitätssicherung, indem es deutliche Kommunikationskanäle und Zuständigkeiten schafft.

Außerdem erlaubt das Release-Management eine bessere Steuerung und Übersicht über den Software-Lebenszyklus. Es bietet einen systematischen Ansatz für die Handhabung von Änderungen, einschließlich der Erkennung, Einteilung und Gewichtung von Änderungswünschen. Dies führt zu einer erhöhten Rückverfolgbarkeit und ermöglicht es den Teams, den Status von Releases zu überwachen und mögliche Probleme frühzeitig zu erkennen. Durch die Vereinheitlichung von Release-Abläufen und -Richtlinien kann das Release-Management auch dazu beitragen, die Compliance mit Regeln und Normen sicherzustellen, was vor allem in regulierten Branchen essenziell ist. Insgesamt hilft ein effektives Release-Management dabei, die Geschäftskontinuität zu sichern und den Geschäftsnutzen von IT-Investitionen zu optimieren.

► **Configuration-Management (Konfigurationsmanagement)**

Ein *Configuration-Management* schafft eine stabile und verlässliche Betriebsumgebung für Produkte und Systeme Ihrer IT-Infrastruktur. Es erlaubt die Erkennung und Steuerung von Systemkomponenten, die Handhabung von Änderungen und die Erhaltung der Integrität und Nachverfolgbarkeit im gesamten Lebenszyklus. Ein Configuration-Management unterstützt die Leistung und Wirksamkeit von IT-Prozessen, indem es dafür sorgt, dass alle Systemkomponenten richtig eingestellt sind und gut zusammen funktionieren. Es hilft auch dabei, Stillstandzeiten zu reduzieren und die Servicequalität zu erhöhen, indem es schnelle und präzise Diagnosen und Lösungen für Probleme bietet.

Außerdem ist das Configuration-Management wichtig für die Reduzierung von Risiken. Durch eine präzise Dokumentation und Steuerung von Änderungen können IT-Teams mögliche Folgen von Änderungen abschätzen und unvorhergesehene Schwierigkeiten vermeiden. Es hilft auch dabei, Vorschriften und Standards einzuhalten, indem es einen Nachweis für Änderungen liefert und sicherstellt, dass nur genehmigte Änderungen vorgenommen werden. Letztlich erlaubt CM

eine wirksame Planung und Abstimmung von Änderungen, was zu einer besseren Zusammenarbeit zwischen Teams und einer höheren Stakeholder-Zufriedenheit führt. Insgesamt trägt ein effektives Configuration-Management dazu bei, den Betrieb des Geschäfts zu sichern und den Nutzen von IT-Investitionen zu optimieren.

#### ► **Service-Level-Management (SLM)**

Die Abstimmung der Kundenerwartungen und der IT-Organisationskapazitäten ist ein wichtiger Aspekt des SLM für die IT. Es erlaubt das Festlegen, Messen und Berichten von Service Level Agreements (SLAs, OLAs), die die Qualität, Verfügbarkeit und Leistung von IT-Services vorgeben. Das SLM sorgt dafür, dass die IT-Services den vereinbarten Standards entsprechen, und fördert somit die Kundenzufriedenheit und das Vertrauen in die IT-Organisation. Außerdem hilft das SLM bei der Entscheidungsfindung, indem es nützliche Informationen über die Leistung von IT-Services liefert und Verbesserungsmöglichkeiten identifiziert.

Das *Service-Level-Management* ist auch wichtig für die Reduzierung von Risiken und die Verwaltung der Kosten. Durch das Messen der Servicequalität und das frühe Erkennen von Schwierigkeiten können IT-Teams vorbeugend handeln, um Störungen zu vermeiden und die Geschäftskontinuität sicherzustellen. Das SLM ermöglicht auch eine effiziente Planung und Verteilung von Ressourcen, indem es den Bedarf an IT-Services prognostiziert und die Nutzung von IT-Ressourcen verbessert. Dies kann helfen, die Betriebskosten zu minimieren und den Return on Investment (ROI) zu erhöhen. Insgesamt hilft ein effektives SLM dabei, den Geschäftswert von IT-Investitionen zu steigern und einen qualitativ hochwertigen IT-Service zu bieten, der die Geschäftsziele fördert.

#### ► **Availability-Management (Verfügbarkeitsmanagement)**

Das *Availability-Management* hat das Ziel, die IT-Services für Ihr Unternehmen durchgehend zuverlässig verfügbar sind. Es umfasst die Gestaltung, Umsetzung und Kontrolle von Maßnahmen, die gewährleisten, dass IT-Services innerhalb der abgestimmten Servicezeiten bereitstehen und den Geschäftsbedürfnissen entsprechen. Indem es Ausfallzeiten reduziert und eine hohe Serviceverfügbarkeit sicherstellt, trägt das Availability-Management dazu bei, die Geschäftskontinuität aufrechtzuerhalten, die Kundenzufriedenheit zu steigern und den Geschäftsnutzen zu erhöhen. Außerdem hilft es der IT-Organisation dabei, Schwachstellen aufzudecken und zu beheben, die sich negativ auf die Serviceverfügbarkeit auswirken könnten.

Das Availability-Management hat auch einen wichtigen Einfluss auf die Risikoreduzierung und die Kostensenkung. Indem sie die Serviceverfügbarkeit überwachen und Probleme frühzeitig erkennen, können IT-Teams präventiv handeln, um Ausfälle zu verhindern und die Servicequalität zu steigern. Es hilft auch bei der Planung und Verteilung von IT-Ressourcen, indem es den Bedarf an IT-Services abschätzt und die IT-Ressourcennutzung effizient gestaltet. Dies kann dazu beitra-

gen, die Betriebskosten zu verringern und den Return on Investment (ROI) zu erhöhen. Insgesamt ermöglicht ein wirksames Availability-Management, den geschäftlichen Nutzen von IT-Investitionen zu maximieren und einen hochwertigen IT-Service anzubieten, der die Geschäftsziele fördert.

► **IT Service Continuity Management (ITSCM)**

Das *IT Service Continuity Management* stellt die Geschäftskontinuität auch unter Notfall- und Krisenbedingungen sicher. Es beinhaltet die Planung und Durchführung von Aktionen, um IT-Services bei einem Ausfall oder einer Störung schnellstmöglich wiederherzustellen. Das ITSCM hilft, Geschäftsunterbrechungen zu vermeiden, die Kundenzufriedenheit zu steigern und den Geschäftswert zu maximieren, indem es die Ausfallzeiten minimiert und eine rasche Wiederherstellung von IT-Services garantiert. Außerdem hilft es der IT-Organisation, Schwachstellen zu erkennen und zu beheben.

Wichtige Aspekte des Continuity-Managements sind die IT-Risikoreduzierung und die Kostenersparnis. Durch das Erstellen und Anwenden von Business-Continuity-Plänen und Disaster-Recovery-Plänen können IT-Teams Notfall- und Krisensituationen bewältigen und die Folgen von IT-Serviceunterbrechungen begrenzen. Außerdem hilft es bei der Planung und Zuweisung von IT-Ressourcen, indem es den Bedarf an IT-Services abschätzt und die IT-Ressourcennutzung verbessert.

► **Identity and Access Management (Identitäts- und Zugriffsmanagement)**

*Identity und Access Management (IAM)* schützt und bewahrt die IT-Systeme und Unternehmenswerte, denn es verwaltet digitale Identitäten und Zugriffsberechtigungen, um zu garantieren, dass nur befugte Benutzer auf die IT-Ressourcen zugreifen können, für die sie explizit freigeschaltet wurden. Durch die Regulierung, wer welche Ressourcen nutzen kann, hilft IAM dabei, Datenverluste zu vermeiden, die Compliance zu erfüllen und das Vertrauen der Benutzer in die IT-Organisation zu erhöhen. Außerdem hilft es der IT-Organisation bei der Erkennung und Behebung von Sicherheitsrisiken, die die IT-Sicherheit gefährden könnten.

Das IAM ist auch für die Steigerung der Effizienz und Produktivität von Bedeutung. Durch die Automatisierung von IAM-Prozessen können IT-Teams Zeit und Ressourcen einsparen, die ansonsten für die manuelle Verwaltung von Benutzerkonten und Zugriffsrechten erforderlich wären. Es verbessert auch die Benutzererfahrung, indem es den Benutzern erlaubt, nahtlos auf die Ressourcen zuzugreifen, die sie benötigen, ohne mehrere Anmeldeinformationen eingeben zu müssen. Dies kann dazu führen, dass die Benutzer zufriedener sind und die IT-Services besser annehmen. Insgesamt hilft ein effektives IAM, den Geschäftswert von IT-Investitionen zu erhöhen und einen sicheren und benutzerfreundlichen IT-Service bereitzustellen, der die Geschäftsziele fördert.

### ► Service Desk (SD)

Der Service Desk ist eine zentrale Kontaktstelle für Benutzer, die Hilfe bei IT-bezogenen Problemen und Anfragen benötigen. Er hat eine wichtige Funktion bei der Sicherstellung der Betriebskontinuität, indem er rasche und effiziente Lösungen für IT-Probleme anbietet (1st-Level-Support). Durch das Bereitstellen eines einheitlichen und effektiven Kundenservices verbessert der Service Desk die Kundenzufriedenheit und das Vertrauen in die IT-Organisation. Außerdem hilft der Service Desk der IT-Organisation dabei, wiederkehrende Probleme zu erkennen und zu lösen, die sich negativ auf die IT-Leistung auswirken könnten.

Mit Service-Desk-Automation können IT-Teams wertvolle Zeit und Ressourcen einsparen, die sie sonst für die manuelle Lösung von Support-Anfragen verwenden müssten. Er verbessert auch das Benutzererlebnis, indem er den Benutzern erlaubt, mühelos Hilfe zu bekommen, ohne mehrere Schritte befolgen zu müssen. Dies kann helfen, die Benutzerzufriedenheit zu steigern und die Nutzung der IT-Services zu fördern. Insgesamt hilft ein effizienter Service Desk dabei, den geschäftlichen Nutzen von IT-Investitionen zu erhöhen und einen qualitativen IT-Service zu bieten, der die Geschäftsziele unterstützt.

Die IT-Prozesse orientieren sich oft an bewährten Vorgehensweisen, wie sie zum Beispiel im ITIL-Framework (*IT Infrastructure Library*) beschrieben sind. Durch die Einführung und Verbesserung dieser Prozesse wird gewährleistet, dass die IT-Serviceleistung für das Unternehmen und für Kunden beständig, verlässlich und qualitativ hochwertig ist.

### KI und Automation

In der jüngsten Zeit haben sich die Möglichkeiten zur Automation von Standardreaktion und der KI-gestützten Analyse von Vorfällen immens weiterentwickelt. Die Komplexität der IT erfordert es, diese Möglichkeiten zu nutzen. Chatbots können in Serviceportalen Standardanfragen von Anwendenden automatisch beantworten und ermöglichen es den Mitarbeitenden, sich auf besondere Fälle zu konzentrieren. Die KI-gestützte Analyse von Sicherheitsinformationen wiederum erkennt z. B. Angriffsmuster schneller und kann mit vorfallbezogenen Aktionen, z. B. verpflichtender Multifaktor-Authentifizierung, reagieren.

Auf KI-Unterstützung gerade im Kontext der IT-Sicherheit zu verzichten, kann man getrost als grob fahrlässig bezeichnen.

### 1.4.5 IT-Servicemanagement

Der Begriff IT-Management wird oftmals als Abkürzung des *IT-Servicemanagements* (ITSM) wahrgenommen. Ein IT-Servicemanagement bezieht sich auf alle Verfahren,

Prozesse und Richtlinien, die ein Unternehmen bei der Verwaltung und Umsetzung der IT-Dienstleistungen innerhalb des Unternehmens unterstützen (darum wird es in Kapitel 12 gehen).

Unternehmen übernehmen häufig vordefinierte Empfehlungen (Best Practices), um einen strukturierten Servicemanagement-Ansatz zu gewährleisten. Wie überall in der IT-Branche gibt es jedoch zahlreiche Rahmenkonzepte, sogenannte Frameworks, für das ITSM, aus denen man wählen kann.

Zu den bekannteren ITSM-Frameworks gehören:

- ▶ ITIL® – Information Technology Infrastructure Library
- ▶ COBIT – Control Objectives for Information and Related Technology
- ▶ MOF – Microsoft Operations Framework
- ▶ eTOM – Enhanced Telecom Operations Map
- ▶ TOGAF – The Open Group Architecture Framework

Was die gängigsten ITSM-Frameworks anbelangt, so hat jedes von ihnen einen anderen Nutzen und Einsatzzweck. ITIL hat sich seit Jahren als De-facto-Standard für die Abbildung von IT-Servicemanagement-Anforderungen und -Prozessen in der IT-Branche etabliert.

Aber sind IT-Servicemanagement und IT-Management wirklich das Gleiche?

Nein, denn das IT-Servicemanagement ist nur ein Bestandteil des IT-Managements. Ebenso hat das ITSM natürliche Grenzen in der Anwendung. Es kann nicht auf jeden Aspekt angewandt werden, selbst wenn Hersteller von ITSM-Lösungen Ihnen etwas anderes erzählen.

Gerade in der gleichzeitigen Verwaltung zentralisierter und dezentralisierte Systeme und Prozesse offenbaren sich die Schwächen. Auftretende Schwächen einer einmal eingeführten ITSM-Lösung werden gerne durch individuelle Anpassungen und Erweiterungen kompensiert, was wiederum Aktualisierungen oder eine Migration der ITSM-Lösung erschwert oder gar unmöglich macht.

#### 1.4.6 Standardisierung

Die Standardisierung der IT-Infrastruktur und der IT-Komponenten ist ein Wunsch, der in Foliensätzen und Zieldefinitionen immer wieder genannt wird. Ebenso oft, wie der Wunsch formuliert wird, wird auch davon abgewichen. Gerade diese Abweichung von Standard ist es, was die IT-Branche, und hier insbesondere das Beratungsgeschäft, antreibt.

Die Einführung von standardisierten IT-Komponenten ist in vielerlei Hinsicht schmerhaft. Zum einen müssen sich IT-Administratoren von ihrer individuell auf-

gebauten IT-Infrastruktur verabschieden, zu der sie im Laufe der Zeit eine besondere Beziehung entwickelt haben. Gerade der Wechsel einer technologischen Plattform birgt das Risiko ausgedehnter Diskussionen über den Sinn einer neuen Lösung.

Ähnlich sieht es bei den Anwendern im Unternehmen aus. Seit der Einführung von IT-unterstützten Lösungen am Arbeitsplatz haben sich Anwender daran gewöhnt, dass ihnen fast jeder Wunsch erfüllt wurde. Wenn nun eine neue Lösung nicht die gleiche Schaltfläche in der gleichen Farbe an der gleichen Bildschirmposition bietet, wird lautstark protestiert. Im schlimmsten Fall führt dies zu einem stillen inneren Boykott der neuen Lösung und zu einem Scheitern der Einführung.

#### 1.4.7 Demokratisierung der IT

In der alten IT-Welt haben Anwender wenig Spielraum, um ihre betrieblichen Herausforderungen in den Fachabteilungen eigenständig zu lösen. Sie sind auf starre und langwierige Prozesse zur Ermittlung von Anforderungen, Evaluierung und Einführung von Softwarelösungen angewiesen. Oft genug scheitert die Einführung von Lösungen, um betriebliche Abläufe zu verbessern.

Die Digitalisierung von Geschäftsaufgaben ist eine der großen Herausforderungen für Unternehmen. Dies kann nur gelingen, wenn Sie die Anwender in den Fachabteilungen aktiv einbinden und ihnen die Werkzeuge an die Hand geben, um eigenständig Lösungen umzusetzen. Niemand kennt die Anforderungen und Bedürfnisse besser als die Fachabteilungen selbst.

Damit dies gelingen kann, muss die IT-Abteilung nicht nur die Werkzeuge bereitstellen, sondern auch Verantwortung abgeben, die IT wird demokratischer.

Dies ist alles andere als einfach. In einer Arbeitswelt, in der Menschen es seit Jahrzehnten gewohnt sind, nur die Aufgaben zu erledigen, die in ihrer Arbeitsplatzbeschreibung aufgeführt sind, bedarf es zuerst eines Kulturwandels. Ohne Kulturwandel kommt es zwangsläufig zu einer Ablehnung der neuen Werkzeuge.

### 1.5 IT-Kosten

Die IT eines Unternehmens verursacht Kosten, das lässt sich nicht wegdiskutieren. Aber andererseits stellt die IT natürlich einen wichtigen Faktor für die Effektivität, Konkurrenzfähigkeit und Finanzstabilität des Unternehmens dar.

Eine wichtige Aufgabe besteht somit darin, ein angemessenes Gleichgewicht zwischen kostengünstiger und innovativer Nutzung von Technologien zu finden. Unternehmen müssen nicht nur ihre vorhandenen IT-Kosten verbessern, sondern auch mit den stetig wandelnden technologischen Umgebungen mithalten können. Ein vorausschauendes Kostenmanagement in der IT erlaubt Ihnen, Investitionen besser zu

planen, Ressourcen gezielter einzusetzen und damit einen echten Nutzen für das Unternehmen zu erzeugen. In diesem Zusammenhang ist eine gründliche Untersuchung und Anpassung der IT-Ausgaben erforderlich, um zu gewährleisten, dass die Investitionen nicht nur den aktuellen Anforderungen entsprechen, sondern auch eine stabile Basis für zukünftiges Wachstum und Konkurrenzfähigkeit schaffen.

### 1.5.1 Profit- oder Cost-Center

Sowohl *Cost-Center* als auch *Profit-Center* existieren in der IT eines Unternehmens.

- ▶ Ein *Cost-Center* ist zum Beispiel die Abteilung für IT-Support, die Dienstleistungen wie technischer Support, Serverwartung und interne Softwareentwicklung anbietet. Diese Abteilungen sind für den Geschäftsbetrieb unerlässlich, tragen aber nicht direkt zum Umsatz bei. Ein Cost-Center verursacht primär Kosten.
- ▶ Ein *Profit-Center* hingegen ist eine Abteilung, die ein Produkt oder eine Dienstleistung herstellt und vertreibt, das bzw. die Einnahmen bringt. Ein Beispiel wäre die Produktionsabteilung eines Unternehmens, das Computerhardware produziert und verkauft. Diese Abteilung trägt unmittelbar zum Umsatz des Unternehmens bei.

Ob die IT also ein Cost-Center oder ein Profit-Center ist, hängt von der der konkreten Struktur und Strategie des Unternehmens ab.

Die IT wird als Cost-Center angesehen, wenn sie vor allem als eine Hilfsfunktion verstanden wird, die für das Funktionieren der Geschäftsprozesse erforderlich ist, aber keinen unmittelbaren Einfluss auf das Umsatzwachstum hat. In diesem Fall wird sie als Kostenpunkt gesehen, der Ressourcen benötigt, um notwendige Services anzubieten, aber keinen direkten Gewinn erzielt. Wenn die IT direkt zum Wert des Unternehmens beiträgt und sogar selbstständig Umsatz oder Gewinn erzielen kann, wird sie als Profit-Center angesehen. Dies trifft eher auf Unternehmen zu, bei denen die IT ein wesentlicher Teil des Geschäftsmodells ist, wie z. B. in Technologieunternehmen oder Unternehmen, deren Hauptangebote digitale Services sind. Die IT hat in vielen modernen Unternehmen einen Wandel von einer reinen Kostenstelle zu einem strategischen Partner und Wertschöpfer vollzogen. Durch die wachsende Digitalisierung und Technologisierung kann die IT immer mehr zum Innovationspotenzial, zur Effizienzoptimierung und zur Generierung neuer Geschäftschancen beitragen.

Beachten Sie, dass die IT nicht immer klar als Cost-Center oder Profit-Center eingestuft werden kann. Oft gibt es IT-Aufgaben, die eher als Cost-Center angesehen werden, wie z. B. die Wartung der Infrastruktur und die Sicherstellung der Betriebsbereitschaft, während andere IT-Bereiche als Profit-Center gelten können, wenn sie direkt zum Umsatz beitragen. Diese Unterscheidung kann großen Einfluss auf Ihre Arbeit haben. Darum geht es ausführlich in Kapitel 4, »Finanzmanagement«.

### 1.5.2 Lizenzmanagement

IT-Lizenzmanagement (ausführlich besprochen in Kapitel 8) ist ein zentraler Prozess in Ihrem Unternehmen, der den legalen und effizienten Umgang mit kommerzieller oder auch freier Software sicherstellt. Es beeinflusst alle Bereiche des Unternehmens, von der Beschaffung über jeden PC-Arbeitsplatz bis hin zum Management. Ein aktives Lizenzmanagement ermöglicht es Ihrem Unternehmen, Softwarelizenzen umfassend zu verwalten, was zu erheblichen Vorteilen, wie Kosteneinsparungen (Lead-Buyer) und effizienterer Ressourcennutzung, führen kann. Darüber hinaus hilft es Ihrem Unternehmen, die Nutzung von Software im Einklang mit den individuellen Lizenzbedingungen der Hersteller zu halten, was wichtig ist, um rechtliche Konsequenzen und finanzielle Verluste zu vermeiden.

Darüber hinaus ist die Anwendung einer Lizenzmanagement-Software ein wichtiger Bestandteil des IT-Asset-Managements von Unternehmen und von grundlegender Bedeutung für die Cybersicherheit und die allgemeine IT-Verwaltung.

Ein wesentlicher Punkt, der bei der Nutzung von Cloud-Diensten berücksichtigt werden sollte, ist das Risiko einer *Überlizenenzierung*. Dies bedeutet, dass mehr Lizenzen erworben wurden, als tatsächlich benötigt werden. Durch ein effektives Lizenzmanagement kann diese Überlizenenzierung vermieden werden, indem der Bedarf an Cloud-Lizenzen genau ermittelt und die Nutzung optimiert wird.

Ihr Unternehmen kann Audits von Softwareanbietern unterzogen werden, um sicherzustellen, dass ihre Softwarelizenzen ordnungsgemäß eingesetzt werden. Ein funktionierendes Lizenzmanagement erleichtert die Vorbereitung auf solche Audits, indem es eine klare Dokumentation des Lizenzstatus und der Nutzung bereitstellt.

# Kapitel 5

## Enterprise-Architektur

*Enterprise-Architektur ist mehr als nur ein klangvoller Begriff – sie ist der Schlüssel, um komplexe IT-Landschaften strategisch, nachhaltig und teamübergreifend zu gestalten.*

Der Begriff *Enterprise-Architektur* wird wie viele andere Begriffe, die Sie in die diesem Buch kennenlernen, inflationär oder außerhalb jeden Kontexts verwendet. Dies liegt in weiten Teilen daran, dass diese englische Bezeichnung schnell Eindruck schindet, wohingegen der Begriff Unternehmensarchitektur wenig bedeutungsvoll ist. Mit der Bezeichnung der technischen Anforderungen und des betrieblichen Ist-Zustands geht auch die Rollenbezeichnung *Enterprise-Architekt* einher, die wir uns im Abschnitt 5.2 genauer anschauen, denn auch wenn die unterschiedlichen Architekten-Rollen in jedem Unternehmen anders zugeschnitten werden, erfüllen sie eine wichtige Aufgabe. Achten Sie daher darauf, dass sie für Ihr Unternehmen passend definiert und dokumentiert sind.

Ohne eine gut geplante Enterprise-Architektur ist ein sicherer und stabiler Betrieb einer IT-Infrastruktur nicht möglich. Daher stehen die Entwicklung der Enterprise-Architektur und ein Verständnis der zugehörigen Komponenten am Anfang dieses Kapitels (siehe Abschnitt 5.1). Denn nur so lässt sich der Betrieb der IT-Plattform als Basis für den Geschäftsbetrieb Ihres Unternehmens durch das *Business-Continuity-Management* (BCM) absichern (siehe Abschnitt 5.3). Das BCM hilft Ihnen, Betriebsrisiken zu erkennen, zu bewerten und Prozesse gegen mögliche Störungen zu entwickeln. Eine Störung der IT-Infrastruktur kann nicht nur den Geschäftsbetrieb zum Stillstand bringen, sondern im schlimmsten Fall das Ende des Unternehmens bedeuten.

Ein wichtiger Schritt, um Ausfälle und Sicherheitsprobleme bereits während der Architekturplanung zu adressieren, ist die Aufteilung der Gesamtumgebung in Entwicklungs-, Test und Produktionsumgebungen. Das schauen wir uns in Abschnitt 5.4 an.

Zu guter Letzt erfahren Sie in Abschnitt 5.5, wie eine Enterprise-Architektur umgesetzt wird.

## 5.1 Entwicklung einer Enterprise-Architektur

Die Komplexität heutiger IT-Infrastrukturen mit all ihren erforderlichen Komponenten für einen sicheren und stabilen Betrieb erfordert ein ganzheitliches Verständnis der Gesamtumgebung.

In diesem Kapitel werfen wir einen Blick auf die Entwicklung einer ganzheitlichen IT-Infrastruktur für Ihr Unternehmen, die Rolle des Enterprise-Architekten und die Herausforderungen bei der Umsetzung. Gerade die kontinuierliche Einführung und stete Umsetzung einer Architektur ist eine kräftezehrende und langwierige Aufgabe. Diese Aufgabe kann ein Enterprise-Architekt nicht allein durchführen. Das Fachwissen der einzelnen IT-Teams, wie z. B. Netzwerk, Backend- oder Client-Services, ist notwendig, um eine zukunftssichere IT-Architektur umzusetzen und zu betreiben.

Die Entwicklung einer ganzheitlichen und planvollen IT-Architektur ist Voraussetzung für einen stabilen und sicheren Betrieb Ihrer IT-Infrastruktur. Nur mit einer zentral abgestimmten, sich stetig weiterentwickelnden Architektur können Sie sicherstellen, dass Ihr Unternehmen die Möglichkeiten moderner IT-Komponenten ausschöpft.

Die technischen Komponenten sind allerdings nur Mittel zum Zweck. Sie benötigen eine umsetzbare Vision zur Nutzung dieser Komponenten. Ohne eine solche Vision lassen Sie das Potenzial der erworbenen Komponenten ungenutzt. Diese Vision wird von allen IT-Teams gemeinschaftlich getragen und mit dem Fachwissen des jeweiligen Teams weiterentwickelt.

Schauen wir uns zuerst die Komponenten einer Enterprise-Architektur an.

### 5.1.1 Komponenten einer Enterprise-Architektur

Die Komponenten einer Enterprise-Architektur sind nicht nur von der Größe eines Unternehmens abhängig, sondern auch vom Geschäftszweck. Je nach Branche ergeben sich äußere Zwänge durch besondere gesetzliche Anforderungen für das Unternehmen. Diese müssen in einer Enterprise-Architektur berücksichtigt sein. Dies ist umso komplizierter, wenn Ihr Unternehmen in mehreren Ländern (Rechtsräumen) aktiv ist. Der Enterprise-Architekt kann nicht alle rechtlichen Anforderungen kennen. Daher ist es notwendig, in einem engen Dialog mit der Rechtsabteilung des Unternehmens oder einer externen Rechtsberatung zu stehen.

Eine besondere Herausforderung stellt sich Ihnen, wenn Sie in eine über die Jahre organisch gewachsene IT-Infrastruktur Ordnung hineinbringen möchten. In einer solchen Umgebung ist es oftmals notwendig, vorhandene Komponenten zurückzubauen, bevor man mit der Implementierung einer abgestimmten und durchdachten IT-Plattform beginnen kann.

Um eine IT-Plattform zu entwickeln, müssen Sie zuerst die Komponenten, die Hauptbausteine der neuen Plattform identifizieren und ihre Bedeutung innerhalb der Plattform gewichten. Welche der folgenden Komponenten sich in Ihrer Enterprise-Architektur wiederfinden, hängt ganz von der Größe und den Bedürfnissen Ihres Unternehmens und der IT-Infrastruktur ab.

Die relevanten Aspekte und Fragestellungen, die Sie betrachten müssen, finden Sie hier kurz aufgelistet. Im Anschluss daran schauen wir uns die einzelnen Punkte noch einmal detaillierter an.

► **Vision einer Plattform**

Die Vision einer IT-Plattform setzt sich das Ziel, eine umfassende IT-Infrastruktur zu entwickeln, die verschiedene Anwendungen und Dienstleistungen miteinander verbindet. Diese Plattform soll gewährleisten, dass alle IT-Elemente harmonisch zusammenwirken, um die geschäftlichen Ziele wirksam zu fördern. Sie bietet zudem eine flexible und skalierbare Umgebung, die in der Lage ist, sich an zukünftige Bedürfnisse anzupassen.

► **Umzug oder Transformation?**

Der Unterschied zwischen der Transformation und dem Umzug einer IT-Plattform besteht hauptsächlich im Umfang und in der Komplexität. Bei einer Transformation werden Daten und Anwendungen auf ein neues System übertragen, häufig mit Änderungen oder Upgrades. Ein Umzug hingegen bezeichnet die physische Verlagerung der IT-Plattform von einem Standort zu einem anderen, ohne signifikante Änderungen an Software oder Daten vorzunehmen.

► **On-Premises**

In der IT bezieht sich On-Premises darauf, dass die IT-Infrastruktur und Software innerhalb des Unternehmens selbst betrieben wird. Das Unternehmen trägt die Verantwortung für Verwaltung, Wartung und Sicherheit der Systeme. Im Gegensatz dazu werden bei Cloud-Lösungen diese Dienste von externen Anbietern über das Internet bereitgestellt.

► **Cloud-Dienste**

Cloud-Dienste sind IT-Ressourcen, die über das Internet zur Verfügung gestellt werden und nicht lokal auf Firmencomputern oder -servern gespeichert sind – wir gehen in Kapitel 13 ausführlicher darauf ein. Diese Dienste umfassen Speicherplatz, Rechenleistung, Software und andere IT-Ressourcen, die flexibel und skalierbar sind. Nutzer zahlen in der Regel nur für die tatsächlich genutzten Ressourcen, was sowohl die Kosten als auch den Verwaltungsaufwand reduziert.

► **Geschäftsanwendungen**

Geschäftsanwendungen sind Softwarelösungen, die gezielt dafür konzipiert wurden, betriebliche Abläufe zu unterstützen und zu verbessern. Buchhaltung, Kun-

denverwaltung, Projektmanagement und vieles mehr werden so effizienter oder überhaupt erst vernünftig möglich. Diese Software kann entweder vor Ort installiert oder als Cloud-Service bereitgestellt werden.

► **Client-Plattform**

Eine Client-Plattform umfasst die Geräte und Software, die Nutzer direkt verwenden, wie Computer, Tablets und Smartphones. Über sie erfolgt der Zugriff auf Anwendungen und Daten, die auf Servern oder in der Cloud gespeichert sind. Eine gut verwaltete Client-Plattform gewährleistet effizientes und sicheres Arbeiten, sowohl am Unternehmensstandort als auch »von überall« für das mobile Arbeiten.

► **Server-Plattform**

Die Server-Plattform bildet den Kern der IT-Infrastruktur Ihres Unternehmens und beinhaltet zentrale Computersysteme und Software, die Unternehmensdaten speichern und Unternehmensanwendungen bereitstellen. Diese Server sind in der Regel leistungsfähige Computersysteme, die vielen Benutzern gleichzeitig Dienste anbieten können. Sie garantieren eine sichere Datenspeicherung und eine zuverlässige Ausführung von Anwendungen, sodass Benutzer jederzeit darauf zugreifen können.

► **Datensicherung**

Datensicherung bedeutet, geschäftskritische Daten regelmäßig zu kopieren und an einem sicheren Ort abzulegen, um im Falle eines Verlusts eine Wiederherstellung zu ermöglichen. Dies bietet Schutz vor Datenverlust durch Hardwaredefekte, Softwarestörungen oder Cyberangriffe. Eine effektive Datensicherung gewährleistet, dass ein Unternehmen seine Daten zügig wiederherstellen und den Geschäftsbetrieb zeitnah weiterführen kann.

► **Datenschutz**

Der Datenschutz für eine IT-Plattform stellt sicher, dass persönliche und sensible Informationen vor unbefugtem Zugriff und Missbrauch geschützt sind. Dies beinhaltet Maßnahmen wie Verschlüsselung, Zugangskontrollen, Mandantentrennung und regelmäßige Sicherheitsaudits. Das Ziel ist es, die Privatsphäre der Nutzer zu gewährleisten und gesetzlichen Vorgaben nachzukommen.

► **Notfallwiederherstellung**

Notfallwiederherstellung bedeutet, dass ein Unternehmen über Strategien und Prozeduren verfügt, um IT-Systeme und Daten nach einem schwerwiegenden Ausfall, einem Notfall oder einer Krise zügig wiederherzustellen. Dies schließt regelmäßige Datensicherungen, redundante Systeme sowie umfassende *Wiederherstellungspläne* (WHP) ein. Ziel ist es, den Geschäftsbetrieb rasch wieder aufzunehmen und Datenverluste auf ein Minimum zu reduzieren.

Neben der individuellen Einschätzung aus Unternehmenssicht spielen auch gesetzliche Anforderungen eine Rolle. Wenn Ihr Unternehmen zur kritischen Infrastruktur (KRITIS, [https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/kritis\\_node.html](https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/kritis_node.html)) oder einem regulierten Geschäftsfeld gehört, müssen Sie weitergehende Anforderungen an Ihrer Enterprise-Architektur berücksichtigen.

### Vollständigkeit der Komponenten

Ich habe die in diesem Kapitel betrachteten Bausteine einer Enterprise Architecture aus eigener Erfahrung ausgewählt. Sie haben daher keinen Anspruch auf eine 100%ige Vollständigkeit. Dies ist auch dem Umstand geschuldet, dass sich Themen in der IT stetig weiterentwickeln.

Die zu berücksichtigenden Komponenten sind von Unternehmen zu Unternehmen unterschiedlich.

Die Entwicklung einer Enterprise-Architektur für ein Unternehmen ist immer auch eine Spekulation auf die Zukunft. Man entwickelt auf Basis des Vorhandenen eine Vision einer Zielumgebung für die nächsten fünf Jahre und darüber hinaus. Der Planungshorizont für die zwei bis drei Jahre ist granularer als für die fernere Zukunft.

Lassen Sie uns einen detaillierteren Blick auf die einzelnen Komponenten einer Enterprise-Architektur werfen. Zunächst geht es allerdings noch um grundsätzlichere Fragen.

### Vision der Plattform

Die Entwicklung einer klaren Vision für die IT-Enterprise-Architektur eines Unternehmens ist entscheidend, um eine langfristige Ausrichtung und erfolgreiche Umsetzung sicherzustellen – wie Ihre Architektur aufgebaut ist, hängt selbstverständlich davon ab, was die Ziele Ihres Unternehmens sind.

Eine klar formulierte Plattform-Vision ist die gemeinsame Ausgangsbasis für alle Beteiligten im Unternehmen. Durch die Definition der strategischen Ziele und des gewünschten Endzustands können alle Teams und Abteilungen besser verstehen, wie ihre Arbeit zur Mission ihres Unternehmens beiträgt.

Die Definition einer Vision ist zudem für eine effektive Ressourcenallokation notwendig. Sie ermöglicht es, Prioritäten festzulegen, und hilft dabei, Investitionen in Technologien, Schulungen und Infrastruktur auf das zu fokussieren, was die strategischen Ziele am besten unterstützt. Das optimiert die Kosten und sorgt dafür, dass Investitionen schneller Früchte tragen.

Die Entwicklung einer Vision für die IT-Enterprise-Architektur fördert auch die Innovationskraft des Unternehmens. Durch die Festlegung klarer Ziele und Standards

werden Mitarbeiter dazu ermutigt, kreative Lösungen zu entwickeln, um diese Vision zu verwirklichen. Eine klare Ausrichtung auf gemeinsame Ziele fördert die Zusammenarbeit und den Wissensaustausch, was wiederum die Agilität und Anpassungsfähigkeit des Unternehmens erhöht.

Mit einer Vision für die Enterprise-Architektur stellen Sie den Leitfaden für Entscheidungsprozesse zur Verfügung. Wenn unerwartete Herausforderungen auftreten oder neue Chancen entstehen, können Sie und andere Entscheidungsträger auf die definierten Ziele zurückgreifen. Das ist die Basis für eine konsistente Ausrichtung der IT und verhindert, dass Sie von kurzfristigen Entwicklungen abgelenkt werden.

Eine Vision hat die weitsichtige Ausrichtung der IT im Blick. Sie entwerfen die Plattform-Vision für einen Planungshorizont von fünf bis acht Jahren.

### **Migration oder Transformation**

Am Anfang steht die Frage, ob eine bestehende IT-Infrastruktur nur umziehen soll oder vollständig transformiert werden soll. Ein einfacher Umzug kann dazu führen, dass bestimmte ineffiziente Strukturen und Prozesse beibehalten werden, während eine Transformation die Chance bietet, veraltete Systeme zu optimieren und moderne Technologien zu integrieren. (Das ist besonders wichtig, wenn sich die Architektur grundlegend ändert, beispielsweise beim Umzug in die Cloud. Schauen Sie sich dazu auch Abschnitt 13.4 an.)

Ein weiterer wichtiger Aspekt ist die Kosten-Nutzen-Analyse. Die Wahl zwischen Umzug und Transformation hat direkte Auswirkungen auf die finanzielle Investition und die langfristigen Betriebskosten. Eine umfassende Transformation erfordert höhere anfängliche Investitionen, bietet jedoch oft langfristige Kosteneinsparungen und verbesserte Effizienz im Betrieb. Umzug und Transformation haben ähnliche Anforderungen hinsichtlich der zur Umsetzung erforderlichen Mitarbeitenden.

Die Frage, wie skalierbar und flexibel Ihre IT sein muss, ist ein weiterer wichtiger Faktor. Bei einer Transformation können Systeme besser an zukünftige Anforderungen angepasst werden und flexibler auf sich ändernde Geschäftsanforderungen reagieren. Ein einfacher Umzug schränkt diese Flexibilität ein und wird zu einem späteren Zeitpunkt erneute Anpassungen erforderlich machen – getreu dem Motto: Wer billig kauft, kauft zweimal.

Die Sicherheit der IT-Systeme gilt es ebenso zu berücksichtigen. Bei einer Transformation haben Sie die Möglichkeit, veraltete Sicherheitsstandards hinter sich zu lassen und modernste Sicherheitsprotokolle zu implementieren. Ein einfacher Umzug wird bestehende Sicherheitsrisiken beibehalten, wenn diese nicht gezielt, sofern möglich, angepasst werden.

### 5.1.2 On-Premises

Die lokale (On-Premises-)Infrastruktur spielt eine zentrale Rolle in der IT-Enterprise-Architektur Ihres Unternehmens. Sie ermöglicht eine direkte Kontrolle über die Hardware und Netzwerkkomponenten, was eine präzise Anpassung an die spezifischen Anforderungen Ihres Unternehmens erlaubt. Diese Kontrolle ist besonders wichtig, wenn Sie spezielle Compliance-Anforderungen oder Sicherheitsrichtlinien einhalten müssen. Nur so können Sie die Sicherheit der Daten und Anwendungen gewährleisten. Zu dieser Kontrolle gehört insbesondere auch die Zugangs- und Zutrittskontrolle zu den Räumlichkeiten, wie z. B. Serverraum oder ein ganzes Rechenzentrum.

#### On-Premises oder On-Premise?

Die korrekte englische Bezeichnung für die lokale IT-Infrastruktur ist »On-Premises«. Dies ist die einzige korrekte Schreibweise. Alle anderen Varianten haben in der englischen Sprache völlig andere Bedeutungen.

Die lokale Infrastruktur bietet (meistens) eine höhere Leistung und Bandbreite im Vergleich zu Cloud-basierten Lösungen. Dies ist entscheidend für Unternehmen mit ressourcenintensiven Anwendungen, die eine schnelle und zuverlässige Leistung erfordern. Durch den Betrieb von Servern und Netzwerken vor Ort können Unternehmen ihre Workloads optimal steuern und die Reaktionszeiten der Applikationen verbessern. Nicht alle Applikationen, auch moderne, unterstützen zuverlässig die Nutzung von in der Cloud gespeicherten Dateien.

Dies mag auf den ersten Blick wie ein Widerspruch zu den Vorteilen von Cloud-Diensten wirken. Die große Herausforderung ist, dass es nicht die eine allgemeingültige Antwort auf die Frage gibt, ob On-Premises- oder aber Cloud-Komponenten größere Vorteile für ein Unternehmen bieten. Es kommt immer auf die individuellen Anforderungen und den Funktionsumfang der in Ihrem Unternehmen genutzten Applikationen an. Wir dürfen an diesem Punkt nicht vergessen, dass es hier um die Bedeutung der On-Premises-Infrastruktur innerhalb der IT-Strategie geht. Und hier spielt sie eine besondere Rolle, je nach den Sicherheitsanforderungen Ihres Unternehmens. Nicht ohne Grund betreiben viele Unternehmen eine hybride IT-Infrastruktur. Applikationen mit besonderen technischen Anforderungen werden in der lokalen Infrastruktur betrieben, während gute skalierbare Webanwendungen direkt in der Cloud bereitgestellt werden.

Eine weitere Rolle spielt die lokale Infrastruktur im Hinblick auf die vollständige Integration bestehender IT-Systeme. Wenn Ihr Unternehmen über umfangreiche und komplexe lokale Infrastrukturen verfügen, können Sie diese weiter nutzen und (meist) nahtlos in Ihre IT-Strategie integrieren. Dies erleichtert den Übergang zu neuen Technologien und minimiert mögliche Unterbrechungen im laufenden Be-

trieb. Schließlich beginnen die wenigsten Unternehmen mit dem Aufbau einer gänzlich neuen IT-Infrastruktur. Dies ist nur bei neu gegründeten Unternehmen der Fall.

Der Betrieb einer lokalen IT-Infrastruktur bietet eine gewisse Unabhängigkeit von der Verfügbarkeit von Internetverbindungen. In Situationen, in denen eine zuverlässige Internetverbindung am Standort Ihres Unternehmens oder einer Niederlassung nicht gewährleistet ist, können lokale Systeme weiter betrieben werden, um erforderliche Dienste für den Geschäftsbetrieb und Produktionsstätten bereitzustellen.

Dies ist besonders wichtig für Unternehmen, die in abgelegenen Regionen tätig sind, oder in Bereichen, in denen eine Internetverfügbarkeit schlachtweg nicht zuverlässig ist. In solchen Regionen stellt die Nutzung von Cloud-Diensten ein besonderes Unternehmensrisiko dar. In vielen Fällen sind Unternehmen darauf angewiesen, eine lokale IT-Infrastruktur mit Anbindungen an einen oder mehrere Cloud-Anbieter im Hybrid-Betrieb zu betreiben. Die Ausprägung und Verteilung der IT-Komponenten müssen hierbei nicht nur einer technischen und finanziellen Bewertung, sondern auch einer sicherheitstechnischen Betrachtung folgen.

### 5.1.3 Cloud-Dienste

Die Cloud-Dienste bieten einen wichtigen Vorteil für die IT-Unternehmensarchitektur: flexible Skalierbarkeit.

Cloud-Plattformen ermöglichen es Unternehmen, die benötigten Applikationsressourcen nach Bedarf zu erhöhen oder zu verringern, was zu einer optimierten Nutzung und damit zu einer besseren Kostenkontrolle führt. Diese Skalierbarkeit ist besonders wichtig für Unternehmen, die auf saisonale Schwankungen oder unvorhersehbare Lastspitzen, z. B. bei Bestellungen, Buchungen oder in der Produktion, reagieren müssen.

Ein weiterer Vorteil ist die bessere Verfügbarkeit und Zuverlässigkeit von Anwendungen. Cloud-Dienste bieten in der Regel *georedundante Infrastrukturen* durch eine weltweite Verteilung von Rechenzentren, was Ausfallzeiten minimiert und eine höhere Verfügbarkeit gewährleistet. Dies ist besonders wichtig für Ihre geschäftskritischen Anwendungen, die rund um die Uhr verfügbar sein müssen, um den reibungslosen Betrieb Ihres Unternehmens zu gewährleisten. Die Angebote der Cloud-Dienstleister sind, insbesondere im Hinblick für die Verfügbarkeiten und abgesicherten Ausfallszenarien, sehr unterschiedlich. Manche bieten nur eine Redundanz der Systeme, andere wiederum eine mehrfach georedundante Verfügbarkeit, um unterschiedlichen Ausfallszenarien begegnen zu können. Dies spiegelt sich meist im Preis wider. Dafür kann eine *Multi-Cloud-Anbindung* aufgebaut werden, um die Vorteile mehrerer Cloud-Anbieter nutzen zu können.

Sicherheitsaspekte sind ebenfalls von großer Bedeutung. Cloud-Dienste bieten moderne Sicherheitsmaßnahmen, wie z. B. Verschlüsselung, Zugriffskontrolle und Überwachung, die in einer lokalen IT-Infrastruktur nur mit sehr großem Aufwand umzusetzen sind. Durch die Nutzung marktführender Cloud-Anbieter kann Ihr Unternehmen von deren Fachkenntnissen im Bereich Sicherheit profitieren, was zu einer insgesamt verbesserten Datensicherheit während des Datenzugriffs und der *Data-at-Rest*-Datenablage führt.

Die Agilität und Innovationsfähigkeit Ihres Unternehmens werden durch Cloud-Dienste gesteigert. Dies mag sich für Sie wie Buzzwords anhören, es sind aber keine. Es kommt jedoch, wie immer, darauf an, wie Sie »die Cloud« nutzen. Nicht jede Applikation ist in der Lage, die Vorteile der Cloud automatisch nutzen zu können. Meist ist dies nur nach dem Wechsel zu einer neuen Applikation oder nach der Neuentwicklung einer individuellen Lösung möglich. Darauf gehen wir genauer in Abschnitt 13.4 ein.

Durch die Bereitstellung von Entwicklungs- und Testumgebungen in der Cloud kann Ihr Unternehmen schneller neue Anwendungen entwickeln und nutzen. Die Cloud ermöglicht es auch, Ressourcen für Forschung und Entwicklung effizienter einzusetzen, da sie schnell und bedarfsgerecht zugänglich sind. Dies lässt sich im ersten Moment wie eine Sammlung von Marketingaussagen, jedoch haben die Erfahrungen der letzten Jahre genau dies belegt. Gerade für die Entwicklung von Applikationen und auch den Test von kommerziellen Applikationen möchte ich Ihnen die Nutzung von separaten Cloud-Umgebungen ans Herz legen. In Ihrer produktiven Cloud-Umgebung sind all Ihre sensiblen Unternehmensdaten gespeichert.

Eine Cloud-Nutzung bietet eine verbesserte und sichere Zusammenarbeit und Mobilität für Mitarbeiter. Die Möglichkeit, von überall aus sicher auf Unternehmensanwendungen und -daten zuzugreifen, ermöglicht die Arbeit von verteilten Teams und fördert so die Flexibilität der Mitarbeiter. Dies trägt zu einer modernen und flexiblen Arbeitsumgebung bei, was besonders in Zeiten von Remote-Arbeit und global verteilten Teams wichtig ist. Auch im Hinblick für die Rekrutierung neuer Arbeitskräfte für Ihr Unternehmen ist dies wichtig. Interessante Kandidaten wenden sich eher innovativen Arbeitgebern zu.

### 5.1.4 Applikationen

Die Planung und Auswahl der Unternehmens- und Office-Anwendungen ist von entscheidender Bedeutung für die IT-Enterprise-Architektur Ihres Unternehmens. Damit Sie fundierte Entscheidungen zur Applikationsauswahl treffen können, ist eine umfassende Analyse der geschäftlichen Anforderungen im Dialog mit den Abteilungen notwendig.

Zu einer Bedarfsanalyse (siehe Kapitel 11, »Requirements Engineering«) gehört die Identifizierung der Abteilungen, deren spezifischen Bedürfnisse sowie die Einbindung der Mitarbeitenden in den Prozess. Nur so können Sie sicherstellen, dass die gewählten Anwendungen die Arbeitsabläufe unterstützen. Diese Aufgabe wird von IT-Abteilungen nur sehr ungern durchgeführt, da man hierzu den direkten Dialog mit den Fachabteilungen suchen muss. Sie können hierbei auch auf externe Beratung zurückgreifen, was jedoch Unglück und Segen zugleich ist. Einerseits kommunizieren die Mitarbeitenden der Fachabteilungen mit Externen vorurteilsfrei, und es gibt weniger Kommunikationshürden als gegenüber Mitarbeitenden der IT. Andererseits können (dürfen) vielleicht nicht alle unternehmerischen Details mit Externen besprochen werden.

Die Planung muss auch zukünftige Entwicklungen und technologische Trends berücksichtigen, um eine langfristige Skalierbarkeit und Flexibilität der IT-Infrastruktur und der genutzten Applikationen zu gewährleisten. Dies ist immer nur nach bestem Wissen und Gewissen möglich. Denn Sie können nicht voraussehen, ob der Hersteller eines ausgewählten Produkts im nächsten Jahr übernommen und das von Ihnen gewählte Produkt vom Markt genommen wird.

Die Integration verschiedener Unternehmensanwendungen ist eine der zentralen Anforderungen an die IT-Abteilung. Die nahtlose Kommunikation zwischen den verschiedenen Systemen ist notwendig, um einen sicheren Datenaustausch zu gewährleisten. Die Verwendung standardisierter Schnittstellen und Protokolle ist die Voraussetzung, um die Interoperabilität der Applikationen zu gewährleisten und den Aufwand für Anpassungen zu minimieren. Versuchen Sie, soweit möglich, proprietäre Protokolle und Schnittstellen zu meiden.

Von individuellen Einzellösungen sollten Sie (fast immer) absehen, denn die Nutzung von standardisierten Applikationen sorgt für eine konsistente Benutzererfahrung und vereinfacht die Verwaltung, Schulung und Wartung (siehe Abschnitt 6.5). Individuelle Softwarelösungen erfordern separate Schulungen und verursachen höhere Kosten für Lizenzierung, Implementierung und Wartung. Durch die Konsolidierung auf eine integrierte Applikationsplattform können Sie nicht nur Ihre betriebliche Effizienz steigern, sondern auch die Gesamtbetriebskosten z. B. durch automatische Softwareverteilung oder geringeres Helpdesk-Aufkommen reduzieren.

### 5.1.5 Client-Plattform

Eine gut geplante und eingeführte Client-Plattform ermöglicht eine einheitliche Benutzererfahrung. Die Standardisierung von Client-Systemen, Betriebssystemen und Endgeräten stellt sicher, dass Mitarbeiter in Ihrem Unternehmen konsistente und

nahtlose Arbeitsumgebungen nutzen. Dies fördert die Akzeptanz des »Arbeitswerkzeugs« und trägt so zur Produktivität der Mitarbeitenden bei. Zusätzlich sorgt eine standardisierte Client-Plattform durch vereinfachte Support- und Wartungsprozesse für eine Kostenoptimierung im IT-Betrieb.

Gleichermaßen gilt für die Implementierung von Sicherheitsrichtlinien. Durch die Vereinheitlichung können Ihre IT-Teams zentral Sicherheitspatches, -updates und Richtlinien ausrollen, um Sicherheits- und Betriebsrisiken zu reduzieren. Dies ist besonders relevant, da Unternehmen immer öfter Cyberangriffen ausgesetzt sind und ein umfassender Schutz der Client-Systeme notwendig ist, um Datenintegrität und Vertraulichkeit zu sichern. Hierbei spielt auch die Reaktionsgeschwindigkeit in einem Sicherheitsfall eine wichtige Rolle, für die die Standardisierung einen klaren Vorteil bietet.

Eine standardisierte Client-Plattform bietet eine effiziente Ressourcennutzung. Durch die Standardisierung können Sie in Ihrem Unternehmen ihre IT-Ressourcen für die Einrichtung und den Betrieb der Komponenten optimieren, da Support und Wartung vereinfacht werden. Dies führt zu geringeren Gesamtbetriebskosten und ermöglicht Ihnen, Ressourcen effektiver zu allozieren. So können Sie z. B. ein neues Laptop-Gerät direkt vom Hersteller oder Distributor an neue Mitarbeitende senden lassen. Die unternehmensspezifische Einrichtung des Geräts erfolgt vollautomatisch. Der Zwischenschritt einer vorgelagerten manuellen Provisionierung durch Ihr IT-Team entfällt, ganz abgesehen vom zusätzlichen Aufwand für den doppelten Versand eines Geräts.

### 5.1.6 Datensicherung

Die Datensicherung gehört ebenso zur IT-Enterprise-Architektur eines Unternehmens, unabhängig von dessen Größe. Die regelmäßige Sicherung von Daten gewährleistet die Widerstandsfähigkeit der IT-Plattform gegenüber unvorhergesehenen Ereignissen wie Hardwareausfällen, Softwarefehlern oder menschlichen Fehlern. Durch den Verlust von Daten könnten kritische Geschäftsinformationen dauerhaft verschwinden, was erhebliche finanzielle und operationale Auswirkungen haben kann.

Eine weitere wichtige Funktion der Datensicherung ist die Einhaltung von rechtlichen und datenschutzrechtlichen Vorgaben. Unternehmen müssen oft Daten für eine bestimmte Dauer speichern, um gesetzliche Auflagen zu erfüllen. Eine wirksame Datensicherungsstrategie hilft dabei, diesen Anforderungen gerecht zu werden, und bewahrt Ihr Unternehmen vor rechtlichen Folgen.

Durch eine verlässliche Datensicherung können Sie gewährleisten, dass Sie im Falle einer Störung oder eines Cyberangriffs rasch wieder an Ihre wichtigen Daten gelangen können. Dies verringert Ausfallzeiten und unterstützt den Geschäftsbetrieb. Eine

Datensicherung dient somit der Verringerung von Risiken für den Geschäftsbetrieb. Sie ist ein wichtiger Teil der IT-Sicherheitsstrategie und des Business-Continuity-Managements.

### 5.1.7 Datenschutz

Der Datenschutz spielt in der IT-Enterprise-Architektur eine zentrale Rolle, um die Sicherheit, Vertraulichkeit und Verfügbarkeit von sensiblen Daten zu gewährleisten. Zum einen ist Datenschutz erforderlich, um rechtliche Vorgaben für Verarbeitung und Speicherung von Unternehmensdaten zu erfüllen. Ergänzend haben Länder strenge Datenschutzregeln, die von Unternehmen verlangen, dass sie die persönlichen Daten ihrer Kunden und Mitarbeitenden schützen. Dies kann u. U. auch die Einschränkung beinhalten, dass solche Daten nur im jeweiligen Land, z. B. China, verarbeitet werden dürfen. Solche rechtlichen Anforderungen haben unmittelbar Einfluss auf die von Ihnen zu planende IT-Architektur. Die Missachtung solcher Regeln kann zu schwerwiegenden rechtlichen Folgen für das Unternehmen führen.

Zum anderen ist Datenschutz ein wichtiger Faktor für das Risikomanagement. Unternehmen sind immer häufiger mit Cyberattacken, Datenpannen und anderen Sicherheitsrisiken konfrontiert. Durch die nahtlose Integration von Datenschutzmaßnahmen in die IT-Enterprise-Architektur können mögliche Gefahren erkannt, bewertet und wirksam reduziert werden. Dies hilft, die finanziellen Schäden und den potenziellen Vertrauensverlust zu begrenzen.

Datenschutz spielt ebenso eine zentrale Rolle für das Vertrauen in Ihr Unternehmen. Kunden und Stakeholder wollen, dass ihre persönlichen Daten sicher und vertraulich behandelt werden. Eine solide Datenschutzarchitektur fördert das Vertrauen der Beteiligten und erhöht die Kundenloyalität. Unternehmen, die Datenschutz ernst nehmen, können sich von Konkurrenten abheben und so als verantwortungsvolles Unternehmen angesehen werden.

Datenschutz verbessert auch die Nutzung und Qualität der Daten. Durch die Festlegung von klaren Datenschutzrichtlinien und -verfahren sorgen Sie dafür, dass Daten nur gemäß den geltenden Datenschutzvorschriften verarbeitet und gespeichert werden.

Schließlich erlaubt eine sorgfältige Integration von Datenschutz in die IT-Enterprise-Architektur eine bessere Anpassung an sich stetig weiterentwickelnde Datenschutzbedingungen. Durch die Abstimmung der Architektur auf neue Gesetze und Technologien können Unternehmen flexibel und proaktiv auf Veränderungen in der Datenschutzlandschaft reagieren. Dies gewährleistet nicht nur den aktuellen Compliance-Status, sondern auch eine langfristige Anpassungsfähigkeit und Zukunftsfähigkeit der IT-Infrastruktur. Dies ist, wie schon zuvor erwähnt, gerade für global agierende Unternehmen wichtig.

### 5.1.8 Notfallwiederherstellung

Die Notfallwiederherstellung (auch als *Disaster Recovery* bekannt) ist ein wesentlicher Bestandteil der IT-Enterprise-Architektur, da sie gewährleistet, dass ein Unternehmen wichtige Geschäftsprozesse auch nach unvorhersehbaren Zwischenfällen zeitnah fortsetzen kann.

- ▶ Erstens verhindert die Notfallwiederherstellung einen Datenverlust. Durch regelmäßige Sicherungen und Wiederherstellungsverfahren werden wesentliche Unternehmensdaten geschützt, was die Geschäftskontinuität bei Hardwareproblemen, Cyberangriffen oder Naturkatastrophen sicherstellt.
- ▶ Zweitens sorgt die Notfallwiederherstellung für eine geringe Ausfallzeit. Unternehmen können ihre Services und Anwendungen schnell wieder in Betrieb nehmen, was die Leistungsfähigkeit und den Kundenservice erhält. Dies hilft, finanzielle Schäden und eine mögliche Rufschädigung zu vermeiden.
- ▶ Drittens unterstützt die Notfallwiederherstellung die Einhaltung von branchenspezifischen Regeln und Gesetzen. Einige Branchen verlangen eine solide Disaster-Recovery-Strategie, um gesetzlichen Vorgaben nachzukommen.

Ein weiterer Vorteil der Notfallwiederherstellung ist die Risikominderung. Ihr Unternehmen kann sich vor den finanziellen Verlusten und betrieblichen Gefahren schützen, die durch Unterbrechungen der Geschäftsabläufe entstehen können.

Außerdem fördert eine wirkungsvolle Notfallwiederherstellung die Resilienz der IT-Enterprise-Architektur. Die Fähigkeit, nach Notfällen wieder rasch in den Regelbetrieb zu kommen, erhöht die Widerstandsfähigkeit des Unternehmens gegenüber verschiedenen Bedrohungen, ob technischer, menschlicher oder externer Natur. Insgesamt hilft die Notfallwiederherstellung dabei, die langfristige Stabilität und Wettbewerbsfähigkeit Ihres Unternehmens zu gewährleisten.

Diese Aspekte sind so wichtig, dass Sie ihnen besondere Aufmerksamkeit schenken sollten. Ihre IT-Architektur muss so aufgebaut sein, dass sie nicht nur bei schönem Wetter funktioniert. Was passiert, wenn es zu Störungen, Ausfällen oder Notsituationen kommt?

Diese Frage wird im Rahmen des *Business-Continuity-Managements* behandelt, das besonders dann wichtig wird, wenn Sie für kritische Infrastrukturen verantwortlich sind. Aber auch sonst: Kein Unternehmen kann es sich heutzutage mehr leisten, wenn die IT längere Zeit ausfällt. Grund genug, sich in Abschnitt 5.3 besonders mit diesem Thema zu befassen.

### 5.1.9 Schatten-IT

Wenn Sie neu in der Rolle des IT-Managers sind, werden Sie rasch feststellen, dass nicht alle IT-Systeme und Anwendungen, die im Unternehmen genutzt werden, auch

offiziell durch Ihre Abteilung betreut oder genehmigt sind. Diese inoffiziellen Lösungen werden unter dem Begriff *Schatten-IT* zusammengefasst. Gemeint sind damit alle Technologien – von Cloud-Diensten über mobile Apps bis hin zu selbst beschaffter Hardware –, die von Fachabteilungen oder einzelnen Mitarbeitenden ohne Einbindung der IT-Abteilung genutzt werden.

Diese Schatten-IT entsteht häufig aus einem nachvollziehbaren Wunsch der Mitarbeitenden nach Effizienz und Flexibilität. Wenn zentrale IT-Prozesse als zu langsam, unflexibel oder unpassend empfunden werden, greifen Mitarbeitende zu eigenen Lösungen, um ihre Aufgaben schneller oder komfortabler zu erledigen. Was auf den ersten Blick pragmatisch erscheint, birgt jedoch erhebliche Risiken, insbesondere im Kontext einer zu entwickelnden *Enterprise-Architektur*.

Eine Enterprise-Architektur verfolgt ja das Ziel, die IT-Landschaft Ihres Unternehmens strategisch, konsistent und zukunftssicher zu gestalten. Schatten-IT steht diesem Anspruch diametral entgegen. Sie entzieht sich der zentralen Steuerung, unterläuft Sicherheits- und Compliance-Vorgaben und erschwert die Integration neuer Systeme. Zudem führt sie zu Dateninseln, Redundanzen und erhöhten Betriebskosten.

Für Sie als IT-Manager bedeutet das: Jede nicht abgestimmte Lösung kann (und wird) die Stabilität und Skalierbarkeit Ihrer Architektur gefährden.

Um dem entgegenzuwirken, müssen Sie frühzeitig für Transparenz sorgen. Suchen Sie *aktiv* den Dialog mit den Fachbereichen, um deren Bedürfnisse zu verstehen und gemeinsam tragfähige Lösungen zu entwickeln. Eine moderne Enterprise-Architektur sollte nicht nur technische Standards definieren, sondern auch Raum für Innovation und Flexibilität lassen, jedoch innerhalb klarer Governance-Strukturen. Etablieren Sie Richtlinien, die die Einführung neuer Tools regeln, ohne den Handlungsspielraum der Fachabteilungen unnötig einzuschränken.

Letztlich ist Schatten-IT kein Zeichen von Ungehorsam, sondern ein Indikator dafür, dass Ihre IT-Strategie nicht alle Anforderungen abdeckt. Wenn Sie es schaffen, diese Signale konstruktiv zu nutzen und in Ihre Architekturplanung zu integrieren, legen Sie den Grundstein für eine IT-Landschaft, die sowohl sicher als auch anpassungsfähig ist.

## 5.2 Rollen und Aufgaben

Die Aufgabe, die ganze IT-Architektur eines Unternehmens zu planen, wird auf mehrere Schultern verteilt. Hauptverantwortlich ist der Enterprise-Architekt, der in der täglichen Arbeit von Lösungsarchitekten und technischen Architekten unterstützt wird. Aber wie immer gilt, dass die genauen Definitionen variieren. Einige Organisationen verwenden diese Begriffe synonym, und die Verantwortlichkeiten überschneiden sich. Klären Sie die spezifischen Anforderungen und Erwartungen, bevor Sie eine dieser Rollen übernehmen.

### 5.2.1 Enterprise-Architekt (EA)

Die Rolle des Enterprise-Architekten wird durch Mythen begleitet. Dies ist insbesondere dem Umstand geschuldet, dass es nicht die »eine« Beschreibung dieser Funktionsrolle innerhalb der IT gibt. Wie in so vielen Bereichen der IT lautet die Antwort: »Es kommt drauf an.«

Der Enterprise-Architekt konzentriert sich auf die Gesamtsicht und -struktur eines Unternehmens. Die Rolle ist verantwortlich für die Entwicklung und Verwaltung einer umfassenden IT-Strategie, die die Unternehmensziele und -anforderungen unterstützt. Ein Enterprise-Architekt arbeitet auf einer abstrakten Ebene und betrachtet die Zusammenhänge zwischen verschiedenen Systemen, Prozessen, Daten und Technologien im gesamten Unternehmen. Er stellt so sicher, dass die IT-Infrastruktur die geschäftlichen Ziele effektiv unterstützt. Diese Architekten entwickeln Richtlinien, Standards und die Roadmaps für die gesamte IT-Infrastruktur des Unternehmens und sorgen dafür, dass alle IT-Initiativen in Übereinstimmung mit diesen Leitlinien stehen. Idealerweise hat ein Unternehmen einen Enterprise-Architekten, der von einem Team von Lösungsarchitekten (*Solution Architect*) und technischen Architekten (*Technical Architect*) unterstützt wird.

Wenn Sie sich selbst in der Rolle als Enterprise-Architekt sehen oder wenn Sie diese Rolle für Ihr Unternehmen etablieren möchten, kommt es darauf an, Ihr Unternehmen und insbesondere die IT Ihres Unternehmens sehr gut zu kennen. Zur Rolle des Enterprise-Architekten gehören aus meiner Sicht folgende Kernkompetenzen:

- ▶ gute Kommunikationsfähigkeiten, um die Zusammenarbeit mit den IT-Teams und den aktiven Geschäftsbereichen durchzuführen und ausgewogen zu steuern
- ▶ gute Konfliktlösungsfähigkeiten, um die unterschiedlichen Interessen der IT-Teams in Einklang zu bringen und der Geschäftsführung gegenüber vertreten zu können
- ▶ Visionär sein. Ein Enterprise-Architekt muss langfristig vorausdenken können und kommende Technologien und Trends für das Unternehmen adaptieren. Ob man jedoch jeden Hype und jeden Trend mitmachen muss, schauen wir uns in Kapitel 16 an.
- ▶ Übersetzer technischer Themen, um einfache wie komplexe IT-Themen für die Entscheidungsebenen sorgsam und verständlich aufzubereiten
- ▶ offener und aktiver Umgang mit Fehlern und Fehlentscheidungen, um innerhalb der IT eine positive Fehlerkultur zu pflegen
- ▶ gesundes Selbstbewusstsein, um IT-Richtungsentscheidungen der IT vor C-Level-Gremien standhaft zu vertreten

- ▶ grundlegendes Wissen um die Basisarchitektur der vorhandenen IT-Lösungen
- ▶ idealerweise auch Kenntnisse der Herstellungsprozesse oder Produktionsumgebungen in einem Unternehmen

### **Standhaft in C-Level-Besprechungen**

Der Enterprise-Architekt ersetzt nicht den CIO. Jedoch wird man als Enterprise-Architekt gerne zu Besprechungen auf C-Level eingeladen, um technische Sachverhalte zu erklären und weitere entscheidungsrelevante Informationen darzubieten.

Ja, es kommt einer Darbietung auf einer Bühne gleich, bei der man gerne für Entscheidungsempfehlungen gegrillt wird. Hier müssen Sie als Enterprise-Architekt darauf achten, sich nicht zu einer Aussage wie »Das kann man auch anders lösen« hinreißen zu lassen.

Der Enterprise-Architekt muss nicht nur die technischen Möglichkeiten und Abhängigkeiten bewerten können, sondern auch ein Verständnis über die betrieblichen Anforderungen und Entwicklungswünsche des »Business« haben. Dieser Aufgabe kommt eine besondere Rolle innerhalb des Unternehmens zu, da Mitarbeiter der IT traditionell ein eher unterkühltes Kommunikationsverhältnis zu den Geschäftsbe reichen haben. Man versteckt sich gerne hinter technischen Lösungen, wie z. B. einem Ticketsystem, um den direkten Kontakt mit Endanwendern zu vermeiden.

In weltweit agierenden Unternehmen stellen sich für den Betrieb einer IT-Infrastruktur besondere Herausforderungen.

### **Kein Einzelkämpfer**

Die Rolle des Enterprise-Architekten ist nicht die Rolle eines Einzelkämpfers. Sie ist vielmehr die Speerspitze aller IT-Teams, um dem CIO und der Geschäftsführung gegenüber die abgestimmten Anforderungen der IT zu vertreten.

Es darf nicht vergessen werden, dass die IT in vielen Unternehmen als Kostentreiber und notwendiges und leider unvermeidbares Übel wahrgenommen wird. Dies ist oftmals der Grund, warum es keinen Enterprise-Architekten gibt oder warum die Rolle als zusätzliche Aufgabe mit einer anderen Rolle kombiniert wird. Dies führt automatisch zu Konflikten in den IT-Teams und zu einem unbefriedigenden Ergebnis.

Die Rolle des Enterprise-Architekten ist idealerweise eine dedizierte, einzeln zu besetzende Position innerhalb der IT-Organisationseinheit.

Der Enterprise-Architekt gibt verbindliche Entscheidungsempfehlungen für die IT des Unternehmens, die über den verantwortlichen CIO in die Geschäftsführung getragen werden.

### 5.2.2 Lösungsarchitekt (Solution Architect)

Ein Lösungsarchitekt ist für die Entwicklung umfassender Lösungen verantwortlich, die die geschäftlichen Anforderungen eines Unternehmens erfüllen. Diese Rolle beinhaltet in der Regel die Gestaltung von Systemen und Anwendungen auf einer höheren, ganzheitlichen Ebene. Der Lösungsarchitekt berücksichtigt dabei nicht nur technologische Aspekte, sondern auch geschäftliche Anforderungen, Budgets und andere nicht technische Faktoren. Lösungsarchitekten arbeiten oft eng mit den verschiedenen Stakeholdern zusammen, um sicherzustellen, dass die entwickelten Lösungen die Bedürfnisse des Unternehmens erfüllen.

Der Lösungsarchitekt fokussiert sich auf spezifische Projekte oder Lösungen innerhalb des Unternehmens. Diese Rolle ist dafür verantwortlich, sicherzustellen, dass die technische Umsetzung eines Projekts den Anforderungen und Standards des Unternehmens entspricht. Lösungsarchitekten entwerfen und dokumentieren detaillierte technische Pläne für einzelne Projekte und arbeiten eng mit den Entwicklungs- und Implementierungsteams zusammen, um sicherzustellen, dass die Lösung den Vorgaben entspricht.

Diese Architekten sind oft tiefer in technische Details involviert und konzentrieren sich darauf, wie verschiedene Systeme miteinander integriert werden können, um die gewünschte Lösung zu erreichen.

### 5.2.3 Technischer Architekt (Technical Architect)

Ein technischer Architekt hingegen konzentriert sich mehr auf die technische Seite der Architektur, insbesondere auf die Entwicklung von technischen Designs und Architekturen für einzelne Systeme oder Anwendungen. Diese Rolle beinhaltet oft eine tiefere technische Expertise in bestimmten Technologien, Plattformen oder Software-Stacks. Technische Architekten sind für die Auswahl von Technologien, das Erstellen von Design-Dokumenten und die Gewährleistung der technischen Integrität einer Lösung verantwortlich. Sie arbeiten eng mit den Entwicklerteams zusammen, um sicherzustellen, dass die technische Implementierung den Anforderungen entspricht.

In einem gewissen Sinn kann man sagen, dass der Lösungsarchitekt eher auf die Gesamtlösung und die Integration von verschiedenen Systemen abzielt, während der technische Architekt sich tiefer in die technischen Details einzelner Komponenten vertieft.

### 5.3 Business-Continuity-Management

Der Weiterbetrieb des Unternehmens im Falle einer Störung, unabhängig von deren Größe, ist kritisch für seinen Fortbestand. Die englische Bezeichnung *Business-Continuity-Management*, kurz BCM, begegnet vielen Unternehmen als Bestandteil einer ISO-Zertifizierung z. B. ISO 27001.

BCM ist ein wichtiger Managementprozess, um sicherzustellen, dass Ihr Unternehmen den normalen Geschäftsbetrieb während einer Unterbrechung, eines Notfalls oder einer Krise weitestgehend ungestört aufrechterhalten kann.

#### Störung oder Katastrophe

Aus Sicht der IT sind die Übergänge zwischen einer Störung und einer Katastrophe unscharf. Bei einer Katastrophe denken wir oftmals zuerst an ein katastrophales Naturereignis, was zu einer Störung des Geschäftsbetriebs führen kann. Eine technische Katastrophe kann z. B. eine Ransomware-Verbreitung in Ihrem Datenspeicher sein. Beides stellt keine einfache Störung mehr dar. Ebenso kann sich eine IT-Störung zu einer Katastrophe ausweiten.

Achten Sie bei der Identifikation der Risiken, denen Ihr Unternehmen begegnen muss, insbesondere auf regionale Besonderheiten. Hierzu gehören z. B. Erdbeben, Überflutung oder Feuer.

Solche Risiken zu betrachten und als Bestandteil einer Enterprise-Architektur zu berücksichtigen, wird aus IT-Sicht gerne vergessen.

Ein Beispiel für ein solches »Vergessen« ist der Serverraum eines Unternehmens in der Hamburger Hafen-City. Dort wurde der Serverraum unterhalb der möglichen Wasserlinie bei einer Sturmflut geplant und gebaut. Um die Anlieferung von Hardware zu erleichtern, wurde ein Zugang über ein Parkdeck ermöglicht, das sich ebenfalls unterhalb der Wasserlinie befindet.

BCM ist kein reines IT-Thema. Die IT spielt jedoch einen wichtigen Teil innerhalb des gesamten BCM-Prozesses. Die IT-Aspekte werden dabei vom IT-Service-Continuity-Management (ITSCM) abgedeckt. Hierbei werden organisatorische und technische Gegenmaßnahmen für theoretisch mögliche Schadensereignisse definiert.

Während sich organisatorischen Maßnahmen meist leicht umsetzen lassen, sieht es bei technischen Gegenmaßnahmen (der *IT-Notfallvorsorge*) schon deutlich anders aus, da diese immer mit Investitionen einhergehen. Neben den Risiken der Naturgewalten und IT-Störungen jeder Art müssen Sie auch Risiken durch menschliche Fehler betrachten. Fehlbedienungen in der IT oder in Produktionsanlagen können ebenfalls katastrophale Auswirkungen haben.

### 5.3.1 Richtlinien und Strategien

Bei der Entwicklung von Richtlinien und Strategien für das BCM geht es um mehr als nur um die Reaktion auf außergewöhnliche Ereignisse wie Naturkatastrophen oder Cyber-Angriffe. In den BCM-Richtlinien werden die notwendigen Überbrückungsmaßnahmen definiert und in festgeschriebene Handlungsmaßnahmen umgesetzt.

Für die Entwicklung der für Ihr Unternehmen passenden Strategie und die sich daraus ableitenden Richtlinien müssen Sie folgende Punkte definieren:

- ▶ Warum ist die sichere Fortführung des Betriebs (auch Notbetrieb) während eines außergewöhnlichen Ereignisses notwendig?
- ▶ Geht es darum, den Betrieb von Anwendungen, die Verfügbarkeit von Produkten und Diensten, den Zugriff auf Daten oder die Sicherheit von Standorten und Menschen zu gewährleisten? Für jedes Unternehmen stellt sich die Situation anders dar. Manche Unternehmen unterliegen rechtlichen Anforderungen, die einen Business-Continuity-Plan erfordern. Sie benötigen Klarheit über die Gründe zur Weiterführung des Betriebs in einer Ausnahmesituation.
- ▶ Wer ist für die Definition der Business-Continuity-Maßnahmen verantwortlich?
- ▶ Wer ist für den Test und die Umsetzung der definierten Maßnahmen zuständig?
- ▶ Wer kontrolliert die korrekte Umsetzung der Maßnahmen während und nach einem Ereignis?
- ▶ Welchen Umfang haben die notwendigen Maßnahmen?
- ▶ Wie und in welchem Zeitraum überprüfen Sie die Wirksamkeit der definierten Maßnahmen?
- ▶ Wie und in welchem Zeitraum erfolgt eine Anpassung der definierten Maßnahmen?

Der Kommunikation kommt im gesamten BCM-Prozess eine besondere Bedeutung zu. Unabhängig davon, wie umfangreich die BCM-Richtlinien in Ihrem Unternehmen ausfallen, müssen alle beteiligten Personen über den aktuellen Stand informiert sein, um im Fall der Fälle richtig reagieren zu können.

Die Definition dessen, was für die Fortführung des Geschäftszwecks erforderlich ist, ist ein Kernbestandteil für die Entwicklung einer belastbaren und sicheren Enterprise-Architektur.

### 5.3.2 Folgenabschätzung für das Unternehmen

Bei der Folgenabschätzung ermitteln Sie, welche Daten in Ihrem Unternehmen vorhanden sind, wo sie gespeichert sind, wie sie erfasst und verarbeitet werden und wie

auf diese Informationen zugegriffen wird. Bei der Katalogisierung bestimmen Sie, welche dieser Daten für Ihr Unternehmen am kritischsten sind. Ebenso definieren Sie, welche Ausfallzeiten akzeptabel sind, sollten diese Daten oder Anwendungen nicht verfügbar sein.

Viele Unternehmen streben zwar eine 100-prozentige Betriebszeit während eines außergewöhnlichen Ereignisses an. Dies ist jedoch nicht immer zu realisieren. Oftmals wird aus rein betriebswirtschaftlichen Gründen davon abgesehen, da der Erwerb und der Betrieb redundanter Systeme zu teuer sind. Daher müssen Sie bei der Betrachtung der Folgeabschätzung für Ihr Unternehmen errechnen, welches maximale zeitliche Ziel für die Wiederherstellung des Regelbetriebs notwendig und akzeptabel ist. Diese Zeit wird als *Wiederherstellungszeit (RTO, Recovery Time Objective)* bezeichnet.

Aus Sicht der Enterprise-Architektur bezieht sich dies nicht nur auf die Wiederherstellung einer Datensicherung, sondern auf alle Komponenten, die für einen funktionsfähigen Zustand der IT-Infrastruktur notwendig sind. Und dies beginnt mit der Wiederherstellung der Stromversorgung für den Betrieb, gefolgt vom Anfahren der ausgefallenen Systemkomponenten und dem Starten der erforderlichen Applikationen in der richtigen Reihenfolge.

Außerdem sollten Unternehmen das Ziel des Wiederherstellungspunkts kennen, d. h. das Alter der Daten, das für Kunden und Ihr Unternehmen akzeptabel ist, um den Betrieb wieder aufzunehmen. Man kann es auch als den Akzeptanzfaktor für Datenverluste bezeichnen. Sie müssen also wissen, welches Delta an Datenverlust im Fall eines katastrophalen Ereignisses akzeptabel ist und mit einem überschaubaren Aufwand, z. B. durch Neueingabe der Daten, erneut erfasst werden kann.

### 5.3.3 Risikoabschätzung (Risk Assessment)

Die Durchführung einer *Risikoabschätzung* ist alles andere als einfach. Führen Sie eine möglichst detaillierte Betrachtung der Auswirkungen durch Bedrohungen und Risiken auf Ihr Unternehmen durch. Je nach Unternehmensart und Geschäftsfeld ergeben sich ganz unterschiedliche Risiken, die Sie betrachten müssen:

- ▶ externe Personen, die als Dienstleister für Ihr Unternehmen tätig sind
- ▶ Mitarbeiter, die dem Unternehmen Schaden zufügen möchten
- ▶ Konkurrenzunternehmen
- ▶ Marktbedingungen
- ▶ politische Rahmenbedingungen im In- und Ausland
- ▶ Naturereignisse

Eine Risikobewertung umfasst potenzielle Risiken für Ihr Unternehmen, so unwahrscheinlich Sie Ihnen auch vorkommen mögen.

Die folgenden Punkte können eine Bedrohung für Ihr Unternehmen darstellen:

- ▶ Verlust an Personal
- ▶ Veränderung von Kundenvorlieben und -verhalten
- ▶ fehlende Reaktionen auf Sicherheitsvorfälle im Unternehmen
- ▶ fehlende finanzielle Flexibilität
- ▶ Nichteinhaltung von sich ändernden rechtlichen Vorschriften
- ▶ Verlust von Zertifizierungen oder Glaubwürdigkeit

Sie sehen, dass nicht alle Risiken und Bedrohungen für ein Unternehmen eindeutig greifbar sind, sondern sich oftmals in weichen Kriterien verstecken.

Alle theoretischen Risiken müssen auf ihre Eintrittswahrscheinlichkeit und ihre potentielle Auswirkung auf das Unternehmen geprüft werden. Die Wahrscheinlichkeit und die Auswirkung sind der Schlüssel für eine gute Risikobewertung. Dieser Schlüssel ist bei jedem Unternehmen anders ausgeprägt.

Nach der Identifikation und Kategorisierung der Risiken ist es entscheidend, die Risikotoleranz festzulegen. Sie müssen ermitteln, welche Probleme vorrangig behandelt werden sollten. Als Nächstes geht es um die Entwicklung, Evaluation und vor allem die Kostenabschätzung potenzieller Lösungen, da nicht alle Lösungsansätze finanziell tragbar sind. Auf Grundlage dieser Informationen legen Sie Prioritäten fest: Welche Risiken müssen unbedingt angegangen werden und welche kann das Unternehmen hinnehmen? Die erstellte Reihenfolge nach der Risikobewertung bestimmt, für welche Risiken als Erstes eine Lösung gefunden werden muss.

Die Risikobewertung ist kein statischer Prozess, der nur einmal durchlaufen werden muss. Planen Sie eine regelmäßige Wiederholung der Risikobewertung, insbesondere im Hinblick auf die erfolgreiche oder nicht erfolgreiche Durchführung umgesetzter Maßnahmen aus früheren Bewertungen. Wir können in diesem Handbuch keine eindeutige Empfehlung für ein Bewertungsintervall aussprechen. Jedoch sollte mindestens einmal jährlich ein Review der Risikobewertungen stattfinden.

#### 5.3.4 Validierung und Prüfung

Ein wesentlicher Bestandteil zur Sicherstellung des Geschäftsbetriebs bei einem Schadensereignis ist die regelmäßige Validierung und Prüfung der Auswirkungen und der Maßnahmen zur Begegnung eines Ereignisses. Die Durchführung von regelmäßigen Tests der Maßnahmen führt zu einem selbstverständlichen Handeln im Ernstfall. Es wäre fatal, sich erst dann mit den Maßnahmen vertraut zu machen.

Das Testen der Maßnahmen dient ebenso der Prüfung, ob die theoretisch geplanten Maßnahmen realistisch umgesetzt werden können und ob die Reihenfolge der einzelnen Schritte richtig und sinnvoll sind. Eine positive Fehlerkultur ist hier ausschlag-

gebend, um auch kleine Fehler sichtbar zu machen und so zu einer besseren Risiko-begegnung zu kommen.

Im Hinblick auf die IT bedeutet dies, dass Sie in regelmäßigen Abständen eine Notfall-wiederherstellung des gesamten IT-Betriebs testen müssen. Und dies beinhaltet nicht nur die möglichst erfolgreiche Wiederherstellung einer Datensicherung.

### 5.3.5 Identifizierung von Ereignissen

Eine klare und eindeutige Beschreibung, was ein besonderes Ereignis ist und was nicht, ist für das *Auslösen* der Business-Continuity-Maßnahmen unerlässlich. Wenn Sie unterschiedliche Varianten eines Ereignisses betrachten müssen, müssen diese Varianten auch schriftlich festgehalten sein. In einer Notsituation ist kein Raum für unterschiedliche Interpretationen.

Definieren Sie auch Aktionen für Ereignisse, die eine definierte Vorgehensweise erfordern, aber bisher nicht im Detail betrachtet wurden. Stellen Sie sich solch eine Definition als »Catch-All«-Regel vor.

Mit diesen Auslösern wissen Ihre Teams, wie sie zu reagieren haben.

Im IT-Management ist es entscheidend, den Unterschied zwischen Geschäftskontinuität (*Business Continuity*) und Notfallwiederherstellung (*Disaster Recovery*) zu verstehen.

- ▶ *Geschäftskontinuität* (oder *Business Continuity*) bezieht sich auf die Planung und Maßnahmen, die sicherstellen, dass wesentliche Geschäftsprozesse selbst bei Störungen weitergeführt werden können. Dazu gehören die Risikobewertung, die Entwicklung von Strategien zur Risikominderung und die Implementierung von Verfahren, die den Betrieb aufrechterhalten. Ziel ist es, Unterbrechungen zu minimieren und die Auswirkungen auf den Geschäftsbetrieb zu reduzieren. Regelmäßige Tests und Übungen sind notwendig, um sicherzustellen, dass alle Beteiligten auf verschiedene Szenarien vorbereitet sind.
- ▶ Die *Notfallwiederherstellung* zielt darauf ab, IT-Systeme und Daten nach größeren Störungen wiederherzustellen. Dabei steht die rasche Wiederherstellung der Funktionsfähigkeit im Vordergrund. Dies umfasst die Anlage und Wartung von Back-ups, das Erstellen von Wiederherstellungsplänen und das Durchführen von Tests zur Sicherstellung der Planwirksamkeit. Der Schwerpunkt liegt auf der Minimierung von Datenverlusten und der zügigen Wiederaufnahme des Betriebs. Notfallwiederherstellungspläne sind ein unerlässlicher Bestandteil des IT-Managements, um die Resilienz Ihres Unternehmens sicherzustellen.

Während die Gewährleistung der Geschäftskontinuität proaktive Maßnahmen erfordert, ist die Notfallwiederherstellung reaktiv und wird erst nach einem Vorfall eingeleitet. Beide Konzepte sind jedoch eng verknüpft und ergänzen sich gegenseitig.

Ein effektiver Plan zur Geschäftskontinuität sollte auch Aspekte der Notfallwiederherstellung beinhalten. Dies stellt sicher, dass ein Unternehmen sowohl auf kleinere Unterbrechungen als auch auf größere Krisen vorbereitet ist. Durch die Kombination dieser Ansätze kann ein Unternehmen seine Widerstandsfähigkeit gegenüber verschiedenen Bedrohungen erhöhen.

Für Neulinge im IT-Management ist es entscheidend, diese Unterschiede zu kennen und darauf basierend Strategien zu entwickeln. Die Sicherstellung der Geschäftskontinuität sowie die Notfallwiederherstellung sind zentrale Elemente eines effektiven Risikomanagements. Beide erfordern regelmäßige Überprüfung und Anpassung, um den aktuellen Anforderungen und Bedrohungen gerecht zu werden. Durch die Umsetzung dieser Maßnahmen können Unternehmen ihre Betriebsprozesse schützen und ihre langfristige Stabilität sichern. Ein sorgfältig ausgearbeiteter Plan in diesen Bereichen kann den Unterschied zwischen einer raschen Erholung und einem langwierigen Betriebsausfall bedeuten.

Die Sicherstellung des Geschäftsbetriebs beinhaltet also die organisationsweiten Pläne und Richtlinien, um das Unternehmen sicher zu führen. Eine Wiederherstellung im Krisenfall wiederum beinhaltet die Maßnahmen, die ausgeführt werden, wenn ein Zwischenfall eintritt.

Eine Notfallwiederherstellung besteht aus den spezifischen Reaktionen und ist auf den jeweiligen Vorfall bezogen. Diese Reaktionen basieren auf der Risikoermittlung und den ermittelten Maßnahmen zur Gefahrenabwehr.

Eine große Bedeutung kommt der Nachbesprechung (*Lessons Learned*) zu. Nach jedem Vorfall müssen Sie prüfen, ob die geplanten und durchgeführten Maßnahmen die Gefahr geeignet abgewehrt oder beseitigt haben. Sollte dies nicht der Fall sein, müssen die Maßnahmen überarbeitet werden.

### 5.3.6 Die Rolle der Kommunikation

Der Kommunikation kommt beim Management der Sicherstellung des Geschäftsbetriebs eine besondere Bedeutung zu. Man spricht nicht ohne Grund von einer *Krisenkommunikation*.

Diese Kommunikation muss von einem dedizierten Kommunikationsteam gesteuert und ausgeführt werden. Mit einer gut aufgestellten Krisenkommunikation stellen Sie sicher, dass die Kommunikation mit Kunden, Verbrauchern, Mitarbeitern, leitenden Angestellten, Medienvertretern und anderen Interessengruppen transparent und konsistent ist.

Es ist üblich, dass Mitarbeitern, die der Krisensituation aktiv ausgesetzt sind, jegliche Kommunikation mit externen Personen untersagt wird, um das Unternehmen vor negativen Auswirkungen zu schützen. Solch eine strikte Richtlinie muss Teil der de-

finierten BCM-Regeln sein. Eine konsistente Kommunikationsstrategie ist während und nach einem Vorfall unerlässlich.

Eine solch strikte Strategie hilft den unterschiedlichen Krisenreaktionsteams im Unternehmen, sich auf ihre Aufgaben zu konzentrieren und sich um die Sicherstellung des Geschäftsbetriebes zu kümmern.

Die Botschaften müssen, man kann es nicht oft genug wiederholen, konsistent und präzise sein und von einer verantwortlichen Person des Unternehmens kommen. Hierzu gehört, gerade bei länger dauernden Ereignissen, über Fortschritte, kritische Bedürfnisse und Probleme zu kommunizieren. Je nach Zielgruppe kann die Art der Kommunikation variieren, sie sollte aber auf denselben Informationsquellen beruhen.

### 5.3.7 Resilienz und Reputationsmanagement

Das Fehlen eines Plans zur Sicherstellung der Kontinuität des Geschäftsbetriebs birgt für das Unternehmen erhebliche Risiken. Ohne solch einen Plan ist das Unternehmen schlecht auf mögliche Probleme und Betriebsrisiken vorbereitet.

Mögliche Risiken nehmen keine Rücksicht auf Unternehmen, die keinen Plan haben.

*Alles, was schiefgehen kann, wird auch schiefgehen.*

*([https://de.wikipedia.org/wiki/Murphys\\_Gesetz](https://de.wikipedia.org/wiki/Murphys_Gesetz))*

Zu den Dingen, die passieren und zu erheblichen Problemen führen können, gehören z. B.:

► **Ausfallzeiten von Cloud-basierten Systemen und Applikationen**

Schon wenige Minuten Ausfallzeit können zu immensen Umsatzeinbußen führen.

► **Verlust des Renommees und der Markenidentität**

Anhaltende oder häufige Ausfallzeiten können das Vertrauen der Kunden in das Unternehmen untergraben.

► **Verlust der Zertifizierung des Unternehmens oder Konventionalstrafen und Bußgelder (NIS2 oder KRITIS)**

Mit dem Verlust einer erforderlichen Zertifizierung kommt es zum Verlust einer Beauftragung.

► **Nichteinhaltung gesetzlicher Auflagen bei Finanzdienstleistungen, im Gesundheitswesen und der Energiewirtschaft**

Mögliche Untersagung des Geschäftsbetriebs bei wiederholten Verstößen.

Die Möglichkeiten negativer Auswirkungen auf den Geschäftsbetrieb, jenseits der eigentlichen Störung, können existenzielle Auswirkungen haben. Es geht weniger da-

rum, welche Maßnahmen Sie für die Sicherstellung des Betriebs treffen, sondern dass Sie überhaupt welche treffen.

Wir wollen uns nach diesem allgemeinen Exkurs ins BCM einem besonderen BCM-Baustein zuwenden, dem Notfallhandbuch.

### 5.3.8 Notfallhandbuch

Ein Notfallhandbuch ist ein zentrales Element für den IT-Wiederherstellungsplan im Falle eines kompletten Systemausfalls oder einer Krise und ein wegweisendes Dokument innerhalb des Business-Continuity-Management-Frameworks.

Einige Unternehmen verzichten aus einer falschen Annahme der Unverwundbarkeit auf das Erstellen und Aktualisieren eines solchen Handbuchs – dies ist jedoch riskant. In Notfällen treten erheblicher Stress und Unsicherheit auf, und ein Notfallhandbuch kann vor allem weniger erfahrenen IT-Mitarbeitern Orientierung und Stabilität bieten. Ein Notfallhandbuch dient der Unterstützung im Notfall, z. B. durch Checklisten. Man beginnt nicht erst im Notfall, sich mit dem Handbuch vertraut zu machen.

#### Digitales Notfallhandbuch

In Zeiten vollständiger Digitalisierung ist die Versuchung groß, ein Notfallhandbuch vollständig digital abzubilden, sei es als Word-Datei in einer SharePoint-(Online-)Dokumentenbibliothek oder als digitale Informationssammlung in einer Softwarelösung wie *Confluence*.

Ich rate von der rein digitalen Nutzung eines Notfallhandbuchs ab. Sicherlich erleichtert Ihnen eine digitale Ablage die Pflege und Versionierung, jedoch ist es unumgänglich, das Handbuch in ausgedruckter Form griffbereit zu haben. Schließlich kann ein Notfall auch den vollständigen Verlust der IT-Infrastruktur und den Zugriff auf das Internet bedeuten. Gut vorbereitet sind Sie, wenn Sie beide Medien vorrätig haben: einmal in Papierform und einmal als digitale Kopie. Aber Achtung: Alle Versionen müssen identisch sein, sonst entsteht schnell Chaos!

Halten Sie immer mindestens zwei Ausgaben des IT-Notfallhandbuchs an unterschiedlichen Orten im Unternehmen vor. Bedenken Sie, dass das IT-Notfallhandbuch nur ein Bestandteil des Notfallhandbuchs für das Unternehmen darstellt.

Ein Notfallhandbuch hat die Aufgabe, Ihnen alle notwendigen Informationen für eine Notfallsituation in leicht lesbarer Form und eine Struktur der erforderlichen Abläufe und Aktionen zu geben. Es ist also ein hilfreiches und unterstützendes Hilfsmittel und kein lästiges Übel.

Ein Notfallhandbuch muss alle wichtigen Kontakte mit allen erforderlichen Kontaktinformationen enthalten. Ergänzt wird dies durch eine Kontaktmatrix, aus der her-

vorgeht, wer wen wie und warum informiert. Nur so kann sichergestellt werden, dass keine wertvolle Zeit verloren geht.

Ebenso wichtig sind auch Informationen, mit wem nicht gesprochen wird. Dies ist besonders wichtig, um einen unkontrollierten Informationsfluss an die Medien zu verhindern. Anfragen von Medien sind im Regelfall immer an die Kommunikationsabteilung Ihres Unternehmens zu verweisen.

Um den Notfallzugriff auf IT-Systeme sicherzustellen, müssen auch die Informationen und Anmeldedaten für Notfallkonten im Handbuch enthalten sein. Da die Eintragung von Kennwörtern im Handbuch ein Sicherheitsrisiko darstellt, sollten Sie nur Informationen zum sicheren Ablageort der zugehörigen Kennwörter vermerken. Zu den Notfallkonten gehört beispielsweise ein Microsoft-365-Breakglass-Account (<https://learn.microsoft.com/entra/identity/role-based-access-control/security-emergency-access>).

## 5.4 Implementierungsumgebungen einrichten

Unterschätzen Sie die Risiken bei der Einführung von neuen IT-Lösungen nicht. Im schlimmsten Fall kommt es z. B. durch eine Softwareaktualisierung zu einem Stillstand der Produktion oder zu einem anderen schwerwiegenden Fehler, der zu einem Betriebsstillstand führt.

Die Einrichtung von Entwicklungs- und Test- sowie Abnahmumgebungen ist entscheidend für den Erfolg und die Integrität einer IT-Enterprise-Architektur. Leider sparen sich viele Unternehmen die Einrichtung solcher Umgebungen. Ohne die realen Risiken einer unbedachten Einführung neuer Softwarekomponenten zu betrachten, werden einzige die Kosten dieser Umgebungen in Betracht gezogen.

### Testumgebungen – ja, nein, vielleicht?

Der betriebliche Alltag als Berater zeigt, dass viele Unternehmen sich den Betrieb einer Implementierungsumgebung aus Kostengründen sparen. Neue Produkte werden unmittelbar in der einzigen vorhandenen IT-Umgebung implementiert, nämlich in der produktiven. Dies ist oftmals im Mittelstand der Fall. Über den Sinn oder Unsinn von Testumgebungen habe ich im Laufe der Zeit unzählige Diskussionen geführt.

Ich kann nur empfehlen, mindestens eine Testumgebung zu nutzen, um nicht nur neue Produkte, sondern auch Konfigurationsänderungen zu testen, bevor Sie diese in Ihrer produktiven IT-Infrastruktur einführen.

Ja, der Betrieb zusätzlicher Umgebungen ist mit Betriebskosten verbunden. Eine Störung oder sogar der vollständige Ausfall Ihrer produktiven IT ist unterm Strich wesentlich teurer.

Mit einer Entwicklungs- und Testumgebung testen Sie neue Funktionen oder Verbesserungen an der Architektur, ohne dass Sie den laufenden Betrieb stören. Dies erhöht die Qualität und Zuverlässigkeit der IT-Lösung im Ganzen und vermeidet unnötige Kosten oder Verzögerungen bei der Umsetzung. Eine Abnahmumgebung wiederum ermöglicht Ihnen, die Funktionsfähigkeit und Leistung einer IT-Lösung unter realistischen Bedingungen zu prüfen, bevor sie in die produktive Umgebung überführt wird. So reduzieren Sie das Risiko von unerwarteten Fehlern oder Ausfällen, die sich negativ auf die Geschäftsprozesse oder die Kundenzufriedenheit auswirken könnten.

Die wichtigsten Argumente für die Einrichtung von Entwicklungs- und Testumgebungen sind:

► **Fehlererkennung und -behebung**

In einer Entwicklungs- und Testumgebung können Anpassungen an der Architektur getestet werden, um potenzielle Fehler und Unstimmigkeiten zu identifizieren, bevor sie in die produktive Umgebung eingeführt werden. Indem Fehler frühzeitig gefunden werden, können Probleme gelöst werden, bevor sie den laufenden Betrieb beeinträchtigen.

► **Risikominimierung**

Durch die Testumgebung kann man Änderungen in einer realistischen Situation testen, ohne das aktive System zu stören. Dies trägt dazu bei, das Risiko von plötzlichen Störungen oder Fehlern zu verringern, da mögliche Probleme vor dem Übergang in den Echtzeitbetrieb erkannt und gelöst werden können.

► **Qualitätssicherung**

Das Bereitstellen einer eigenen Test- und Abnahmumgebung ermöglicht es, Veränderungen an der Architektur gründlich zu prüfen, um die Qualität und Stabilität zu sichern. Dabei werden nicht nur die technischen Elemente, sondern auch die Verbindung mit anderen Systemen, die Nutzerfreundlichkeit und die Befolgung von Vorgaben und Normen berücksichtigt.

► **Parallelentwicklung**

Entwicklungs- und Testumgebungen ermöglichen es, parallel an verschiedenen Änderungen oder Projekten zu arbeiten, ohne dass diese sich gegenseitig beeinträchtigen. Dies fördert eine effiziente Entwicklung und ermöglicht es, neue Funktionen oder Verbesserungen unabhängig voneinander zu testen.

Dies gilt gleichermaßen für Softwareeigenentwicklungen wie für Konfigurationsanpassungen oder -erweiterungen für Branchensoftwarelösungen.

► **Schutz der Produktionsumgebung**

Die Produktivumgebung ist der entscheidende Bereich der IT-Infrastruktur, da sie unmittelbar die Geschäftsabläufe unterstützt. Durch den Einsatz eigenständiger Entwicklungsumgebungen und Testsysteme wird das Risiko negativer Einflüsse

auf den Livebetrieb verringert. Fehler können so vorab in einem kontrollierten Umfeld erkannt und behoben werden.

Man darf sich jedoch nicht der Illusion hingeben, dass der Einsatz von Testumgebungen das Risiko eines Fehlers bei der Implementierung eines neuen Releases in der Produktionsumgebung auf 0 % minimiert. Naturgemäß existieren immer minimale Variationsunterschiede zwischen den Umgebungen, die im ungünstigsten Fall doch zu einem Fehler führen könnten. Diesem Restrisiko begegnen Sie durch einen Rollback-Plan, um den Betriebszustand vor dem Release-Rollout schnell wieder herstellen zu können.

► **Abnahmeprozess**

Abnahmetests im Rahmen eines individuellen Abnahmeprozesses dienen dazu, dass die zuständigen Interessengruppen in Ihrem Unternehmen die Veränderungen prüfen und ihre Zustimmung erteilen können, bevor sie in die Produktionsumgebung eingeführt werden. Im Regelfall sind dies die innerbetrieblichen Fachabteilungen, die auch die ursprüngliche Produkt- bzw. Funktionsanforderung gestellt haben. Idealerweise gehören zu diesem Personenkreis Menschen, die in der Lage sind, aussagekräftige Rückmeldungen bei eventuell auftretenden Fehlern zu geben.

Der Abnahmeprozess gewährleistet somit, dass die Modifikationen den Anforderungen gerecht werden und die Nutzererwartungen erfüllt sind, bevor sie in die Produktionsumgebung überführt werden und einem größeren Nutzerkreis, zu dem u. U. auch externe Kunden gehören können, zur Verfügung gestellt werden.

► **Dokumentation und Wissensaufbau**

Entwicklungs- und Testumgebungen sind außerdem nützliche Instrumente für die Dokumentation und den Austausch von Kenntnissen. Sie ermöglichen es Entwicklern und Testern, ihre Erkenntnisse festzuhalten und weiterzugeben, was das Verständnis der Systemarchitektur im gesamten Team verbessert.

Sie sollten unbedingt Entwicklungs- und Test- sowie Abnahmumgebungen einrichten, alles andere ist ein großes Risiko! Diese Umgebungen sind wesentliche Bestandteile eines umfassenden Change-Management-Prozesses, der dazu beiträgt, die Stabilität, Qualität und Sicherheit der IT-Landschaft zu gewährleisten.

#### **5.4.1 Entwicklung**

Die Entwicklungsumgebung soll die Kreativität der Softwareentwickler nicht einschränken oder hemmen. Gerade im Rahmen eines DevOps-basierten Vorgehens ist es wichtig (siehe Kapitel 14), dass unterschiedliche Lösungsansätze ausprobiert und abgewogen werden können. Dies birgt naturgemäß Chancen und Risiken zugleich.

Eine gute Entwicklungsumgebung zeichnet sich durch einen hohen Grad an Automatisierung aus, um benötigte Ressourcen einfach, schnell und standardisiert bereitzustellen. Durch den Einsatz von Werkzeugen zur Infrastrukturautomatisierung wie Ansible, Puppet oder Chef können Umgebungen konsistent und im Self-Service durch Entwickler bereitgestellt werden.

Hier eine allgemeine Empfehlung zu geben, ist nahezu unmöglich, da sich die Anforderungen in jedem Unternehmen unterscheiden. Je nach Geschäftsfeld oder Industriezweig sind ganz unterschiedliche Voraussetzungen einzuhalten. Es kann sogar so weit gehen, dass sich selbst die Entwicklungsumgebung, im Hinblick auf Netzwerk- und Zugriffsprotokolle nah an der Produktionsumgebung orientieren muss.

#### 5.4.2 Test und Abnahme

Die Implementierung einer dedizierten Test- und Abnahmeplattform innerhalb der internen IT zahlt sich in vielerlei Hinsicht aus. So eine Plattform ermöglicht es Ihnen, eine zentrale und standardisierte Umgebung für das gesamte Spektrum an Test- und Abnahmeverfahren vorzubereiten. Das führt dazu, dass alle Tests unter einheitlichen Bedingungen stattfinden können, was sowohl die Vergleichbarkeit der Ergebnisse verbessert als auch die Wahrscheinlichkeit von Fehlern verringert. Durch die Verwendung einer Plattform wird gewährleistet, dass alle involvierten Personen dieselben Tools und Verfahren anwenden, wodurch die Konsistenz und die Verlässlichkeit der Testverfahren gestärkt werden.

Ein zusätzlicher bedeutender Nutzen für Ihr Unternehmen ist die gesteigerte Sicherheit und Überwachung der Testabläufe. Indem Sie auf eine hauseigene Test- und Abnahmeplattform setzen, verhindern Sie die Notwendigkeit, vertrauliche Daten und Informationen an Drittunternehmen weiterzugeben. Dies reduziert das Risiko von Datenlecks und unberechtigten Zugriffen erheblich. Außerdem kann Ihre IT-Abteilung die Plattform gemäß den besonderen Sicherheitsvorgaben Ihres Unternehmens einrichten und individuell anpassen, was zu einem erhöhten Schutzniveau führt.

Die Möglichkeit, eine interne Test- und Freigabeplattform flexibel zu gestalten und anpassen zu können, stellt einen weiteren erheblichen Vorteil dar. Die interne Verwaltung erlaubt schnelle Anpassungen an veränderte Anforderungen des Unternehmens. Es ist unkompliziert, neue Tests und Szenarien hinzuzufügen, ganz ohne externe Anbieter. Dies führt zu einer zügigen Bewältigung neuer Herausforderungen und verbessert die Flexibilität Ihres Unternehmens.

Zudem sollten Sie die Kosteneinsparungen beachten. Trotz möglicherweise hoher Anfangsinvestitionen für eine eigene Plattform stellen sich langfristig signifikante Einsparungen ein. Externe Dienstleister sind oftmals mit hohen und wiederkehrenden Kosten verbunden. Eine intern betriebene Plattform reduziert jedoch Betriebs-

kosten durch Nutzung bestehender Ressourcen. Effizienzsteigerung und Fehlerreduktion können zusätzlich Kosten senken.

Eine dedizierte Plattform für Tests und Abnahmen begünstigt die Kooperation und den Wissensaustausch in Ihrem Unternehmen. IT-Mitarbeitende haben die Möglichkeit, ihre Kompetenzen durch die Mitwirkung an Entwicklung und Pflege der Plattform fortlaufend zu vertiefen. Das fördert nicht nur das Expertenwissen im Unternehmen, sondern erleichtert auch die Zusammenarbeit zwischen verschiedenen Bereichen und Teams.

#### 5.4.3 Produktion

Eine produktive IT-Infrastruktur ist das Rückgrat jedes modernen Unternehmens. Gerade für die Nutzung einer Cloud-Infrastruktur ist diese Agilität eines der Kernversprechen. Ohne eine robuste IT-Infrastruktur könnten viele Ihrer täglichen Geschäftsprozesse ins Stocken geraten, was zu Verzögerungen, erhöhten Kosten und unzufriedenen Kunden und Kundinnen führen würde.

Die Sicherheit Ihrer IT-Infrastruktur ist ebenfalls von größter Bedeutung. In einer Zeit, in der Cyberangriffe immer häufiger und raffinierter werden, müssen Sie sicherstellen, dass Ihre Daten und Systeme geschützt sind. Eine produktive IT-Infrastruktur umfasst robuste Sicherheitsmaßnahmen, die Ihre sensiblen Informationen vor unbefugtem Zugriff und Datenverlust schützen. Dies ist nicht nur wichtig für den Schutz Ihrer eigenen Daten, sondern auch für die Einhaltung gesetzlicher Vorschriften und den Schutz der Daten Ihrer Kunden.

Die Produktionsumgebung ist der Kernbestandteil einer produktiven IT-Infrastruktur. Diese Umgebung stellt sicher, dass alle Anwendungen und Systeme, ob in der Cloud oder On-Premises, unter realen Bedingungen getestet und betrieben werden. Eine stabile und gut verwaltete Produktionsumgebung minimiert das Risiko von Fehlern und Ausfällen, die die Geschäftsprozesse in Ihrem Unternehmen beeinträchtigen können. Sie ermöglicht es Ihnen, neue Funktionen und Updates sicher und effizient zu implementieren, ohne den laufenden Betrieb zu stören.

#### 5.4.4 Tipps zur Umsetzung

Die Einrichtung einer Entwicklungs- und Test- sowie Abnahmeumgebung ist entscheidend, um die Qualität von eigenentwickelter Software und die Integrationsfähigkeit von Drittanbieterlösungen zu gewährleisten und einen reibungslosen und nachvollziehbaren Implementierungsprozess zu ermöglichen. Hier sind einige Tipps für die Umsetzung dieser Umgebungen.

### Replikat der Produktionsumgebung einrichten

Eine Replikation der Produktionsumgebung stellt die Konsistenz für die Entwicklung und den Test neuer Lösungen sicher. Wenn die Entwicklungsumgebung die gleichen Konfigurationen, Daten und Abhängigkeiten wie die Produktionsumgebung hat, können die Entwickelnden und Testenden sicherstellen, dass ihre Änderungen keine unerwarteten Seiteneffekte oder Inkonsistenzen verursachen, wenn sie auf die Produktionsumgebung übertragen werden. Dies erleichtert die Fehlersuche, die Versions- und die Qualitätskontrolle.

Ebenso wichtig ist die Performance der Umgebungen. Nur wenn die Entwicklungs- und Testumgebung die gleiche Hardware, Software und Netzwerkinfrastruktur wie die Produktionsumgebung nutzen, kann die Leistung der zu implementierenden Lösungen realistisch bewertet und optimiert werden. Dies hilft, Engpässe, Latenzen und Skalierbarkeitsprobleme zu vermeiden oder zu beheben, bevor sie sich negativ auf die Benutzererfahrung in der Produktivumgebung auswirken.

Ein weiterer Grund ist die Sicherheit. Die Testumgebung muss die gleichen Sicherheitsrichtlinien, Protokolle und Standards wie die Produktionsumgebung einhalten, damit beim Test von Applikationen die Sicherheit der Lösungen gewährleistet und Risiken wie Datenverlust, Datenschutzverletzungen oder Cyber-Angriffe minimiert werden können. Dies schützt nicht nur die Integrität und Vertraulichkeit der Daten in allen Umgebungen, sondern auch den Ruf und die Haftung Ihres Unternehmens. Ebenso zeigt sich bereits im Test, ob die (Sicherheits-)Richtlinien in der produktiven Umgebung sich eventuell negativ auswirken.

### Versionierung und Code-Repository nutzen

Neben der Replikation der Produktionsumgebung ist es auch wichtig, ein effektives Versionskontrollsystem und ein zentrales Code-Repository für die Entwicklungs- und Testumgebungen zu implementieren. Dies hat mehrere Vorteile für die Zusammenarbeit in Ihrem IT-Team.

Zunächst erleichtert es die Abstimmung von Modifikationen und verhindert Überschneidungen. Wenn mehrere Entwickler und Tester an einem Projekt arbeiten, ist es notwendig, dass sie ihre Modifikationen regelmäßig abgleichen und zusammenführen. Ein Versionskontrollsystem zusammen mit einem Code-Repository vereinfacht diesen Vorgang, indem es einen zentralen Anlaufpunkt für die Kontrolle und das Management der Änderungen bietet.

Weiterhin verbessert es die Nachvollziehbarkeit und Verantwortung. Durch den Einsatz eines Versionskontrollsystems sowie eines Code-Repositorys ist es möglich, lückenlos zu dokumentieren, wer welche Änderungen zu welchem Zeitpunkt und aus welchem Grund vorgenommen hat. Das unterstützt die Projektkontrolle, ermöglicht

gezieltes Feedback, hilft bei der Identifikation von Problemen und dem Erarbeiten von Lösungen.

Es erhöht die Zuverlässigkeit und Wiederverwendbarkeit. Mit einem Versionskontrollsystem und einem entsprechenden Code-Repository haben Sie die Möglichkeit, auf frühere Versionen Ihres Codes zurückzugreifen und diese bei Bedarf zu rekonstruieren. Dieser Vorteil erweist sich als hilfreich beim Debugging, der Implementierung neuer Funktionen oder der Anpassung Ihrer Lösungen an unterschiedliche Bedingungen oder Einsatzgebiete.

#### **Automatisierte Build-Prozesse etablieren**

Automatisierte Build- und Integrationsprozesse sind ein wesentlicher Bestandteil moderner Softwareentwicklung und bieten zahlreiche Vorteile, die Ihre Arbeit erheblich erleichtern können. Zunächst einmal ermöglichen sie eine kontinuierliche Integration (*Continuous Integration*), bei der Änderungen regelmäßig und automatisch in das Hauptprojekt integriert werden. Dies reduziert die Wahrscheinlichkeit von Integrationsproblemen, die oft erst spät im Entwicklungszyklus entdeckt werden. Durch die frühzeitige Erkennung und Behebung von Fehlern sparen Sie nicht nur Zeit, sondern verbessern auch die Qualität Ihres Codes.

Ein weiterer wichtiger Aspekt ist die Effizienzsteigerung. Automatisierte Prozesse übernehmen repetitive Aufgaben wie das Kompilieren von Code, das Ausführen von Tests und das Bereitstellen von Builds. Dies bedeutet, dass Ihr Team sich auf wichtigere Aufgaben konzentrieren kann, wie das Entwickeln neuer Features oder das Verbessern bestehender Funktionen. Zudem werden menschliche Fehler minimiert, da die Automatisierung konsistente und reproduzierbare Ergebnisse liefert. Dies führt zu einer höheren Zuverlässigkeit und Stabilität Ihrer Software.

#### **Containerisierung und Virtualisierung konsequent nutzen**

Die Verwendung von Containern und Virtualisierung für Test- und Abnahmeprozesse bringt viele Vorteile mit sich und steigert die Effizienz Ihrer Entwicklungsarbeit. Container sorgen für eine konsistente, isolierte Umgebung und mindern dadurch Schwierigkeiten, die durch Divergenzen zwischen Entwicklungs- und Produktionsumgebungen auftreten könnten. Mit dieser Methode können Sie darauf vertrauen, dass Ihre Software in der Produktion so performt wie während des Tests.

Ein weiterer Pluspunkt sind die Skalierbarkeit und Anpassungsfähigkeit, die durch Containerisierung und Virtualisierung erreicht werden. Software-Container erlauben das zügige Aufsetzen von neuen Anwendungsinstanzen für unterschiedliche Testumgebungen. Dies ist vor allem vorteilhaft beim Durchführen von Lasttests oder beim Bewerten der Anwendungsperformance unter verschiedenen Bedingungen.

Mithilfe der Virtualisierung ist es wiederum möglich, mehrere virtuelle Maschinen auf einem einzelnen physischen Server zu betreiben, was eine effiziente Ressourcenausnutzung mit sich bringt und Kosten senkt. Es lassen sich verschiedenartige Betriebssysteme und Konfigurationen prüfen, ohne zusätzliche Hardware anschaffen zu müssen.

Container und Virtualisierung tragen wesentlich zur verbesserten Kollaboration und Integration innerhalb von Teams bei. Weil sie einfach zu verteilen und nachzubilden sind, können sowohl Entwickler als auch Tester und Betriebsteams die gleichen Arbeitsumgebungen verwenden, was wiederum Kommunikation und Teamarbeit stärkt. Das gesamte Team profitiert von einer einheitlichen Umgebung, was Fehler suche und Korrekturen vereinfacht. Darüber hinaus unterstützt der Einsatz von Containern und Virtualisierung die Verfeinerung Ihrer Continuous-Integration-/Continuous-Deployment(CI/CD)-Workflows durch automatisierte Tests und Deploys in getrennten Umgebungen, was zu zügigeren Entwicklungsprozessen und verbesserter Softwarequalität führt. Aber was ist das überhaupt?

### **Continuous Integration/Continuous Deployment (CI/CD): moderne Ideen der Softwareentwicklung umsetzen**

In der Softwareentwicklung werden die Prinzipien *Continuous Integration (CI)* und *Continuous Deployment (CD)* genutzt, um die Qualität und Produktivität Ihrer Projekte deutlich zu verbessern. Mit CI können Änderungen am Code beständig und automatisiert in das Gesamtprojekt eingespielt werden. Dadurch lassen sich Fehler früh erkennen und beheben, was das Risiko größerer Schwierigkeiten minimiert. So profitieren Sie von einer robusteren Codebasis und gewährleisten eine nahtlose Implementierung neuer Features in existierende Systeme.

CI/CD vereinfacht durch Automatisierung den gesamten Prozess von Build und Deployment und minimiert dadurch Zeitverlust sowie menschliche Fehler. Bei jedem Update laufen automatische Tests, die Qualität sicherstellen. Schnellere und zuverlässigere Updates der Anwendungen tragen dazu bei, das Produkt eher auf den Markt zu bringen und einen Marktvorteil zu sichern.

CI/CD verbessert die Teamarbeit und sorgt für Klarsicht unter den Beteiligten. Mit dem Zugang zu stets aktuellen Code-Versionen wird die Kommunikation gestärkt und die Koordination vereinfacht. Alle sind über die neuesten Änderungen im Bilde, was das gegenseitige Verständnis fördert und gerade in größeren oder verteilten Teams die Zusammenarbeit erleichtert. Letztlich helfen CI/CD-Methoden, Entwicklungszeiten zu reduzieren und eine fortlaufende Qualitätssteigerung der Software zu gewährleisten.

### Realistisch testen

Was bringt es, wenn bei der Entwicklung und Validierung von Anwendungen von Wunschdaten ausgegangen wird, die nicht der Realität entsprechen? Sie brauchen realistische Daten, wenn Sie mit Tests die Qualität und Verlässlichkeit Ihrer Software sicherstellen. Durch das Testen mit solchen Daten lässt sich gewährleisten, dass die Applikation in einem realitätsnahen Umfeld erprobt wird, wodurch mögliche Fehler früh entdeckt und behoben werden können. Dies führt zu einer robusteren und fehlerresistenteren Anwendung für die Produktivumgebung.

Der Gebrauch von realitätsnahen Testdaten trägt zur Optimierung der Nutzererfahrung bei. Durch das Testen Ihrer Software mit Daten, die echten Benutzerinformationen nahekommen, wird gewährleistet, dass alle Funktionen erwartungsgemäß arbeiten. Dies beinhaltet Eingabevervalidierung, Datenverarbeitung und die Ausgabe von Ergebnissen. Realistische Testsätze tragen dazu bei, die Leistung Ihrer Applikation zu steigern und eine konstante Zuverlässigkeit unter diversen Bedingungen sicherzustellen, was wiederum zu gesteigerter Kundenzufriedenheit und einer verbesserten Gesamtnutzererfahrung führt.

Die Verwendung von realitätsnahen Testdaten verbessert die Teamarbeit und den Austausch untereinander. Wenn das gesamte Team die gleichen Daten benutzt, wird das für eine bessere Transparenz sorgen und Problemlösungen vereinfachen. Alle haben ein einheitliches Verständnis der Daten, was die Zusammenarbeit zur Identifizierung und Behebung von Problemen effektiver macht. Weiterhin erlaubt der Gebrauch solcher Testdaten die Standardisierung und Automatisierung von Test- und Freigabeverfahren und steigert dadurch Effizienz und Durchgängigkeit. Realistische Testdaten führen insgesamt zu kürzeren Entwicklungszeiten und einer stetigen Optimierung der Softwarequalität.

### Performance- und Skalierungstests nutzen

Die Durchführung von Performance- und Skalierungstests ist unverzichtbar, um die Zuverlässigkeit und Leistungsfähigkeit von Eigenentwicklungen sowie Anwendungen Dritter zu gewährleisten. Mit Performance-Tests lässt sich ermitteln, wie schnell und reaktionsstark Ihre Software unter unterschiedlichen Belastungsbedingungen arbeitet. So machen Sie mögliche Engstellen und Schwächen frühzeitig aus, bevor sie zu einem Problem für die Anwender werden. Eine optimierte Anwendung verbessert das Nutzererlebnis und kann zu einer signifikanten Erhöhung der Kundenzufriedenheit führen.

Ein weiterer Faktor ist die Skalierbarkeit Ihrer Software. Durch das Durchführen von Skalierungstests wird ermittelt, wie leistungsfähig Ihre Anwendung bei einer ansteigenden Benutzer- und Datenvolumenzahl bleibt. Dies ist vor allem für Systeme relevant, die mit rascher Nutzerzunahme oder hohen saisonbedingten Anfragespitzen

rechnen müssen. Mithilfe dieser Tests lässt sich gewährleisten, dass Ihre Infrastruktur steigenden Belastungen standhalten kann, ohne an Leistung einzubüßen. Dadurch verhindern Sie unvorhergesehene Systemausfälle und sichern die durchgehende Erreichbarkeit Ihrer Services.

Durch regelmäßige Performance- und Skalierungstests wird eine präventive Instandhaltung und Entwicklung Ihrer Anwendungen sichergestellt. Wenn Sie solche Tests durchführen, können Sie zeitnah auf Nutzungsänderungen reagieren und Anpassungen vornehmen. So verbessern Sie Ihre Software stetig und sorgen dafür, dass sie aktuell bleibt. Mit diesen Insights können sie wohlüberlegte Entscheidungen treffen und wissen besser, welche Investitionen notwendig sind.

### Abnahme- und Benutzertests

Akzeptanztests und Tests durch Endbenutzer sind für den Erfolg Ihrer Softwareprojekte unerlässlich, denn sie garantieren, dass die Anwendung den Bedürfnissen und Erwartungen der Nutzer gerecht wird.

*User Acceptance Tests (UAT)* evaluieren die Anwendungssoftware aus Kundensicht, um zu bestätigen, dass alle gewünschten Funktionen korrekt implementiert sind und fehlerfrei funktionieren. Sie decken mögliche Schwachstellen auf, die noch vor dem Übergang in den Produktiveinsatz behoben werden müssen, was wiederum die Notwendigkeit kostspieliger Korrekturen verringert und die Zufriedenheit der Anwender erhöht.

Im Gegensatz dazu richten sich *Benutzertests* an die tatsächlichen Endbenutzer der Software. Diese Tests eröffnen wichtige Erkenntnisse über die Benutzerfreundlichkeit und das gesamte Nutzererlebnis der Anwendung. Durch die Einbindung echter Nutzer in die Testphase kann gewährleistet werden, dass die Software intuitiv und benutzerfreundlich ist, was die Zufriedenheit und Akzeptanz seitens der Benutzer steigert. Benutzertests dienen außerdem dazu, Feedback zu erhalten, um die Anwendung zu optimieren und auf Nutzerbedürfnisse abzustimmen.

Abnahme- und Benutzertests verbessern die Kommunikation und Zusammenarbeit zwischen Stakeholdern, fördern Transparenz und Vertrauen durch Einbindung von Kunden und Nutzern und tragen zur Lösungsfindung bei. Sie steigern die Softwarequalität und optimieren den Entwicklungsprozess, verkürzen die Entwicklungszyklen und erhöhen die kontinuierliche Softwarequalität.

### Den Notfall üben

Das Durchführen von Notfallwiederherstellungstests ist ein unerlässlicher Teil der IT-Sicherheitsstrategie, die schon während der Testphase und vor der Inbetriebnahme stattfinden sollten. Diese Überprüfungen gewährleisten, dass Systeme und Daten effizient und zügig wiederbeschafft werden können, wenn Störungen oder katastro-

phale Ereignisse eintreten. Indem solche unter kontrollierten Bedingungen ausgeführt werden, werden potenzielle Schwächen und Defizite im Wiederherstellungsprozess erkannt, und Sie können aktiv werden, bevor sie sich zu realen Problemen entwickeln können. Dies verleiht Ihnen das Vertrauen, dass Ihre Systeme selbst in Notfallsituationen verlässlich arbeiten.

Die Schulung und das Training Ihres Teams sind ebenso von entscheidender Bedeutung. Indem Sie regelmäßige Übungen zur Notfallwiederherstellung in Ihrer Test- und Staging-Umgebung durchführen, wird Ihr Team mit den erforderlichen Abläufen vertraut werden, um im Falle eines Notfalls zügig und wirksam zu handeln. Dies steigert nicht nur die Einsatzbereitschaft des Teams, sondern stärkt auch dessen Selbstvertrauen in seine Kompetenzen. Zudem gewährleisten diese Simulationen, dass alle wesentlichen Werkzeuge und Ressourcen vorhanden und einsatzbereit sind.

Letztlich tragen solche Tests zur Verminderung von Betriebsunterbrechungen bei und sichern die kontinuierliche Durchführung Ihrer Geschäftstätigkeiten.

## 5.5 Umsetzung

Die Umsetzung einer Enterprise-Architektur ist in den seltensten Fällen leicht, gerade bei der ersten Einführung einer ganzheitlich abgestimmten IT-Architektur.

Die erfolgreiche Umsetzung einer IT-Enterprise-Architektur erfordert Zeit, Engagement und eine ständige Anpassung an sich ändernde Geschäftsanforderungen und Technologielandschaften. Es ist wichtig, dass die Architektur nicht als statisches Dokument betrachtet wird, sondern als lebendiger Rahmen, der sich dynamisch weiterentwickeln kann.

### 5.5.1 Top down oder Bottom up

Um eine IT-Enterprise-Architektur zu entwickeln, ist es ratsam, die *Top-down*-Methode mit der *Bottom-up*-Methode zu kombinieren.

- ▶ Bei der *Top-down-Methode* werden Entscheidungen und Strategien von der Führungsebene einer Organisation vorgegeben und dann nach unten weitergeleitet. Dieser Ansatz erlaubt eine rasche Entscheidungsfindung und eine eindeutige Zielsetzung, da die oberste Ebene die Führung behält. Dies kann jedoch dazu führen, dass die Perspektiven und das Know-how der Mitarbeiter auf den unteren Ebenen nicht genügend berücksichtigt werden.

Mit der Top-down-Methode können Sie die IT-Enterprise-Architektur in Einklang mit der Unternehmensstrategie bringen und eine einheitliche Vision für die ganze Organisation schaffen. Die Methode stellt ebenso sicher, dass die IT-Enterprise-

Architektur die übergeordneten Ziele und Anforderungen des Unternehmens beachtet und Prioritäten bestimmt.

- ▶ Der *Bottom-up-Ansatz* hingegen startet auf der untersten Ebene, wobei die Mitarbeiter, die mehr mit den alltäglichen Prozessen und Problemen zu tun haben, an der Entscheidungsfindung beteiligt werden. Dies steigert die Mitarbeitermotivation und kann zu kreativeren Lösungen führen, da das Wissen und die Kompetenzen der Mitarbeiter eingebracht werden. Der Prozess kann aber mehr Zeit erfordern, da eine breite Übereinstimmung erreicht werden muss.

Die Bottom-up-Methode kann die IT-Enterprise-Architektur an die aktuellen Bedürfnisse und Herausforderungen der operativen Teams anpassen und deren Feedback und Erfahrungen einbeziehen. Eine Bottom-up-Methode nutzt die bestehenden Ressourcen, Fähigkeiten und etablierten Prozesse in Ihrem Unternehmen und macht die IT-Enterprise-Architektur so besser realisierbar.

In den meisten Fällen wird es auf eine *Kombination der beiden Ansätze* hinauslaufen: Sie entwickeln Ihre IT-Enterprise-Architektur in einem schrittweisen und fortschreitenden Prozess und suchen ständig nach Verbesserungen. Die Kombination der Methoden sorgt auch dafür, dass die IT-Enterprise-Architektur den richtigen Grad an Standardisierung und Abgrenzung findet und sowohl die Gemeinsamkeiten als auch die Diversität der verschiedenen Geschäftsbereiche und Funktionen einbezieht.

### 5.5.2 Stakeholder identifizieren und einbinden

Sie müssen unbedingt alle relevanten Stakeholder in den Entwicklungsprozess der IT-Enterprise-Architektur einbeziehen. Jeder Stakeholder bringt eine einzigartige Perspektive und Erfahrung in den Prozess ein, was dazu beitragen kann, potenzielle Probleme frühzeitig zu identifizieren und innovative Lösungen zu finden.

Darüber hinaus fühlen sich die Stakeholder, wenn sie in den Prozess einbezogen werden, eher verpflichtet, Sie bei der Implementierung der Architektur zu unterstützen. Dies fördert eine effektive Kommunikation und ein besseres Verständnis zwischen verschiedenen Abteilungen und Teams.

#### Was ist ein Stakeholder?

*Stakeholder* in Ihrem Unternehmen sind Personen oder Gruppen, die ein Interesse an den Aktivitäten Ihres Unternehmens haben. Sie können direkt oder indirekt betroffen sein und können das Unternehmen beeinflussen oder von ihm beeinflusst werden. Sie können Supporter, Zweifler oder auch aktive Blockierer sein. Daher ist es wichtig eine aussagekräftige Stakeholder-Analyse vorab zu erstellen. Hierzu gehören u. a.:

- ▶ Geschäftsführung
- ▶ Mitarbeitende

- ▶ Investoren
- ▶ Kunden
- ▶ Lieferanten

Im Zusammenhang der Entwicklung und Implementierung einer IT-Enterprise-Architektur liegt der Fokus auf den internen Stakeholdern, also der Geschäftsführung, Führungspersonen der Abteilungen und Mitarbeitenden.

Identifizieren Sie die für Sie und die IT-Enterprise-Architektur wichtigen Stakeholder Ihres Unternehmens mithilfe einer Stakeholder-Matrix. So erhalten Sie einen Überblick über den Einfluss, die Haltung, die Meinung, die Beeinflussbarkeit und das grundlegende Interesse der einzelnen Stakeholder.

Außerdem können Sie durch die Beteiligung aller Betroffenen das Risiko besser erkennen und reduzieren. Sie können gewährleisten, dass die IT-Enterprise-Architektur den Geschäftszielen und -anforderungen entspricht. Insgesamt führt die Beteiligung aller wichtigen Betroffenen zu einer wirksameren und wirtschaftlicheren IT-Enterprise-Architektur. Es ist wichtig, dass Sie eine offene und transparente Kommunikation pflegen und so sicherstellen, dass alle Betroffenen die Gelegenheit haben, ihre Ansichten und Bedenken zu äußern.

### 5.5.3 Orientieren Sie sich an bewährten Vorgaben

In jeder Branche gibt es Richtlinien, Standards und Best Practices, an denen Sie sich orientieren sollten. Dies sorgt im Allgemeinen dafür, dass Ihre Infrastruktur Compliance-Anforderungen erfüllt, dass Kosten reduziert werden und dass die Zukunftssicherheit und Skalierbarkeit Ihrer IT-Infrastruktur gewährleistet werden.

Viele Industrien haben spezifische Compliance-Anforderungen für IT-Systeme, und durch die Befolgung von Standards können Sie garantieren, dass Ihre Systeme diesen Anforderungen genügen. Durch die Vereinheitlichung Ihrer IT-Infrastruktur können Sie Kosten senken und die Einführung neuer Technologien und das Wachstum Ihrer Systeme erleichtern, wenn Ihr Unternehmen expandiert. Daher bieten eindeutige Richtlinien und Standards einen Leitfaden für die Entscheidungsfindung und helfen dabei, Ihre IT-Investitionen zu optimieren.