Vorwort zur 4. Auflage

Zum vierten Mal knappe 500 Seiten durchzuarbeiten, die man selbst über drei Auflagen und 18 Jahre geschrieben hatte, erfordert ein wenig Überwindung. Sieben Jahre nach der letzten Überarbeitung im Jahr 2016 hatte ich allerdings genug Abstand, um es wieder anzugehen. Motivation waren dabei nicht zuletzt auch die Menschen, denen ich begegnet bin und die mir (hoffentlich nicht nur aus Höflichkeit) gesagt haben, dass das Buch ihnen bei ihrer Arbeit geholfen hat.

Die Frage, ob das Buch grundsätzlich noch »funktioniert«, war spannend. Lassen Sie uns das anhand der Themen beantworten:

Der **musterbasierte Ansatz** für das Management von IT-Unternehmensarchitekturen funktioniert nach wie vor. Man kann aus den Unternehmenszielen abgeleitete **Zielmuster** für die IT identifizieren (Kap. 3) und basierend darauf bedarfsgerecht **Managementmuster** anwenden (Kap. 4) und dann dazu eine passende **Informationsbasis** ableiten (Kap. 5).

Fragt sich: Warum nur IT-Unternehmensarchitektur (IT-EAM)? Auf dem Gebiet der businessorientierten Unternehmensarchitektur (EA, EAM) hat sich eine Menge bewegt. TOGAF 10th Edition hat wieder in diese Richtung expandiert und es sind auch neue Global Player auf dem Markt aufgetaucht, wie die Intersection Group (*https://www.intersection.group*) mit ihrer Sprache EDGY (*https://enterprise.design*) zur Gestaltung von Unternehmensarchitektur, -erfahrung und -identität. Ich habe mich trotzdem entschieden, mich weiterhin auf die IT-Seite zu konzentrieren. Die Übergänge sind fließend und Sie werden hier genug Bezüge zu Methoden finden, die dafür sorgen, dass die Unternehmensstrategie sich in der IT-Strategie manifestiert.

Das gilt auch für die Digitalisierung. Für digitale Strategien gibt es Muster [Woerner+22]. Wenn man diese umsetzen möchte, kann man das wieder mit den Zielmustern und Managementstrategien unterfüttern, die in diesem Buch vorgestellt werden. Es war also nicht das Ziel, ein Buch über alles im Unternehmen zu schreiben, sondern sich nach wie vor auf den Anteil des IT-Managements zu konzentrieren.

Den größten Aktualisierungsbedarf hatten die Themen, die sich darauf beziehen, was man als IT-Unternehmensarchitekt neben dem Architekturkern dringend »auch noch« beherrschen muss:

- **Compliance** ist ein so umfassendes Gebiet, dass dort sowieso nur Grundlagen vermittelt werden und wenig Spezialwissen, das veraltet. Von daher war hier mäßig viel zu tun.
- **IT-Sicherheit** ist hingegen ein Gebiet, das sich sehr schnell weiterentwickelt. Hier hat Florian Oelmaier sein Kapitel gründlich überarbeitet, sodass es inzwischen ca. 20 Prozent des kompletten Buches einnimmt. Wenn man sich allerdings CIO-Prioritäten ansieht, dann ist das absolut gerechtfertigt und nötig.
- Für das **IT-Risikomanagement** gibt es sehr viele Änderungen in den Frameworks, die allesamt nach der letzten Überarbeitung des Buches vorgenommen wurden. Sei es COSO 2017 oder COBIT 2019. Beide Frameworks wurden überarbeitet und teilweise wurden Themen fusioniert.
- Die **Makro-Architekturmuster** müssen für den Zweck dieses Buches nicht die »neuesten« sein. Hier geht es vor allem darum, das Prinzip zu zeigen. Von daher war es nicht notwendig, die neueste PaaS-Plattform von Google, Amazon oder Azure hier im Detail zu beschreiben. Dafür gibt es andere Werke.
- TOGAF 10th Edition (neu in 2022), COBIT 2019 (Ende 2018) und auch ITIL 4 (2019) wurden alle nach dem Erscheinen der 3. Auflage dieses Buches gründlich überarbeitet. Daher waren starke Überarbeitungen der entsprechenden Kapitel in diesem Buch notwendig.

Trendthemen wie Lean, Agile und Cloud waren grundsätzlich schon durch die 3. Auflage abgedeckt.

Interessant werden wird der Einfluss durch »generative KI«: Noch sind die Modelle zu schwach, um Inhalte z.B. aus der Kombination von Repositories, Wikis, EAM-Tools und Freitext-Bibliotheken simultan zu bearbeiten, die aus strukturierten Daten, Text und Bildern bestehen oder es erfordern, dass »schöne« Bilder erzeugt werden. Nachdem wir hier erst am Anfang einer rasanten Entwicklung stehen, würde eine nächste Auflage sicher »voll mit KI-Themen« sein – wenn sie nicht sogar von einer generativen KI geschrieben würde. Das war hier leider noch nicht möglich. Der Ausblick (Kap. 16) gibt u.a. einen kurzen Überblick über die Herausforderungen, die zu lösen sind, bis KI einen IT-Unternehmensarchitekten wirklich bei seiner Arbeit unterstützen kann.

München – im April 2024
Wolfgang Keller

1 Einleitung und Überblick

Anforderungen an das IT-Management steigen.

Die Anforderungen an das IT-Management sind über die Jahre, in denen sich die Informationstechnologie weiterentwickelt hat, kontinuierlich gestiegen. Während es in den 1980er-Jahren ausgereicht hat, die sogenannte Beschaffungsseite der IT (siehe Abb. 1–1) im Griff zu haben – also überhaupt eine einigermaßen lauffähige IT betreiben zu können –, hatte sich die Situation bis ca. 2005 dahingehend weiterentwickelt, dass es nun wichtig war, die IT als sogenannten Enabler zu führen. Dafür war es wichtig, als IT-Verantwortlicher primär das Geschäft zu verstehen und es optimal mit den Mitteln der Informationstechnologie zu unterstützen. Noch besser war und ist es, wenn der IT-Verantwortliche in der Lage ist, dem Topmanagement echte Innovation mit IT-Hilfe anzubieten. Nicht jedes Geschäft setzt hier auf den Einsatz von Informationstechnologien. Nachdem heute aber sehr viele Geschäftsprozesse automatisiert und in IT-Systemen abgebildet sind, kann IT oft einen wichtigen Hebel für die Innovation darstellen und ist häufig eine wesentliche Komponente neuer Geschäftsmodelle. Der Trend, dass IT immer mehr zum Bestandteil neuer Geschäftsmodelle wird, spiegelt sich inzwischen auch im Thema »Digitalisierung« wider. IT ist nicht mehr eine Unterstützungsfunktion für Geschäftsmodelle, sondern wird selbst zum Teil des Geschäftsmodells. Häufig werden durch Digitalisierung sehr große Veränderungsprogramme in einer Unternehmens-IT verursacht. Solche großen Programme müssen gesteuert werden, und zwar sowohl, was das Projektmanagement anbelangt, als auch, was die Planung der IT-Unternehmensarchitektur betrifft.

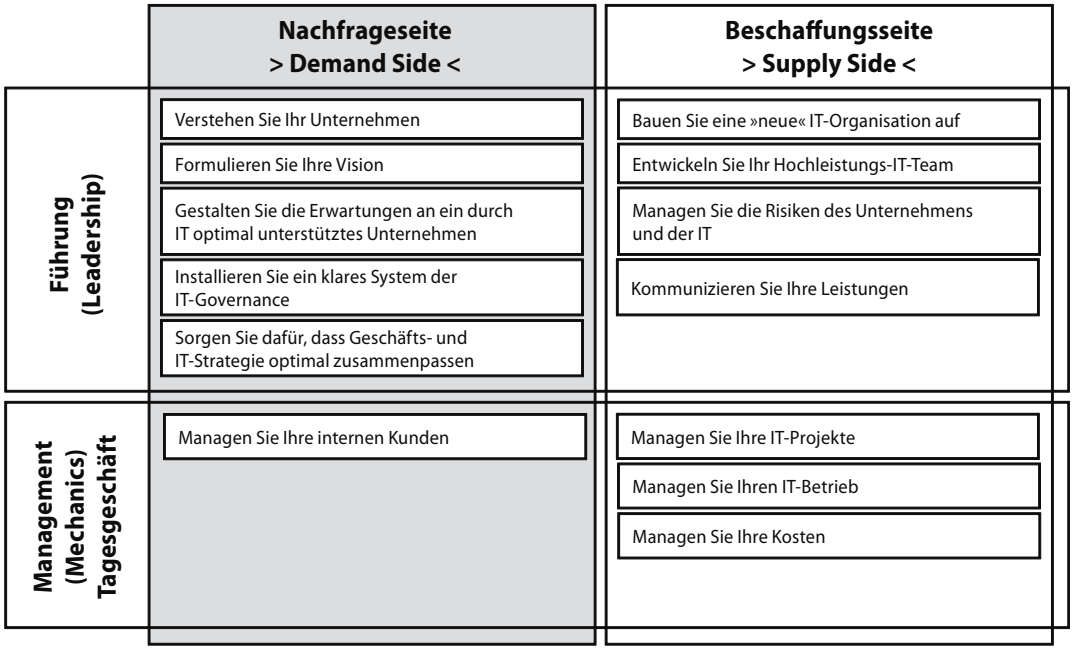


Abb. 1–1 *Agenda eines IT-Vorstands nach [Broadbent+05]*

Time-to-Market

Darüber hinaus haben sich Produktzyklen weiter verkürzt. Dies hat zur Folge, dass sich die IT-Landschaften schneller entwickeln müssen, als dies noch vor fünf oder zehn Jahren der Fall war. Apps für mobile Geräte sind heute bei Updatezyklen von durchschnittlich 30 Tagen angelangt [Kelly16]. Applikationen im Bereich mobiler Geräte und von Webfrontends sind teilweise »permanente Betaversionen«. Sogenannte Kernsysteme oder Bestandssysteme sollten ein solches Tempo eher nicht mitgehen – deshalb wird auch die sogenannte Two-Speed-IT heute kontrovers diskutiert.

Compliance und Sicherheit

Auf der Gegenseite der Beschleunigung finden sich verschärfte Anforderungen an die Compliance (das Einhalten von Gesetzen), eine wesentlich gesteigerte Sensibilität für IT-Sicherheit und Cybersicherheitsarchitektur sowie ein deutlich niedrigeres Risikoniveau, das die Öffentlichkeit, die Kunden, die Aktionäre oder der Gesetzgeber bereit sind zu akzeptieren. Das heißt, Risikomanagement – auch und gerade für die IT – spielt ebenfalls eine wichtige Rolle. Diese drei zuletzt genannten Entwicklungen machen Projekte eher langsamer als schneller.

Aus der Softwarearchitektur, die Einzelsysteme gestaltet, ist bekannt, dass mit Architekturmitteln sich einzelne Anwendungen schneller, sicherer und effizienter ändern lassen. Analog kann man auch ein komplettes Portfolio von Anwendungen so gestalten, dass sich Änderungen möglichst zügig, sicher und effizient durchführen lassen.

IT-Alignment

Die IT-Funktion eines großen Unternehmens muss im Regelfall heute also mindestens zwei Themengebiete beherrschen:

- Einerseits muss sie Enabler für ein Geschäft sein, das sich schnell ändern kann und in vielen Fällen von aggressiven Start-ups angegriffen werden wird,
- andererseits soll sie gesetzliche Auflagen erfüllen und verhindern, dass ein Unternehmen durch Sicherheitsprobleme in negative Schlagzeilen gerät, die schnell existenzbedrohende Ausmaße annehmen können.

Große Unternehmen müssen dabei viele Arten von Wettbewerbern abwehren. Kleine aggressive Start-ups können sich auf kleine lukrative Teile des Geschäftsportfolios des großen Unternehmens konzentrieren und dadurch Teile des Gewinns angreifen. Große Internetunternehmen können sich zwischen ein Unternehmen und seine Kunden schieben und dadurch die Kundenbeziehung gefährden oder Gewinn daraus abschöpfen. KI-Assistenten werden diesen Trend noch gefährlicher für die Unternehmen machen, wenn die Kunden aus Bequemlichkeit einen »künstlich intelligenten« digitalen Assistenten von Google oder Amazon fragen, der dann im Hintergrund die Anfrage des Kunden versteigert und auf den Kanal leitet, der dem Internet-Giganten am meisten für den Kontakt bietet. Bei Onlinewerbung sind solche Versteigerungen bereits üblich. Durch den Einsatz von Assistenzsystemen werden sie sich weiter verbreiten.

Man erkennt leicht, dass sich solche Anforderungen, nämlich die Abwehr schneller oder extrem mächtiger Wettbewerber aus dem Internet, von der Commodity-IT, wie sie noch vor 20–25 Jahren weit verbreitet war, deutlich unterscheiden. IT-Management benötigt heute auch fortgeschrittenere Methoden als beim Erscheinen der ersten Auflage dieses Buches vor fast 20 Jahren. Zum Glück haben sich die Methoden kontinuierlich weiterentwickelt und verbessert.

1.1 Motivation des Buches

Rolle IT-Unternehmensarchitektur

Wenn IT-Management heute für viele Unternehmen wichtiger ist als jemals zuvor, kann man sich die Frage stellen, welche Rolle denn dann IT-Unternehmensarchitektur spielt. So viel sei vorweg gesagt: IT-Unternehmensarchitektur deckt zentrale Gebiete eines fortschrittlichen IT-Managements ab. Abbildung 1–2 zeigt im Vergleich zwei Modelle für IT-Governance. In beiden Modellen sind jeweils die wichtigsten Aufgabenblöcke genannt, die ein IT-Gesamtverantwortlicher organisieren muss, um erfolgreich zu sein. Wenn man die Blöcke kurz durchgeht, ist leicht zu sehen, dass IT-Unternehmensarchitektur eine breite Rolle im IT-Management einnimmt.

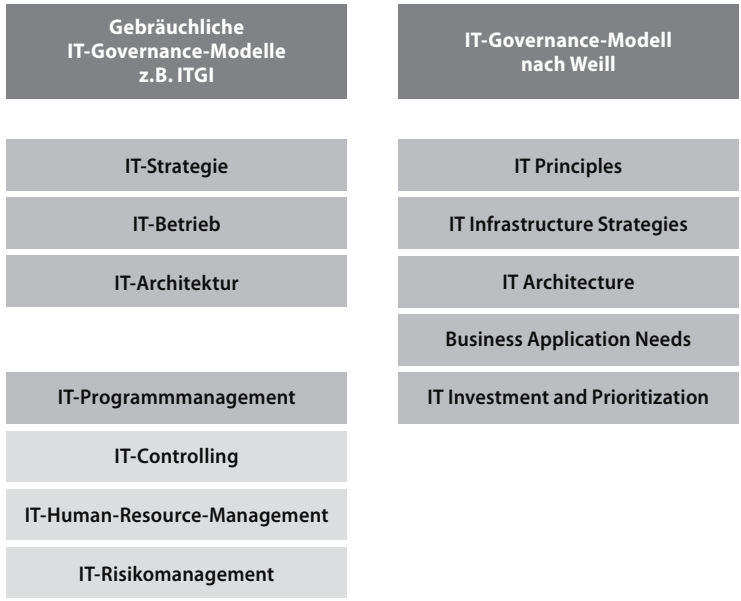


Abb. 1–2 *Aufgabengebiete des IT-Managements – dargestellt anhand der Gliederungen des IT Governance Institute® (ITGI®, links) [ITGI11] und nach Weill (rechts) [Weill+04]*

IT-Strategie

IT-Strategie: Der IT-Unternehmensarchitekt ist meist der maßgebliche Helfer des CIO, wenn es darum geht, eine IT-Strategie zu definieren. Dieses Thema wird sowohl in den Kapiteln über Zielmuster (Kap. 3) als auch über Prozessmuster (Kap. 4) ausführlich erläutert.

IT-Betrieb

IT-Betrieb: Unternehmensarchitekten, die meist ihren Berufsweg in der Softwareproduktion (Programmierung, Softwaredesign, Softwarearchitektur) zurückgelegt haben, vergessen zu oft, dass es wesentlich lohnender sein kann, Infrastruktur statt Software kostenmäßig zu optimieren. Bei vielen Unternehmen macht der Anteil der reinen Betriebskosten bis zu 70 Prozent der gesamten IT-Kosten aus. Es ist relativ klar, dass hier ein deutlich größerer Hebel liegen kann als in der Optimierung von Softwareprojekten. Durch Cloud Computing sind die Möglichkeiten, Betriebskosten zu senken, in den letzten fünf Jahren eher noch umfangreicher geworden. Man muss heute keine eigenen Rechenzentren mehr konsolidieren. Man kann sie in vielen Fällen vollständig in die Cloud auslagern und eigene Rechenzentren damit komplett abschaffen. Entsprechend ist es für einen IT-Verantwortlichen wichtig, über eine Technologiestrategie zu verfügen. Auch eine Sourcing-Strategie ist wichtig, da nicht jedes Unternehmen die komplette Infrastruktur, die es benötigt, selbst betreiben möchte. Dieses Thema erhält weiteren Schub durch Themen wie Cloud und »Software as a Service« (SaaS) und wird in diesem Buch sowohl bei den Zielmustern als auch bei den Prozessmustern behandelt.

IT-Architektur

IT-Architektur: Dass sich IT-Unternehmensarchitektur auch mit IT-Architektur (Lösungsarchitektur) beschäftigen muss, liegt nahe. Die Unternehmensarchitektur erarbeitet u. a. auch die Vorgaben für Zielarchitekturen und Blueprints als Muster für eine Menge von Einzelsystemen. Oft muss man hier allerdings nicht mehr viel selbst erarbeiten. Die meisten Cloud-Provider bieten Open-Source-Software-Stacks an, die schon einmal eine gute Grundlage für eine Lösungsarchitektur bilden. Gewisse Dinge, wie die Oberflächenarchitektur, sind allerdings nach wie vor selbst zu komplettieren, auch wenn es hier ebenfalls wieder sehr gute Vorarbeiten in Form von großteils Open-Source-Umgebungen gibt.

IT-Programmmanagement

IT-Programmmanagement: Dies ist der wesentliche Bereich des IT-Managements, der üblicherweise nicht von den IT-Unternehmensarchitekten selbst betreut wird. Hierfür gibt es in den meisten Unternehmen heute Project Management Offices, die ein unternehmensweites Programmmanagement für alle Vorhaben eines großen Unternehmens betreiben. Dementsprechend wird auch das Thema Multiprojektmanagement (siehe z. B. [Hirzel+19]) in diesem Buch nicht zentral behandelt.

IT-Controlling

IT-Controlling und IT-Human-Resource-Management fallen üblicherweise ebenfalls nicht in das Aufgabengebiet eines IT-Unternehmensarchitekten. Ebenso wird es meistens einen separaten **IT-Risikomanager** geben. Dieser arbeitet häufig eng mit den IT-Unternehmensarchitekten zusammen, da das Risikoregister normalerweise zusammen mit der Informationsbasis der IT-Unternehmensarchitekten gepflegt und visualisiert wird.

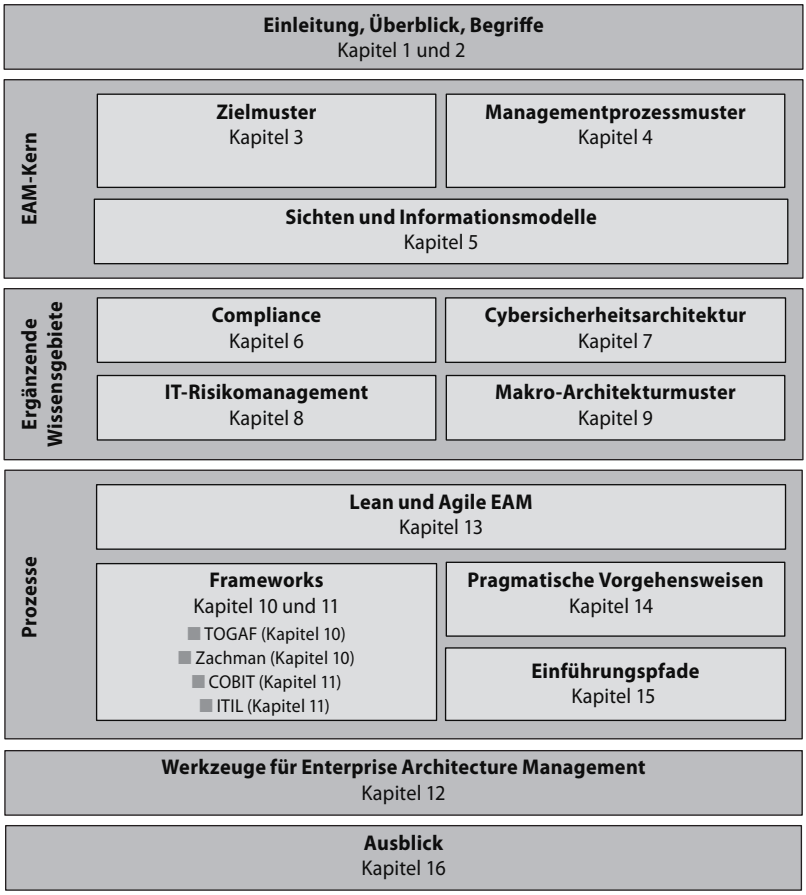
Zusammenfassend kann man also sagen, dass ein CIO (Chief Information Officer), der über eine gute Stabsstelle für IT-Unternehmensarchitektur verfügt, wesentliche Teile seines Aufgabenportfolios damit abdecken kann. Oder anders formuliert: IT-Unternehmensarchitektur deckt einen sehr großen Teil der wesentlichen IT-Managementaufgaben ab, die zentral im Umfeld eines CIO anfallen.

1.2 Struktur des Buches

Überblick über das Buch

Nach Einführung und Überblick und einigen grundlegenden Begriffsdefinitionen (Kap. 2) gliedert sich das Buch in drei große Teile (siehe auch Abb. 1–3).

Abb. 1–3
Kapitelstruktur des Buches



EAM-Kern

EAM-Kern: Der Teil über den Kern von Enterprise Architecture Management (EAM) beschreibt vor allem den Umgang mit den funktionalen (geschäftsorientierten) Anforderungen an die IT-Funktionen eines Unternehmens. Hier erfahren Sie, wie Sie Ihre Funktionen für die IT-Unternehmensarchitektur so aufbauen bzw. anpassen können, dass sie den Anforderungen des Geschäfts genügen.

In der Praxis kann man dabei immer wieder bestimmte Muster entdecken. Solche Muster lassen sich sowohl für Ziele von Unternehmen erkennen als auch für die Art und Weise, wie Unternehmen versuchen, ihre Ziele zu erreichen. In Kapitel 3 finden Sie gebräuchliche **Zielmuster**. Solche Zielmuster beschreiben typische Anforderungen an die IT-

Zielmuster

Funktionen eines Unternehmens Es ist charakteristisch, dass Sie als Unternehmensarchitekt deutlich mehr als ein einziges Ziel verfolgen müssen. Die Zielmuster sind auch nicht immer trennscharf voneinander abgegrenzt. Mithilfe solcher Muster ist es erheblich einfacher und schneller möglich, sinnvolle Ziele für das IT-Management und damit auch die IT-Unternehmensarchitektur zu beschreiben. Zielmuster werden üblicherweise dadurch erfüllt, dass man **Managementprozessmuster** anwendet. Diese finden Sie in Kapitel 4. Für bestimmte Arten von Zielen haben sich heute Prozesse etabliert, die das Erreichen dieser Ziele unterstützen. Eine weitere interessante Frage ist dann, welche **Sichten** und **Informationsmodelle** benötigt werden, um die Managementprozesse zu unterstützen. Deren wesentliche Formen werden in Kapitel 5 diskutiert. Es gibt jedoch Hunderte von möglichen Diagrammformen und Metamodellvarianten, die eine hohe dreistellige bis zu einer kleinen vierstelligen Anzahl von Metaentitäten enthalten. Hier wird das Buch also vor allem auf weiterführende Quellen hinweisen, die umfangreiche Kataloge von Sichten und Informationsmodellen und deren mögliche Metaentitäten enthalten.

Managementprozessmuster

Informationsmodelle

Der musterbasierte Ansatz, der im Buch verwendet wird, unterstellt, dass es kein »one version fits everybody«-EAM gibt, sondern dass Ziele in Unternehmen verschieden sind. Wenn Sie alle möglichen Metaentitäten füllen und alle denkbaren Auswertungen durchführen würden, würden Sie einen viel zu hohen Aufwand für EAM treiben. Es ist preiswerter, genau die Dinge zu tun, die für die Erreichung einer bestimmten Menge von Zielmustern erforderlich sind. Auf diese Weise kann und sollte man sich sein EAM selbst konfigurieren. Dabei helfen nicht nur Zielmuster, sondern auch die dazugehörigen Managementprozessmuster sowie die dazu passenden Sichten und Informationsmodellmuster. Dieses Buch ist damit seit der zweiten Auflage feinteiliger aufgebaut als die erste Auflage, die als Leitlinie für die Gliederung lediglich eine EAM-Prozesslandkarte verwendet hat, wobei diese nach wie vor enthalten ist. Für die vorliegende vierte Auflage wurde der Musteransatz beibehalten. Einzelne Prozesse finden sich nach wie vor auch in den Managementprozessmustern wieder, die seit der ersten Auflage beschrieben wurden.

Musterbasierter Ansatz

Ergänzende Wissensgebiete: In einem anspruchsvollen, modernen Unternehmensumfeld reicht es heute für einen Unternehmensarchitekten bei Weitem nicht mehr aus, nur technisch und funktional »ordentliche Lösungen« bauen zu können. Gesetzgeber, Öffentlichkeit und weitere Stakeholder haben eine Vielzahl von Ansprüchen an die Systemlandschaften von Unternehmen, die weit über die reine betriebswirtschaftliche Funktion und den technischen Aufbau hinausgehen. Solche wei-

Weitere Wissensgebiete

ter gehenden Querschnittsanforderungen kann man mit nicht funktionalen Anforderungen in der inzwischen klassischen Disziplin Softwarearchitektur vergleichen. Sie tragen zum Geschäftszweck unmittelbar nichts bei – wenn man sich allerdings nicht ausreichend um sie kümmert, haben sie das Potenzial, das Unternehmen ernsthaft zu gefährden oder sogar zu vernichten. Dies gilt sowohl für **Compliance** (Kap. 6) als auch für die Themen **IT-Sicherheit** und **Cybersicherheitsarchitektur** (Kap. 7) sowie **IT-Risikomanagement** (Kap. 8). Zum schnellen Finden sinnvoller Lösungen bedienen sich Unternehmensarchitekten darüber hinaus sogenannter Makro-Architekturmuster. Dies sind Architekturmuster im großen Maßstab, z.B. Blaupausen für den fachlichen Aufbau einer kompletten Anwendungslandschaft einer Versicherung oder eines Telekommunikationsunternehmens. **Makro-Architekturmuster** werden in Kapitel 9 beschrieben.

Prozesse der IT-Unternehmensarchitektur

Prozesse: Abgesehen von den Managementprozessmustern in Kapitel 4, die jeweils zu einer Menge von Zielmustern (Kap. 3) passen, gibt es auch Prozessbausteine, die für das Management von IT-Unternehmensarchitekturen unabhängig von den Zielmustern eingesetzt werden.

EAM-Frameworks

Beim Design Ihrer speziellen Prozesse für das Management der IT-Unternehmensarchitektur in Ihrem Unternehmen werden Sie mit großer Wahrscheinlichkeit sogenannte **EAM-Frameworks** sowie weitere Frameworks für das **IT-Management** benutzen. Eine Auswahl der gebräuchlichsten Frameworks finden Sie in den Kapiteln 10 und 11. In einem ausführlichen Abschnitt über TOGAF (Abschnitt 10.2) erhalten Sie einen Überblick über das derzeit wichtigste EAM-Framework.

EAM-Tools

Werkzeuge für Enterprise Architecture Management: Früher oder später werden Sie ein **EAM-Werkzeug** einsetzen. In Kapitel 12 erfahren Sie, wo diese Werkzeuge herkommen, und erhalten Hinweise darauf, wie Sie das passende Werkzeug finden.

Pragmatik

Pragmatisches Vorgehen: Das Buch ist so geschrieben, dass Sie zunächst den kompletten erforderlichen »Lernstoff« vermittelt bekommen, auf dessen Grundlage dann Dinge, wie Lean EAM (Kap. 13), pragmatische Vorgehensweisen (Kap. 14) und Einführungspfade (Kap. 15), diskutiert werden können.

Lean und Agile EAM

In den ca. 10 Jahren seit der zweiten Auflage dieses Buches haben sich als Varianten **Lean EAM** und **Agile EAM** herausgebildet. Ziel der Anwendung von Lean-Prinzipien und agilen Prinzipien auf EAM ist es, ein überbürokratisches EAM im Elfenbeinturm zu vermeiden und stattdessen die Aktivitäten konsequent an der Wertschöpfung für das Unternehmen und an den Bedürfnissen der Betroffenen auszurichten. In Kapitel 13 wird gezeigt, dass der musterbasierte Ansatz mit solchen Über-

legungen sehr gut verträglich ist. In dem musterbasierten Ansatz finden sich sowohl die Muster, die man benötigt, um ein EAM »lean« auszugestalten, als auch solche, um es »agil« zu machen. Im Wesentlichen heißt das in beiden Fällen, Dinge wegzulassen, die nicht von den Stakeholdern benötigt werden.

Wenn Sie sich an einige **pragmatische Vorgehensweisen** halten, erleichtern Sie sich die Arbeit. Eine Auswahl finden Sie in Kapitel 14. Hier wird z. B. die Frage diskutiert, ob perfekte Ordnung (also null Heterogenität) wirklich sinnvoll ist oder wo pragmatische Grenzen liegen.

Einführungspfade

Wenn Ihre Stabsfunktion IT-Unternehmensarchitektur noch nicht etabliert ist, werden Sie sich fragen, wie Sie eine solche Funktion am sinnvollsten einführen. Hierzu finden Sie Informationen in Kapitel 15, Einführungspfade für IT-Unternehmensarchitektur.

Trends

Ausblick: In Kapitel 16 finden Sie zum Abschluss des Buches Aussagen zu Trends beim Management der IT-Unternehmensarchitektur.

Wie alles zusammenpasst: Abbildung 1–4 vermittelt Ihnen einen alternativen Überblick über die wesentlichen Zusammenhänge des Buches.

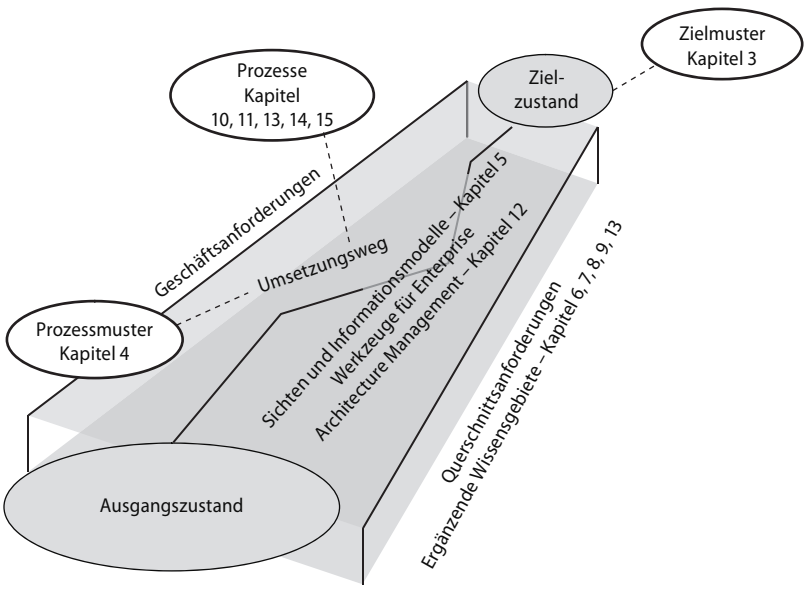


Abb. 1–4
Zusammenhang der Teile des Buches

Vom Istzustand …

Wenn Sie Verantwortung als IT-Unternehmensarchitekt übernehmen, werden Sie immer einen Ausgangszustand Ihrer IT-Landschaft vorfinden. In Kapitel 4 zu Prozessmustern finden Sie u. a. Hinweise dazu, wie man diesen Ausgangszustand beschreiben kann. Sehr häufig wird dazu ein EAM-Werkzeug (Kap. 12) eingesetzt, um die Daten über die existierende IT-Landschaft zu erfassen. In welcher Intensität dies geschieht,

hängt allerdings von den Zielen ab (Zielmuster, siehe Kap. 3), die Sie mit Ihrer Initiative zur IT-Unternehmensarchitektur verfolgen.

… zum Zielzustand

Der Zielzustand, den Sie für jede Periode strategischer Planung herbeiführen wollen, ist davon abhängig, welche Ziele Sie und Ihre Unternehmensleitung mithilfe von IT-Unternehmensarchitektur erreichen wollen. Auch für Ziele gibt es Muster, die man in vielen Unternehmen finden kann. Solche **Zielmuster**, die in vielen Unternehmen in ähnlicher Form angestrebt werden, finden Sie in Kapitel 3.

Managementprozessmuster

Sie werden sich dann für einen Weg entscheiden, wie Sie vom Ausgangszustand in den Zielzustand gelangen können. Dazu haben sich **Managementprozessmuster** bewährt (siehe Kap. 4).

Für die Umsetzung dieser Managementprozesse benötigen Sie Informationen über den Zustand Ihrer IT-Landschaft. Diese werden normalerweise in Sichten aggregiert. Beispiele für solche Sichten sind z.B. sogenannte Softwarekarten, auf denen der Zustand einer IT-Landschaft schnell erfasst und dokumentiert werden kann. Für die Erstellung solcher Karten benötigt man eine Informationsbasis, bestehend aus **Sichten** und **Informationsmodellen**. Eine solche Informationsbasis beinhaltet normalerweise ein Metamodell. In Kapitel 5 finden Sie u.a. Hinweise auf Musterkataloge für Sichten und wie Sie sich anhand von Mustern ein Metamodell für eine passende Informationsbasis zusammenstellen können. So viel sei hier schon vorweg gesagt: Nicht jedes Unternehmen wird dasselbe Metamodell einsetzen. Die Menge an Informationen ist abhängig von den Zielen, die Sie mit Ihrer IT-Unternehmensarchitektur erreichen wollen. Es ist nicht immer sinnvoll, das größtmögliche Metamodell einzuführen, und es ist überhaupt nicht sinnvoll, das größtmögliche Metamodell vollständig mit Informationen zu füllen.

Informationsbasis

Leitplanken

Auf dem Weg vom Ausgangszustand zum Ziel finden Sie zwei Sätze von Leitplanken: Dies sind zum einen die geschäftlichen Anforderungen des Unternehmens, zum anderen die Querschnittsanforderungen, die im Teil über **ergänzende Wissensgebiete** beschrieben sind. Dabei handelt es sich quasi um nicht funktionale Anforderungen wie **Compliance**, **IT-Sicherheit** und **Cybersicherheitsarchitektur** sowie die Ergebnisse des **IT-Risikomanagements** (Kap. 6 bis 8). Sowohl die funktionalen als auch die nicht funktionalen Anforderungen müssen in Ihre Lösungen einfließen.

Compliance

IT-Sicherheit/Cybersicherheitsarchitektur

Risikomanagement

Weitere Hilfsmittel unterstützen Sie dabei, Ihren Weg von der Ausgangssituation zum Ziel erfolgreich zu gehen. **Makro-Architekturmuster** (Kap. 9) können Sie verwenden, um den Zielzustand detailliert zu beschreiben, sofern es sich um Architekturen handelt und nicht um die Veränderung von Kennzahlen (wie z.B. IT-Kosten pro Umsatz). Allge-

meine Prozessmuster, wie z. B. **pragmatische Vorgehensweisen** (Kap. 14), helfen Ihnen, den Weg schneller zu gehen. Auch aus **EAM-Frameworks** (Kap. 10 und 11) und sonstigen **IT-Management-Frameworks** können Sie viele nützliche Anregungen ziehen, um schnell ans Ziel zu gelangen, indem Sie Dinge wiederverwenden und nicht neu erfinden müssen. Und **EAM-Werkzeuge** (Kap. 12) helfen Ihnen dabei, Ihre Informationsbasis zu verwalten. Wenn Sie es nur mit einer zweistelligen Anzahl von Anwendungen zu tun haben sollten, kann die Werkzeugunterstützung geringer ausfallen. Wenn Sie allerdings für ein internationales Großunternehmen tätig sind, werden Sie mit einer vierstelligen Anzahl von Applikationen rund um den Erdball zu tun haben und nicht darum herumkommen, ein umfangreicheres Werkzeug einzusetzen.

EAM-Frameworks

EAM-Tools

Je nachdem, welche Ziele Sie verfolgen (also mit welchen Zielmustern Sie es zu tun haben), werden Sie an unterschiedlichen Enden des Unternehmens anfangen, IT-Unternehmensarchitektur einzuführen. Kapitel 15 zu **Einführungspfaden** wird Ihnen Hinweise dazu geben, welche Wege zu welchen Zielkombinationen passen.

Einführungspfade

1.3 Wer sollte dieses Buch lesen und warum?

Zielgruppen

Dieses Buch wendet sich primär an IT-Unternehmensarchitekten, ihre Vorgesetzten (IT-Gesamtverantwortliche, CIOs) sowie an IT-Mitarbeiter, die eine Karriere als IT-Unternehmensarchitekt ins Auge gefasst haben. Nachdem IT-Unternehmensarchitektur in Projektmodellen heute allerdings immer breiter verankert wird (die meisten Vorgehensmodelle großer Konzerne verweisen auf Checkpoints zur IT-Unternehmensarchitektur), sollten auch Projektleiter in Großunternehmen zumindest über Grundwissen zu Methoden und Vorgehensweisen der IT-Unternehmensarchitektur verfügen. Jeder, für den IT-Management einen Schwerpunkt seiner Aufgaben darstellt, sollte wenigstens in groben Umrissen wissen, wie die Kollegen »Unternehmensarchitekten« arbeiten, so wie jeder Entwickler über Grundlagenwissen zur Softwarearchitektur verfügen sollte.

Im Folgenden wird beschrieben, für welche Unternehmenstypen und für welche Leserkreise welche Kapitel besonders interessant sein können und warum.

1.3.1 Eine Frage der Unternehmensgröße?

Großunternehmen

Die Methoden und Verfahren für IT-Unternehmensarchitektur haben sich Ende der 1990er- und Anfang der 2000er-Jahre in Großunternehmen für Großunternehmen entwickelt. Damals gab es zwar schon die DotCom-Blase. Erfolgreiche sogenannte »exponentielle Unternehmen«, so wie wir sie heute beispielsweise in Form von UBER oder Airbnb beobachten können, gab es damals noch nicht. Als IT-Anwenderunternehmen gab es damals neben den Großunternehmen vor allem Mittelständler. Mittelständische Unternehmen können die in diesem Buch geschilderten Methoden ebenfalls einsetzen. Viele Rollen werden dort allerdings in Personalunion ausgefüllt.

Öffentliche Verwaltung

Zunehmend werden die hier vorgestellten Vorgehensweisen auch in der öffentlichen Verwaltung verwendet – in den USA sind sie für weite Teile der öffentlichen Verwaltung sogar gesetzlich vorgeschrieben. Solche Unternehmen oder Institutionen sind gekennzeichnet durch Milliardenumsätze und/oder IT-Budgets ab einem hohen zweistelligen Millionen-Euro-Bereich. Der größte Auftraggeber für Software weltweit ist das Department of Defense mit einem dreistelligen Milliarden-US-Dollar-Volumen, das jährlich für Software ausgegeben wird. Das Department of Defense hat daher mit DoDAF (Department of Defense Architecture Framework) sogar ein eigenes sehr umfangreiches Architekturframework entwickelt. In großen Behörden sind Methoden der IT-Unternehmensarchitektur mittlerweile in unterschiedlichen Ausprägungen und flächendeckend anzutreffen. Kritisch ist jedoch gerade in der Verwaltung, dass EAM nicht zu einer formalen Übung ausarten darf. Vor allem hier kann es also sinnvoll sein, die geübte Praxis gegen die Ansätze von Lean EAM und agilem EAM zu reflektieren, die in Kapitel 13 beschrieben werden.

Mittelstand

Der Einsatz im Mittelstand unterscheidet sich vor allem durch die Personalausstattung und die Größe und Komplexität der Anwendungsportfolios. Ein CIO eines größeren mittelständischen Unternehmens ist z. B. für ein Gesamt-IT-Budget von 30 Mio. Euro oder US-Dollar verantwortlich – bei beispielsweise 2 Mrd. Euro Umsatz des von ihm mit IT betreuten Unternehmens. Davon entfällt dann ca. 1/3, also 10 Mio. Euro, auf Beschaffung und Wartung der 20 Applikationspakete, oft Standardprodukte und zunehmend auch SaaS (Software as a Service). Ein solcher CIO wird zwar »im Kopf« Methoden der IT-Unternehmensarchitektur verwenden. Er wird in der Regel aber keinen »IT-Unternehmensarchitekten« einstellen, sondern die Aufgaben entweder selbst quasi im Kopf miterledigen – oder aber er wird einen erfahrenen Lösungsarchitekten beschäftigen, der die Aufgaben der IT-Unternehmensarchitektur mit erledigt.

Start-ups

Heute gibt es auch noch die sogenannten exponentiellen Unternehmen, die dadurch charakterisiert sind, dass sie exponentiell wachsen. Unter ihnen finden sich zahlreiche »Einhörner«. Das sind Start-ups, die mit mehr als einer Milliarde Euro oder US-Dollar Unternehmenswert eingeschätzt werden. Oft betreiben solche Unternehmen zwar IT für sehr viele Benutzer – allerdings im Wesentlichen in Form einer sogenannten »One Page Application« für viele Plattformen (diverse Browser, iOS, Android). Aufgrund der hohen Benutzerzahlen benötigen solche Unternehmen zwar eine wirklich gute Lösungsarchitektur für ihre eine oder ganz wenigen Anwendungen. Sie benötigen aber in vielen Fällen keine Unternehmensarchitektur.

Zusammenfassend kann man Folgendes festhalten: In Großunternehmen wird IT-Unternehmensarchitektur nach wie vor angewendet und hat dort auch eine ähnliche Bedeutung wie vor 10–15 Jahren. Viele Mittelständler können die Methoden verwenden. Start-ups mit hohen Benutzerzahlen und wenigen IT-Anwendungen benötigen vor allem eine sehr ausgefeilte Lösungsarchitektur.

1.3.2 IT-Unternehmensarchitekten

IT-Unternehmens-architekten

Das Buch ist primär für IT-Unternehmensarchitekten geschrieben. Wenn Sie in diesem Buch direkt angesprochen werden, dann versetzen Sie sich bitte in die Rolle eines IT-Unternehmensarchitekten. Als solcher erhalten Sie Hinweise, wie Sie Ihren Job so gestalten können, dass er nicht »gefährlich« wird, sondern dass Sie darin erfolgreich werden. Sehr erfahrene IT-Unternehmensarchitekten, die den Job gut beherrschen, werden in diesem Buch lediglich die Bestätigung finden, dass sie sich im Rahmen von »Good Practices« bewegen. Dramatisch Neues werden Sie nicht lernen – eben, weil sich das Feld auch konsolidiert. Wenn Sie auf Dinge treffen, die Sie schon kennen, können Sie diese Themen ja schnell diagonal überfliegen. Unternehmensarchitekten »in Ausbildung« werden von dem Buch deutlich mehr profitieren. Als IT-Unternehmensarchitekt sollte man tendenziell den kompletten Inhalt des Buches kennen – und noch eine Menge weiterer Wissensgebiete, die meist im Buch auch referenziert werden.

Schwerpunkt IT-Management

Das Buch legt einen Schwerpunkt auf die IT-Management-Perspektive und nicht oder nur am Rande auf technische Architekturen und Lösungsarchitekturen. In den Kapiteln zu Zielmustern (Kap. 3) und Managementprozessmustern (Kap. 4) finden Sie wesentliches Managementwissen, das Sie benötigen, um die IT-Funktionen eines großen Unternehmens an den Geschäftszielen auszurichten.

Compliance
IT-Sicherheit/Cybersicherheitsarchitektur
Risikomanagement

Die Bereiche Compliance (Kap. 6), IT-Sicherheit und Cybersicherheitsarchitektur (Kap. 7) sowie IT-Risikomanagement (Kap. 8) sind für Sie insofern wichtig, als sie deutlich machen, dass es neben den eher funktionalen Anforderungen der Ausrichtung Ihrer IT auf den Geschäftszweck Ihres Unternehmens eine immer wichtiger werdende Menge nicht funktionaler Anforderungen gibt, die Sie nicht aus den Augen verlieren dürfen. Eine Nichtbeachtung kann schlicht dazu führen, dass Ihr Unternehmen in seiner Existenz gefährdet wird. Auch wenn Sie als IT-Unternehmensarchitekt nicht der primäre Verantwortliche z. B. für Sicherheitsfragen im Unternehmen sind, dürfen Sie trotzdem keine Architektur genehmigen, die nicht allen Sicherheitsanforderungen Ihres Unternehmens genügt. Sie benötigen daher ein ähnlich tiefes Wissen über Sicherheitsfragen wie z. B. der IT-Sicherheitsbeauftragte Ihres Unternehmens. Ähnliches gilt auch für die Themen Compliance und IT-Risikomanagement. Sie müssen in der Lage sein, in Reviews frühzeitig Verstöße gegen Gesetze zu erkennen sowie auch bei der Beurteilung Ihres bestehenden Anwendungsportfolios IT-Risiken zu sehen und sinnvoll zu erfassen.

Prozesse
Frameworks
Werkzeuge

Der Rest des Buches, die Blöcke über Prozesse, Frameworks und Werkzeuge, wird Ihnen viele nützliche Hinweise für Ihre Tagesarbeit geben. Makro-Architekturmuster (Kap. 9) dürften den meisten IT-Architekten schon vertraut sein. Sie werden hier trotzdem erläutert, um ihren Nutzen zu demonstrieren. In einem Kapitel über pragmatische Vorgehensweisen (Kap. 14) finden Sie nützliche Hinweise, die Ihnen die tägliche Arbeit als IT-Unternehmensarchitekt erleichtern. Zum Beispiel wird dort die Frage diskutiert, wie viel Ordnung (Homogenität) ein Unternehmen überhaupt benötigt. Es wird weiter erläutert, welche Budgetausstattung eine Stabsstelle für IT-Unternehmensarchitektur üblicherweise zur Verfügung haben sollte. Auch finden Sie in diesen Kapiteln eine Diskussion über verbreitete Architekturframeworks wie auch sonstige Frameworks, die im Kontext des IT-Managements heute verbreitet sind und die ein Unternehmensarchitekt folglich in Grundzügen kennen sollte. Früher oder später werden Sie als IT-Unternehmensarchitekt damit konfrontiert werden, ein EAM-Werkzeug aussuchen und einführen zu müssen. Hinweise hierzu enthält das Kapitel 12.

Einführungspfade

Ebenfalls häufig werden Sie mit der Frage befasst sein, wie man eine Funktion für IT-Unternehmensarchitektur im Unternehmen einführen und verankern kann. Standardpfade hierzu beschreibt Kapitel 15.

1.3.3 Verantwortliche für Business Development

IT-Alignment

Auf der Geschäftsseite gibt es häufig Einheiten, die sich mit dem Finden und Umsetzen neuer Geschäftsmodelle befassen. In diesem Buch wird an mehreren Stellen deutlich, dass man massive Zeitvorteile erreichen kann, wenn man Geschäfts- und IT-Seite neuer Produkte und Services simultan plant und entwickelt. Dafür ist es sinnvoll, dass IT-Unternehmensarchitekten die Methoden und Vorgehensweisen der Kollegen kennen, die für Business Development verantwortlich sind. Umgekehrt ist es aber auch sinnvoll, wenn diese Kollegen ein Grundwissen in IT-Planung und speziell IT-Unternehmensarchitektur haben. Langfristig werden beide Kompetenzbereiche tendenziell zusammenwachsen. In fortschrittlichen Unternehmen ist dies bereits geschehen. Geschäftsarchitekten sollten daher heute schon mindestens über ein Grundwissen in IT-Unternehmensarchitektur verfügen.

1.3.4 IT-Vorstände, CIOs und CDOs

IT-Verantwortliche

Als IT-Vorstand bzw. IT-Gesamtverantwortlicher gibt Ihnen dieses Buch Hinweise dazu, wie Sie IT-Unternehmensarchitektur für den eigenen Erfolg einsetzen können. Dies gilt auch für die modernere Form des sogenannten CDO (Chief Digital Officers), der digitale Geschäftsmodelle vorantreiben soll. Ein IT-Unternehmensarchitekt kann eine wesentliche Stütze für Sie sein. Um ihn auszuwählen und gut zu führen, hilft es, die Methoden und Standardaufgaben zu kennen, die er beherrschen sollte. Daher ist dieses Buch auch für IT-Vorstände nützlich.

Zielmuster
Managementprozessmuster

Als IT-Gesamtverantwortlicher sind für Sie vor allem die Kapitel über Zielmuster (Kap. 3) und Managementprozessmuster (Kap. 4) von Interesse. Sie können hier zusammen mit Ihrem IT-Unternehmensarchitekten festlegen, welche Prioritäten er für seine Arbeit setzen soll. Themen wie Sichten und Informationsmodelle (Kap. 5) sind für Sie als Topmanager weniger von Interesse, weil sie das Handwerk Ihres Mitarbeiters betreffen.

Ebenso werden Sie mit Querschnittsanforderungen (Compliance, IT-Sicherheit/Cybersicherheitsarchitektur und IT-Risikomanagement) im Regelfall operativ nichts zu tun haben wollen. Sie werden diese Themen sauber delegieren und lediglich periodisch sicherstellen, dass sie ordnungsgemäß abgehandelt werden, sodass Sie im Problemfall nachweisen können, dass Sie sich mit der notwendigen Sorgfalt darum gekümmert haben. Kapitel 6 bis 8 dieses Buches bieten einen schnellen Überblick und sind als Zusammenfassungen für das Management geeignet.

Auch die Kapitel über Hilfsmittel (Kap. 9 bis 14) gehören nicht notwendigerweise zu Ihrem Aufgabengebiet als IT-Verantwortlicher. Sie werden höchstwahrscheinlich auch diese Aufgaben delegieren.

Einführungspfade

Interessant für Sie sind Überlegungen zu Einführungspfaden in Ihre IT-Unternehmensarchitektur (Kap. 15), wenn eine solche Funktion in Ihrem Unternehmen noch nicht oder noch nicht in vollem Umfang existiert und Sie eine entsprechende Stelle erst schaffen oder massiv ausbauen wollen.

1.3.5 Softwarearchitekten

Softwarearchitekten

Das Erste, was Sie als Softwarearchitekt bei der Lektüre dieses Buches bemerken werden, ist, dass die Methoden, mit denen IT-Unternehmensarchitekten arbeiten, komplett andere sind als diejenigen, mit denen Sie als Lösungsarchitekt arbeiten, wenn Sie sich mit der Softwarearchitektur für ein größeres System befassen – aber eben nicht mit der Planung für 200, 1000 oder noch mehr Systeme.

Compliance

Ein von mir sehr geschätzter Kollege und erfahrener Softwarearchitekt äußerte sich mir gegenüber einmal so, dass ihn dieses »ganze BWL-Konzeptzeugs« nicht interessiere und er speziell das Kapitel 6 über Compliance extrem langweilig finde. Dazu muss man leider sagen, dass mit diesem »BWL-Konzeptzeugs« über die Zukunft ganzer Systemcluster entschieden wird, an denen jeweils auch Arbeitsplätze hängen. Wenn man also nicht eines Morgens unvorbereitet vor der Situation stehen möchte, dass das eigene System »wegrationalisiert« oder »wegkonsolidiert« wurde, ist es sinnvoll, die Methoden der Leute zu kennen, die solche Entscheidungen mit vorbereiten – also die Methoden von IT-Unternehmensarchitekten oder Unternehmensberatern. Und auch Compliance ist kein so langweiliges Thema: Wer einmal die Freude hatte, als Architekt negativ in einem Revisionsbericht erwähnt worden zu sein, der für den Vorstandsvorsitzenden des Zentralvorstands eines globalen Konzerns bestimmt war, wird das Thema nicht mehr so langweilig finden. Speziell dann, wenn der Vorstand aus dem Bericht erfahren hatte, dass er für die dort aufgelisteten Mängel persönlich haftbar gemacht werden könnte. Der entsprechende Vorstand wird Ihnen glaubhaft vermitteln können, dass Sie sich für Revisionsberichte besser interessieren sollten, wenn Sie in der Firma bleiben möchten.

IT-Strategie

Softwarearchitekten sollten ebenso wie auch IT-Unternehmensarchitekten tendenziell das ganze Buch lesen. Wissen über strategische Prozesse schadet nicht, auch wenn es nicht zu Ihrem Tagesgeschäft gehört. Es kann Ihnen auch als Softwarearchitekt, der nur für ein System eines kompletten Anwendungsportfolios verantwortlich ist, helfen, die

Methoden und Arbeitsweisen der Kollegen zu kennen, die Ihr Projekt auf Verträglichkeit mit den Unternehmensrichtlinien überprüfen. Ihnen ist dann die Motivation der Kollegen bekannt, Sie wissen, mit welchen Mitteln sie arbeiten, was sie im Sinne des Gesamtunternehmens akzeptieren dürfen und was nicht. Und Sie erkennen auch, warum diese Kollegen nicht dafür verantwortlich sind, sozusagen als »Überarchitekten« Ihren Job zu machen. Mancher Softwarearchitekt wird sich auch später in einer IT-Unternehmensarchitektur-Funktion wiederfinden. Es ist dann gut, vorher zu wissen, dass die Aufgaben und Erfolgsfaktoren komplett verschieden sind, auch wenn es reichlich Schnittstellen und Berührungspunkte zwischen IT-Unternehmensarchitektur und Projektarchitektur gibt.

Kollegen verstehen

1.3.6 Alle anderen IT-Mitarbeiter

IT-Mitarbeiter

Alle anderen Mitarbeiter der IT-Funktionen von Anwenderunternehmen können von diesem Buch profitieren, weil es hilfreich ist, zu erfahren, wie eine IT-Funktion langfristig von der Geschäftsseite gesehen wird. Man lernt dann zu verstehen, warum über Outsourcing nachgedacht wird, welche Antriebskräfte einen IT-Vorstand zu gewissen Handlungen veranlassen und in welcher Art Unternehmen oder Unternehmenskultur man sich befindet.

Wenn man die fünfte Gruppe »alle anderen IT-Mitarbeiter« außen vor lässt, dann können ca. 10–15 Prozent des IT-Personals von diesem Buch unmittelbar profitieren. In etwa so hoch ist der Anteil von Unternehmens- und Projektarchitekturfunktionen am gesamten IT-Personal. Die Tendenz ist steigend, weil mit wachsendem Anteil an Outsourcing und Standardsoftware (abnehmender Wertschöpfungstiefe) der Anteil der Planungsaufgaben gegenüber reinen Implementierungstätigkeiten zunimmt.

1.3.7 Studierende

Einsatz an Hochschulen

Die erste bis dritte Auflage dieses Buches wurden bereits erfolgreich als Grundlage für Lehrveranstaltungen zu EAM oder IT-Management an verschiedenen Hochschulen eingesetzt. Auch der Autor hat basierend auf seinem Buch insgesamt vier Lehrveranstaltungen im Masterstudium des Hasso-Plattner-Instituts der Universität Potsdam durchgeführt.

1.4 Wie können Sie dieses Buch lesen?

IT-Profis

Dieses Buch ist primär für berufserfahrene IT-Profis geschrieben. Es kann jedoch auch von Berufsanfängern gelesen werden. Auf diese wird allerdings bei der Didaktik nicht immer Rücksicht genommen, da im Sinne des guten Leseflusses die für Profis in der IT allgemein bekannten Basisbegriffe nicht ausführlich definiert werden. Dies geschieht eher kurz in Form von Fußnoten mit weiterführenden Literaturhinweisen. Dieses Buch hat den Anspruch, dass jedes Kapitel für sich sinnvoll gelesen werden kann, damit Sie als Leserin und Leser die Aspekte herausgreifen können, die für Sie neu und interessant sind. Es ist daher so geschrieben, dass man einzelne Kapitel detailliert, andere nur diagonal liest und das Buch dann später zum Nachschlagen wieder »hervorholen« kann.

1.5 Einige Besonderheiten

Sprache

Wenn man ein Buch wie dieses schreibt, denkt man länger darüber nach, ob man es in Deutsch oder »gleich« in Englisch schreiben soll. Englisch hat den Vorteil, dass viele bekannte Begriffe nicht übersetzt werden müssen, dass »denglische« Texte vermieden und potenziell ein größerer Leserkreis erreicht werden kann.

1.5.1 Sprache: Deutsch

Deutsch hat den Vorteil, dass Leserinnen und Leser, die mit der englischen Fachsprache nicht so vertraut sind, das Buch schneller durchlesen können. Ich habe mich also im Sinne der Leserschaft für Deutsch entschieden. Das hat allerdings auch Nachteile, z. B. dass man dabei mit Wortmonstern hantieren muss, die man eigentlich im Sinne eines flüssigen Schreibstils gerne vermeiden würde. Es reicht in diesem Buch beispielsweise nicht aus, einfach »Architektur« zu schreiben, weil in der deutschen Fachsprache im Gegensatz zur englischen zwischen Begriffen wie IT-Architektur, IT-Unternehmensarchitektur oder Geschäftsarchitektur zu unterscheiden ist.

Wenn Sie aus der Beraterwelt vertraute Begriffe wie CIO, CFO, CxO, C-Level Officer, Challenge, Cost Cutting und ähnliche manchmal etwas sparsam eingesetzt sehen, hat das nichts damit zu tun, dass der Autor sie nicht auch beherrscht – sie wurden nur bewusst reduziert verwendet, um das Buch nicht mit englischen Akronymen zu überladen.

1.5.2 Verwendung von Wikipedia-Definitionen

Definitionen

Ein weiteres Thema ist der Umgang mit Definitionen. Das Buch enthält mehrere Definitionen aus Wikipedia. Über den Ruf von Wikipedia kann man sicher diskutieren, im Falle der Auswahl der Begriffe in diesem Buch waren diese Definitionen jedoch oftmals die instruktivsten. So erschien es sinnvoller, sie zu verwenden, als sie mit Gewalt durch andere, unverständlichere zu ersetzen. Die Wikipedia-Definitionen wurden gründlich plausibilisiert und auch nur dann verwendet, wenn keine andere gut erreichbare Quelle zur Verfügung stand.

1.6 Was sich seit der ersten Auflage geändert hat

Die erste Auflage dieses Buches repräsentierte den Kenntnisstand der IT-Unternehmensarchitektur von 2006. Die vierte Auflage, die Sie hier vor sich haben, ist 2024 erschienen – 18 Jahre später, was in der IT eine »halbe Ewigkeit« ist.

Musterbasierter Ansatz

Seit damals hat nicht nur die Bedeutung und Verbreitung des Themas IT-Unternehmensarchitektur stark zugenommen. Durch Forschungsarbeiten hat sich auch der Blick auf die Systematik und das Raster geändert, mit dem das Gebiet heute (2024) dargestellt werden kann. Dies hatte starke Auswirkungen auf die Struktur und den Umfang der zweiten Auflage, die 2011 entstand. Zwischen 2011 und 2016 hat sich im Kernfeld der IT-Unternehmensarchitektur nicht dramatisch viel verändert. Geändert hat sich vor allem, dass nun auch auf der Geschäftsseite etwas entsteht, was als »Enterprise Business Architecture« [Sensler+15] bezeichnet wird, und dass es mit den exponentiellen Unternehmen einen neuen Typus sehr teurer Unternehmen mit sehr vielen Benutzern gibt, die interessant zu betrachten sind [Ismail+14]. Nach weiteren sieben Jahren von 2016 bis 2023 war es vor allem wichtig, die Bezüge zu wichtigen Frameworks wie TOGAF 10 (2022), COBIT 2019 oder ITIL 4 (2019) zu überarbeiten, die in diesem Zeitraum aktualisiert wurden.

Ordnungsprinzip
Muster

Als grundlegendes Ordnungsprinzip wird seit der zweiten Auflage nicht mehr nur die Prozesslandkarte für das Architekturmanagement verwendet, die in einer früheren Form der ersten Auflage zugrunde lag. Es wird stattdessen eine eher modulare und auf Mustern basierende Herangehensweise an das Thema gewählt (zur Erläuterung siehe Abschnitt 2.3). Sie beruht auf Forschungsarbeiten der Technischen Universität München zu EAM-Patterns. Dieser musterbasierte Ansatz ist zu der ursprünglichen Darstellung einer Prozesslandkarte hinzugekommen und erlaubt ein feineres Anpassen einer IT-Unternehmensarchitektur-Funktion an die Ziele des jeweiligen Unternehmens. Die in den letzten

10 Jahren aufgetauchten Variationen Lean EAM und Agile EAM sind damit ebenfalls gut verträglich (siehe dazu Kap. 13).

Als IT-Unternehmensarchitekt haben Sie es somit einfacher, sich die Aspekte herauszusuchen, die Sie genau in Ihrem Unternehmen für die Ziele Ihrer IT-Funktion benötigen. Dieses Vorgehen spiegelt sich wider in den Kapiteln über Zielmuster (Kap. 3), Managementprozessmuster (Kap. 4) sowie Sichten und Informationsmodelle (Kap. 5). An Prozessmustern ist vor allem das Management von Business-IT-Alignment mit Capabilities (Abschnitt 4.2) vergleichsweise neueren Datums.

SOA

Von ca. 2005 bis ca. 2017 ist eine SOA-Welle über die Unternehmen geschwappt: Manche mögen sagen, dass SOA tot sei. Tatsache ist jedoch, dass gerade große Unternehmen heute ein Service Portfolio Management (Abschnitt 4.8) betreiben und dies nicht im Sinne von ITIL, sondern in Form von SOA-Diensten, die analog zu Anwendungsportfolios gemanagt werden müssen. Hier gibt es auch Querbezüge zum Management von Geschäftsprozessen und auch zu den moderneren Ausprägungen von serviceorientierten Architekturen, die in Abschnitt 13.3 beschrieben sind. Wenn Sie heute IT-Profis nach SOA fragen, kann es sein, dass man Ihnen sagen wird, das sei ja »komplett veraltet«, weil die Literatur dazu ca. 15 Jahre alt ist. Leider wird das API-Management moderner Microservice-Architekturen nicht ähnlich breit diskutiert wie einstmals SOA, sodass es schwer ist, die damalige Diskussion so zu aktualisieren, dass dies dann wirklich auf breiter praktischer Erfahrung beruht.

Compliance

Der Compliance-Druck auf die Unternehmen nimmt stetig zu. Das Buch trägt dem dadurch Rechnung, dass dieser Aspekt immer wieder betont wird. In Kapitel 6 über Compliance werden Compliance-Frameworks erläutert. Solche unternehmensweiten Frameworks für das Compliance-Management sind durch die Korruptionsskandale stark gefördert worden. Das Kapitel über Compliance kann jedoch nur Denkanstöße geben. Den Anspruch, sämtliche Rechtsgrundlagen aufzulisten, haben nicht einmal Spezialwerke zum Thema. Diese (wie auch das vorliegende Buch) können nur Hilfestellung zum Auffinden der Rechtsgrundlagen geben, die für die verschiedenen Branchen und Länder relevant sind.

IT-Sicherheit/Cybersicherheitsarchitektur

Ebenso hat der Druck auf die Themen IT-Sicherheit und Cybersicherheitsarchitektur noch weiter zugenommen. Das Kapitel zu diesen Themen (Kap. 7) wurde daher für jede Auflage überarbeitet und ist stark gewachsen. Es wurde mit Florian Oelmaier von einem anerkannten Experten auf diesem Gebiet beigesteuert. In der ersten Auflage wurden lediglich Frameworks für die IT-Sicherheit aufgeführt. Doch die Themen IT-Sicherheit und Cybersicherheitsarchitektur haben heute so stark an Bedeutung gewonnen, dass man als IT-Architekt und IT-Unternehmensarchitekt auch dazu tiefere Kenntnisse benötigt.

Risikomanagement

Dasselbe gilt für das IT-Risikomanagement (Kap. 8). Auf diesem Gebiet sind die Unternehmen in den letzten 15 Jahren deutlich rigider geworden. Große Lösungsarchitekturen werden jetzt in Form von Makro-Architekturmustern abgehandelt. Darunter fallen auch sogenannte Blueprints und Facharchitekturen.

Pragmatik

Die Aussagen über pragmatische Vorgehensweisen für IT-Unternehmensarchitekten (Kap. 14) sind nach wie vor gültig. Hier hat es lediglich eine größere Änderung gegeben, nämlich die Behandlung von Lean und Agile EAM. Fragen, wie beispielsweise »wie viel Ordnung sein muss – und wie viel Unordnung man sich noch erlauben kann«, sind von aktuellen Entwicklungen relativ unabhängig und werden daher seit der ersten Auflage im Wesentlichen unverändert behandelt.

TOGAF

In den Kapiteln 10 und 11 finden Sie Informationen zu Frameworks für die IT-Unternehmensarchitektur und die IT im Allgemeinen. Hier fällt vor allem die tiefer gehende Behandlung von TOGAF 10th Edition ins Gewicht. Das TOGAF-Framework hat sich zu einem Quasistandard für Unternehmensarchitektur-Frameworks entwickelt, auch wenn es viele Gebiete nicht abdeckt, die ein Buch zu IT-Unternehmensarchitektur abdecken muss, wie etwa IT-Strategie und Anwendungsportfoliomanagement, um zwei Beispiele zu nennen. Dies ist ein Grund, ausführlich zu diskutieren, welche Felder des kompletten Gebiets der IT-Unternehmensarchitektur durch TOGAF 10th Edition abgedeckt werden.

COBIT

Die Inhalte zu sonstigen IT-Management-Frameworks wie z. B. ITIL sind relativ stabil geblieben, wobei Aktualisierungen berücksichtigt wurden. 2019 wurde wieder ein umfangreich überarbeitetes COBIT-Framework in der Version COBIT 2019 herausgegeben. Die hier vorliegende vierte Auflage setzt daher komplett auf COBIT 2019 auf und nicht mehr auf COBIT 5.

EAM-Tools

An der Art und Weise, wie man EAM-Werkzeuge evaluiert, hat sich seit der ersten Auflage wenig verändert. Kapitel 12 konnte ohne wirklich drastische Änderungen fortgeschrieben werden. Die Eigenschaften der Werkzeuge wurden zwar weiterentwickelt, aber grundlegend haben sie sich nicht geändert. Die Toolstudien der Technischen Universität München wurden nach 2008 nicht mehr fortgeführt. Dafür wurde eine neuere Toolstudie der Firma Syracom verwendet [Ehrlich+15]. Der EAM-Thinktank, der diese Studie veröffentlicht hat, wurde als Kooperation zweier Beratungsfirmen (NovaTec und Syracom) weitergeführt. Wesentliche Updates hat es aber nicht gegeben. Der jeweils aktuelle Gartner Magic Quadrant für EAM-Tools [Gartner22] zeigt zwar, welche EAM-Tools Gartner für die fortschrittlichsten hält. Gartner legt aber seine Bewertungskriterien bei Weitem nicht so weit offen, wie das die Technische Universität München mit ihren Toolstudien [sebis08a] getan hat.

Die für die vierte Auflage erforderlichen Änderungen spiegeln die relative Stabilität des Fachgebiets »IT-Unternehmensarchitektur« wider. Die aufwendigsten Updates waren bei den Bezügen zu den großen Frameworks TOGAF 10 (2022), COBIT 2019 oder ITIL 4 (2019) notwendig. Einen Schub gibt es noch auf dem Gebiet der Enterprise Business Architecture (siehe z.B. [Sensler+15], [Simon+15]) durch die Digitalisierung von Geschäftsmodellen. Um diese zu beschreiben, benötigt man Enterprise Business Architecture, auf die in diesem Buch nur am Rande eingegangen wird. In Abschnitt 10.2 zu TOGAF 10th Edition wird jedoch im Kontext mit TOGAF auf Material dazu verwiesen.

7 Cybersicherheitsarchitektur

Von Florian Oelmaier

Cybersicherheit als Kernprozess im Unternehmen

Spätestens die Bedrohung durch Ransomware hat das Thema Cybersicherheit in jedes Managementgremium getragen [Oelmaier+23]. Die Bedrohung durch die digitale Transformation der organisierten Kriminalität und deren neue »Geschäftsmodelle« betrifft ausnahmslos jedes Unternehmen. Dies ist jedoch nicht die einzige Herausforderung: Es gibt eine Vielzahl anderer Tätergruppen mit anderen Vorgehensweisen. Zeitgleich ist jedes Unternehmen gefordert, mit den digitalen Geschäftsmodellen und der Weiterentwicklung der IT-Technologie Schritt zu halten und seine Unternehmensarchitektur auf einem modernen Stand zu halten. Die Basis für diese Weiterentwicklung muss ein solides Fundament im Bereich Cybersicherheit sein. Wie eine Risiko-Nutzen-Abwägung im Allgemeinen durchzuführen ist, wird auch noch in Kapitel 8 zu IT-Risikomanagement erläutert.

Zugleich haben auch die Gesetzgeber und Regulatoren das Thema Cybersicherheit als wichtigen Zukunftsfaktor für ganze Wirtschaftsräume identifiziert. Die Anzahl der relevanten Industriestandards, Verordnungen und Gesetze zur IT-Sicherheit hat sich vervielfacht. Angefangen mit der DSGVO/GDPR wurde zudem begonnen, die Regelwerke mit empfindlichen Strafen zu belegen. Entsprechend hat die Cybersicherheit mittlerweile zwei Aufgaben: Bedrohungsabwehr und Compliance.

Chief Information Security Officers vs. IT-Unternehmensarchitekten

Die meisten Unternehmen tragen dieser Aufgabenkomplexität Rechnung, indem sie die Position eines Chief Information Security Officer (CISO) schaffen. Der CISO hat viele dringende Aufgaben. Er muss mit seiner Abteilung die nahezu täglich auftretenden kleineren Sicherheitsvorfälle im Auge behalten und daraus die Anfänge größerer Angriffe herausfiltern. Er muss die (hoffentlich selten auftretenden) Fälle von bereits fortgeschrittenen Kompromittierungen im Rahmen eines Alarmstufenmanagements behandeln. Gleichzeitig muss er die regelmäßigen Tätigkeiten (Awareness-Maßnahmen, Audits, Penetrationstests etc.) beaufsichtigen und die aus Compliance-Gründen geforderten Rechenschaftsberichte zeitgerecht erstellen. Alle diese Aufgaben sind dringend. Die wohl

wichtigste Aufgabe des CISO ist es aber, das Unternehmen im Sicherheitsbereich so aufzustellen, dass es inhärent resilient gegen Angriffe und Bedrohungen ist. Leider geht »dringend« immer vor »wichtig«, sodass diese Aufgabe oft in der Aufgabenflut der CISO-Abteilung untergeht. Dies ist jedoch genau die Schnittstelle zwischen Cybersicherheit und IT-Unternehmensarchitektur. In diesem Kapitel geht es um die Maßnahmen an dieser Schnittstelle zwischen IT-Unternehmensarchitektur und CISO-Abteilung. Es geht um die Resilienz des Unternehmens gegenüber Cyberangriffe und die effiziente Umsetzung der Compliance-Anforderungen.

Gemeinsame Aufgabe: Resilienz gegen Cyberbedrohungen

Die Komplexität der unternehmensweiten Anwendungen, die Anzahl der Schnittstellen und die Verbindungen zu fremden, nicht kontrollierbaren Netzwerkumgebungen (Multi-Cloud-Strukturen, Partnernetzwerke etc.) sowie die ständige Weiterentwicklung der Täter und ihrer Angriffsmöglichkeiten erfordern die enge Zusammenarbeit zwischen IT-Sicherheitsexperten und Unternehmensarchitekten. Auch die effektive Einbindung der Sicherheit in die Organisationsstruktur des Unternehmens auf allen Ebenen ist eine erhebliche Herausforderung, die gemeinsam gelöst werden muss.

Dementsprechend nehmen Aufgaben aus den Bereichen Sicherheit, Risikomanagement und Compliance heute einen immer breiteren Raum in Projekten ein. So mancher Projektleiter oder Architekt muss für diese Themen mehr als die Hälfte seiner Zeit aufwenden. Ziel ist es, dass IT-Lösungsarchitekten und IT-Unternehmensarchitekten und die Sicherheitsabteilung sich nicht als Gegner begreifen, sondern gemeinsam an Lösungen arbeiten. Dazu muss die IT-Sicherheitsabteilung frühzeitig eingebunden werden und darf nicht nur als späte, interne Kontrollinstanz verstanden werden. Dies erfordert Innovationbereitschaft aufseiten der IT-Sicherheitsabteilung und grundlegendes IT-Sicherheitswissen aufseiten der Unternehmensarchitektur, um zukünftige Sicherheitsprobleme einschätzen zu können.

Kapitelstruktur

Aufgrund der Wichtigkeit und der Ausdehnung des Gebiets IT-Sicherheit ist dieses Kapitel eines der umfangreichsten des Buches. Es ist analog zum Gesamtwerk in vier große Blöcke unterteilt

- **Zielmuster –** Dieses Kapitel zeigt Werkzeuge auf, mit denen Sie die Ziele Ihrer Cybersicherheitsarchitektur definieren können.
- **Managementprozessmuster –** In diesem Kapitel werden die Prozessmuster erörtert, mit denen die definierten Ziele erreicht werden können.
- **Muster auf Infrastrukturebene**
- **Muster auf Applikationsebene**

Die Verantwortung für den Aufbau einer unternehmensweiten Cybersicherheitsarchitektur liegt beim CISO. Keines der folgenden Unterkapitel ist aus Sicht einer CISO-Abteilung vollständig. Das ist auch gut so, denn der komplette Themenkomplex »Cybersicherheitsarchitektur« rechtfertigt vom Umfang her ein eigenes Buch.

Es ist offensichtlich, dass die Cybersicherheitsarchitektur sehr eng mit der IT-Unternehmensarchitektur verwoben ist. Der Schnittstelle zwischen Unternehmensarchitektur und CISO-Abteilung kommt daher eine besondere Bedeutung für die mittel- bis langfristige Entwicklung des Unternehmens zu. Ziel der folgenden Unterkapitel ist es, dem Unternehmensarchitekten einen Einblick in die Dimension der Arbeit des CISO zu geben, sodass CISO und Unternehmensarchitekt ihre Schnittstelle im Unternehmen adäquat abstecken und reibungslos zusammenarbeiten können.

7.1 Zielmuster

Wenn man gemeinhin von IT-Sicherheit spricht, denkt man vor allem an Hackerangriffe und deren Abwehr; auch Computerviren kommen einem in den Sinn. IT-Unternehmensarchitekten denken dann häufig an demilitarisierte Zonen, Firewalls und beschränkte Kommunikationskanäle oder auch an verschlüsselte Kommunikationsstrecken. Das Thema Informationssicherheit ist aber weiter gefasst.

Information in vielen Formen muss geschützt werden.

Das Ziel von Informationssicherheit ist es, für ein Unternehmen (oder eine sonstige definierte Einheit) Informationen aller Art und aus allen Quellen wirkungsvoll und angemessen zu schützen. Solche Informationen müssen nicht zwangsläufig in Computersystemen gespeichert sein oder elektronisch übertragen werden. Sie können auch als Ausdrucke, handschriftlich oder in diversen anderen physischen Formen von Informationsträgern vorliegen und auf alle erdenklichen Arten übertragen werden.

Die damit verbundenen wesentlichen Begriffe der Informationssicherheit – wie Vertraulichkeit, Integrität und Verfügbarkeit – bilden die Grundlage für den Schutz von Informationen. Darunter fallen auch weitere wichtige Themen, die garantiert werden müssen, z. B. Fälschungssicherheit von Nachrichten (Authenticity, Validity), Zuverlässigkeit der Kommunikation (Reliability) und Nichtabstreitbarkeit der Kommunikation (Non-deniability).

Zusätzlich kann der deutsche Begriff »Sicherheit« noch in zwei Dimensionen aufgespalten werden:

- Security: Sicherheit in Bezug auf Schutz gegen Angriffe (auch solche, die durch menschliche Fehler begünstigt wurden)
- Safety: Sicherheit in Bezug auf die körperliche Unversehrtheit

Zumeist wird »Safety« in deutschen Unternehmen als »Arbeitssicherheit« bezeichnet und nicht von der Sicherheitsabteilung verantwortet. Diese Abgrenzung ist wichtig, da die Arbeitssicherheit ein großes und komplexes Feld ist, das nicht einfach »mitgemacht« werden kann.

Es gibt aber auch Punkte, an denen die Abgrenzung für die Sicherheitsabteilung schwieriger wird. Wenn Informationen durch menschliche Fehler abhandenkommen oder Informationen durch zufällige Ereignisse zerstört werden, ist dies sicherlich eine Verletzung der Informationssicherheit. Typischerweise ist z. B. die Abwehr ganz banaler Gefahren durch Wasser oder Feuer, die sowohl IT-Hardware als auch Materialien wie Papier vernichten bzw. unbrauchbar machen können, Aufgabe der jeweiligen Betriebseinheit (Rechenzentrumsbetrieb, Archiv). Die Abwehr von physischem Diebstahl von Informationsträgern, entweder durch Mitarbeiter des Unternehmens oder Eindringlinge von außerhalb, ist wesentlich schwieriger zuzuordnen.

Die Aufteilung der einzelnen Gefährdungen auf die Organisationsbereiche und die klare und gut kommunizierte Abgrenzung ist ein wichtiger Baustein der Cybersicherheitsarchitektur. Dies gilt insbesondere für das Themengebiet Compliance, da die jeweiligen Standards meist sehr breit gefasst sind. Damit müssen sich mit solchen Standards meist mehrere Abteilungen befassen. Ganz ähnlich verhält es sich mit dem allgemeinen Risikomanagement, in das sämtliche Bedrohungen für das Unternehmen, egal woher, eingetragen werden müssen.

Die Sicherheitsabteilung hat »nur« zwei gleichwertige Zielmuster.

Egal, wie man das Thema abgrenzt, es bleiben aber genau zwei direkte, gleichwertige Zielmuster, die zu bearbeiten sind:

Bedrohungen abwehren

und

Compliance herstellen.

In der Folge gibt es demnach zwei indirekte Zielmuster, die es zu erfüllen gilt. Zum einen müssen die beiden Zielmuster gleichzeitig effektiv erreicht und effizient umgesetzt werden. Dazu müssen die Ziele in Einklang gebracht werden. Zum anderen müssen die Themen in das Risikomanagement integriert werden.

7.1.1 Zielmuster: Bedrohungen abwehren

Trotz aller Bedrohungen und Compliance-Regeln darf das Ziel der Cybersicherheit nicht die theoretisch maximal denkbare Sicherheit sein. Die Anstrengungen aller Beteiligten im Sicherheitsbereich müssen dem Ringen um das richtige Maß an Sicherheit gelten. Diese Kompromisssuche erfolgt auf zwei Ebenen:

- Zum einen ist zu wenig IT-Sicherheit gefährlich und erhöht das Risiko wirtschaftlicher Schäden, während zu viel Sicherheit teuer und unwirtschaftlich ist. Für alle Sicherheitsmaßnahmen müssen also unternehmerisches Risiko und Gesamtkosten gegeneinander abgewogen werden.
- Zum anderen bewegt sich die IT-Sicherheit in einem Spannungsfeld mit anderen Anforderungen an die Systeme: Betreibbarkeit, Datenschutz, Benutzerkomfort und Interoperabilität, um nur einige zu nennen.

Sicherheit muss angemessen sein.

Das Designziel im Bereich der IT-Sicherheit ist also eine »**bedarfsgerechte Sicherheit**«. Was aber ist denn der »Bedarf«? Auf jeden Fall ist der Bedarf nicht gleichmäßig über das Unternehmen verteilt.

»Wer alles schützt, schützt nichts.«

Schon vor Jahren hat sich die Überzeugung etabliert, dass es keinen idealen Einsatz der verfügbaren Ressourcen darstellt, alles in der digitalen Welt gleichmäßig abzusichern. Stattdessen lautet das Motto, lieber einige Dinge weniger zu schützen, dafür andere umso mehr.

Anforderungen sind Grundlage für wirksamen Schutz.

Um einen angemessenen Schutz eines Unternehmens oder einer großen Applikation sicherzustellen, muss die Anforderung an die IT-Sicherheit der einzelnen Teile klar definiert werden. Heute gibt es zwei Wege, um dieses Ziel zu erreichen. Früher wurde zur Bestimmung des Sicherheitsbedarfs eine Schutzbedarfsanalyse (siehe Abschnitt 7.1.1.1) empfohlen. Heute wird meist eine Bedrohungsanalyse (siehe Abschnitt 7.1.1.2) für diese Zwecke eingesetzt. Während sich die Bestimmung des Schutzbedarfs mit der Frage beschäftigt, wie wichtig die Daten für die eigene Firma sind (»asset driven«, Betrachtungsrichtung »von innen«), geht eine Bedrohungsanalyse der Frage nach, wie wertvoll die Daten für einen Angreifer wären (»threat driven«, Betrachtungsrichtung »von außen«). Der größte Vorteil einer Schutzbedarfsanalyse ist ihre generelle Gültigkeit – unabhängig von einer bestimmten Bedrohung gilt der festgestellte Schutzbedarf auch für Ausfälle durch zufällige Ereignisse (Naturkatastrophen, Brand, Stromausfall). Der größte Vorteil einer Bedrohungsanalyse hingegen ist, dass die Ergebnisse eine wesentlich effektivere und effizientere Verteidigung gegen die festgestellten Angriffsszenarien erlauben.

Bedrohungsanalysen liefern oft differenzierte Ergebnisse als Schutzbedarfsanalysen.

Angesichts der hohen Kosten für die Cybersicherheit ist in den meisten Fällen eine Bedrohungsanalyse das bessere Werkzeug und die Basis dafür, die Sicherheit eines Unternehmens im Lichte der identifizierten Bedrohungen zielgerichtet aufzubauen. Das nennt man »*threat driven security*« und gilt als der modernere Weg. Dennoch ist auch das Werk-

zeug der Schutzbedarfsanalyse valide, ein gleichzeitiger Einsatz unterbleibt aber meist aus Kostengründen.

7.1.1.1 Schutzbedarfsanalyse

Das Gesamtrisiko einer Anwendung wird von drei Faktoren bestimmt:

1. Dem Schaden, der dem Unternehmen durch einen Angriff auf die Anwendung entstehen kann
2. Der Eintrittswahrscheinlichkeit eines solchen Schadens, die sich wiederum aus zwei Faktoren zusammensetzt, nämlich:
   a) der Exponiertheit des Systems sowie
   b) der Schwierigkeit eines Angriffs (»Hackerresistenz«)

Risikoanalyse

Um analysieren zu können, wie Sicherheit gefährdet werden kann, werden drei Grundwerte unterschieden: Vertraulichkeit, Integrität und Verfügbarkeit (englisch Confidentiality, Integrity, Availability – CIA).

- Die Vertraulichkeit ist verletzt, wenn Daten oder Code unberechtigt zur Kenntnis genommen oder weitergegeben werden.
- Die Integrität von Daten ist verletzt, wenn die Korrektheit der Daten oder der Funktionsweise von Systemen nicht mehr gegeben ist.
- Die Verfügbarkeit von Daten ist verletzt, wenn autorisierte Benutzer am Zugriff auf Daten und Systeme behindert werden.

Schadenshöhe

Die Schadenshöhe kann entweder in unternehmensweit definierte Schadensklassen eingeordnet oder monetär bemessen werden.

Es ist nur selten möglich, die Schadenshöhe mit Sicherheitsmaßnahmen zu reduzieren, ohne die Funktionalität der Anwendung zu verändern. Zur Reduktion der Schadenshöhe müssten sicherheitskritische Daten oder Prozesse aus dem Projekt entfernt werden.

Eintrittswahrscheinlichkeit

Wie oben beschrieben, reicht die Schadenshöhe allein nicht aus, um das Gesamtrisiko zu bestimmen, sondern sie muss mit der Eintrittswahrscheinlichkeit des jeweiligen Schadens korreliert werden. Diese Eintrittswahrscheinlichkeit eines Angriffs setzt sich aus der Schwierigkeit des Angriffs und der Exponiertheit des Systems zusammen.

Exponiertheit eines IT-Systems

Die Exponiertheit des Systems wird durch die Frage bestimmt, wer grundsätzlich Zugang zum System hat:

- Wer erreicht die Passwortabfrage (nur Mitarbeiter, alle Internetbenutzer)?
- Wer hat einen gültigen Account (Mitarbeiter, Externe, Lieferanten etc.)?
- Wer muss welche Funktionen nutzen?

- Wie wird sich dies in Zukunft entwickeln?
- Wie bekannt ist das System?
- Wie »attraktiv« ist das System für einen Angreifer (Imagegewinn, wie gut verkäuflich sind die erhaltenen Informationen etc.)?

Begrenzung der Exponiertheit

Die Exponiertheit eines Systems kann mit netzwerktechnischen Mitteln (Firewall, VPN, siehe u.a. Abschnitt 7.3.2.3) und einer klaren Rollen- und Rechteverwaltung (siehe Abschnitt 7.4.2.1) auf das notwendige Minimum beschränkt werden. Zusätzlich kann eine Modellierung der Applikation in Schutzzonen die Exponiertheit reduzieren (siehe Abschnitt 7.4.3.1). Weitere Verbesserungen können dann nur noch durch Veränderung der Funktionalität erreicht werden.

Ableitung von Schutzmaßnahmen

Auf Basis der festgestellten möglichen Schadenshöhe und der definierten Exponiertheit kann für jeden Grundwert (Vertraulichkeit, Integrität, Verfügbarkeit) angegeben werden, wie wichtig der Schutz dieses Grundwerts innerhalb der Applikation ist. Je wichtiger der Schutz ist, umso schwieriger muss ein Angriff sein, um das Gesamtrisiko innerhalb akzeptabler Grenzen zu halten.

Die Schwierigkeit eines Angriffs (»Hackerresistenz«) kann durch geeignete Sicherheitsmaßnahmen (siehe die Abschnitte 7.3 und 7.4) deutlich erhöht werden. Das Ergebnis einer Schutzbedarfsanalyse gibt damit vor, welche und wie viele Sicherheitsmaßnahmen ergriffen werden müssen.

IT-Grundschutz-Kataloge

Detaillierte Beschreibungen zur Erstellung von Schutzbedarfsanalysen finden sich

- in den IT-Grundschutz-Katalogen des BSI [BSIGrundschutz23] und
- in den ISO-2700x-Standards (siehe Abschnitt 7.2.4).

7.1.1.2 Bedrohungsanalyse

Eine Bedrohung besteht immer aus drei Komponenten: einem Täter, einem Angriffsvektor bzw. einer Angriffsmethodik und einer Motivation. Erst wenn alle drei Komponenten zusammenkommen, entsteht eine echte Bedrohungssituation.

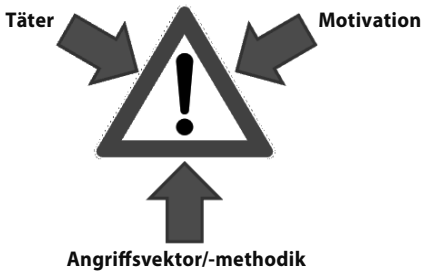


Abb. 7–1
Komponenten von Bedrohungen

Eine Verteidigung ist damit auf drei Arten möglich:

- Reduktion der Angriffsmöglichkeiten durch technische, organisatorische oder personelle Gegenmaßnahmen
- Reduktion der Täterkreise durch Verfolgungsdruck und Abschreckung (z. B. durch Zusammenarbeit mit den Behörden oder die Erhöhung der Entdeckungsmöglichkeiten)
- Reduktion der Motivation durch Einbindung (z. B. durch Bug-Bounty-Programme)

Im Rahmen einer Bedrohungsanalyse sollen nun die möglichen Kombinationen aus Täter, Motivation und Angriffsvektor konkret zusammengetragen werden. Danach erfolgt ein Rating der Bedrohungen, indem die einzelnen Bedrohungsszenarien gemäß ihrer Priorität geordnet werden.

Analyse möglicher Tätergruppen

Als Erstes werden Listen relevanter Täter bzw. Tätergruppen und deren Motivationen aufgestellt. Typische Motivationen von Tätern sind:

- **Ruhm**
  Die Täter wollen die Aufmerksamkeit einer Community bzw. der Öffentlichkeit erregen, um die persönliche Reputation zu steigern. Im Vorfeld helfen Bug-Bounty-Programme bzw. eine kluge Täteransprache. Im Echtfall spielt Schadensbegrenzung durch proaktive Kommunikation eine große Rolle.
- **Geld**
  Der Täter will Geld, meist in Bitcoins. In der Regel werden kurzfristige »Hit & Run«-Aktionen durchgeführt, die innerhalb von wenigen Wochen zu einer Geldzahlung führen sollen. Die Angriffe sind meist ungezielt, d. h., der Täter wählt das Opfer, bei dem er am leichtesten Geld bekommen kann. Typische Verteidigungsstrategie ist die Implementierung ausreichender präventiver Sicherheitsmaßnahmen, um nicht das leichteste Opfer zu sein. Unabhängig von der Zahlungsbereitschaft ist im Echtfall eine professionelle Täterkommunikation empfehlenswert.
- **Know-how**
  Die Täter wollen das Wissen bzw. Know-how des Opfers stehlen, meist in langfristig angelegten und geplanten Aktionen, die gut verdeckt werden. Die Schäden zeigen sich oft erst spät. Zur Schadensbegrenzung hat sich – neben der IT-Forensik – die enge Einbindung der Fachabteilungen bewährt. Wichtigster Baustein in der Verteidigung ist die Identifikation der Informationen, auf die es ein Angreifer abgesehen haben könnte. Diese Daten müssen dann speziell geschützt werden. Meist ist die grundlegende Motivation des Täters zwar Geld, er will aber mit dem Angriff Know-how stehlen.

- **Versehen**
  Ein »Täter« hat als unabsichtlicher Mittäter eine Rolle gespielt oder aus Versehen einen Angriff begünstigt. Im Echtfall ist die Gewissensberuhigung des Täters notwendig. In der Verteidigung spielen Schulungen und Awareness-Trainings die wichtigste Rolle.
- **Rache**
  Der Täter sinnt auf Rache bzw. will seinem Opfer schaden. Die Behandlung im Echtfall ist schwierig, die Täteridentifikation und eine psychologisch fundierte Kommunikation sind wichtig. Die erfolgreichste Verteidigungsstrategie ist es, diese Motivation nicht entstehen bzw. nicht wachsen zu lassen. Künftige Täter können mittels passender »red flags« normalerweise früh erkannt werden.
- **Überzeugung**
  Die Täter wollen einen Missstand beseitigen. Oftmals werden die Opfer nur stellvertretend angegriffen. Je nach Forderung ist eine professionelle Verhandlung mit dem Täter und dessen Identifikation wichtig. Eine Früherkennung ist z. B. durch eine Whistleblower-Hotline oder ähnliche Angebote möglich.
- **Sabotage**
  Ziel der Täter ist es, Maschinen, Dienstleistungen und Produkte des Opfers lahmzulegen. Wichtigster Baustein in der Verteidigung ist eine vorbereitete Notfallplanung, ein geübtes Krisenmanagement und technisches Business Continuity Management. Besonders gefährlich sind Angriffe auf Unternehmen, die eine kritische Infrastruktur betreiben (KRITIS).

Die Täter haben unterschiedliche Voraussetzungen:

Die Motivation der Täter erklärt deren Ziel, die weiteren Voraussetzungen definieren die möglichen Angriffswege.

- **Technische Expertise**
  Gegen Täter mit geringer Expertise kann man sich gut präventiv mit technischen Maßnahmen verteidigen. Für Täter mit hohem technischem Know-how sind Log-Überwachung und ein Sicherheitsbetrieb sowie eingeübte und getestete Notfallprozeduren wichtig.
- **Insiderwissen**
  Täter mit geringem Insiderwissen passen Angriffe kaum an ihre Opfer an, dadurch kann man sich leichter mit Standardmitteln gegen sie verteidigen. Für Täter mit hohem Insiderwissen sind regelmäßige Kontrollen und das konsequente Management hochprivilegierter Zugänge gute Verteidigungsmaßnahmen.
- **Einsatzerfahrung**
  Täter mit geringer Einsatzerfahrung sind im Echtfall unberechenbarer, Angreifer mit hoher Einsatzerfahrung sind dafür schwerer zu identifizieren und eine Verteidigung ist nur mit hohem technischem Aufwand möglich.

- **Vertrauensstellung**
  Täter mit geringer Vertrauensstellung können gut präventiv mit technischen und prozessualen Maßnahmen abgeblockt werden. Für Täter mit hoher Vertrauensstellung sind »red flag«-Erkennung und Notfallpläne wichtiger.
- **Finanzielle Mittel**
  Hohe finanzielle Mittel können Defizite in den anderen Kategorien kompensieren, indem etwa Spezialisten angeheuert werden. Allerdings schöpft nicht jeder Täter für jedes Opfer seine kompletten finanziellen Möglichkeiten aus.

Ein typisches Startportfolio für Täter und Motivationen findet sich in Tabelle 7–1.

Tab. 7–1 *Analyse möglicher Tätergruppen*

Tätergruppe	Motivation	Technische Expertise	Einsatzerfahrung	Insiderwissen	Vertrauensstellung	Finanzielle Mittel
Klassische organisierte Kriminalität (non-Cyber)	Geld	2	4	2	1	3
Cybercrime-Betrug (Business E-Mail Compromise)	Geld	2	4	3	1	3
Cybercrime-Erpressung (Ransomware, DDoS)	Geld	4	4	2	1	3
Cybercrime Malware Operations (Botnetze, Identitätsdiebstahl etc.)	Geld	4	4	1	1	2
White-Hat-Hacker, Sicherheitsforscher	Ruhm, Geld	5	4	2	2	2
Script Kiddies, Hobby-Hacker	Ruhm, Überzeugung	3	1	2	1	1
Medien, Journalisten	Ruhm, Geld	1	4	3	4	2
Unseriöse Politiker	Geld, Ruhm	1	2	3	3	1
Cyber-Söldner	Know-how, Sabotage	4	5	3	2	4
Militärische Cybereinheiten	Know-how, Sabotage	5	5	2	2	5
State-Sponsored Actors	Know-how, Sabotage	5	5	2	2	4
Technische Geheimdienste	Know-how, Sabotage	5	5	4	2	5
Religiös oder politisch motivierte Täter	Überzeugung, Sabotage	1	3	1	1	3
Cyberterroristen	Sabotage	3	3	1	1	4
Whistleblower	Überzeugung, Ruhm	2	1	5	5	1
Non-Profit-Organisationen	Überzeugung, Ruhm	2	3	2	2	3

→

Tätergruppe	Motivation	Technische Expertise	Einsatzerfahrung	Insiderwissen	Vertrauensstellung	Finanzielle Mittel
Hacktivisten	Überzeugung, Sabotage, Ruhm	4	1	1	1	2
Mitarbeiter in Schwierigkeiten	Geld, Know-how, Sabotage	4	1	5	5	1
Frustrierte Mitarbeiter	Rache, Geld	4	1	5	5	1
Rachsüchtige Ex-Mitarbeiter	Rache, Geld	4	1	5	3	1
Konkurrierende Ex-Mitarbeiter	Know-how	3	1	5	3	2
Missgünstige Familienmitglieder von Managern/Eigentümern	Rache, Geld	2	2	4	4	4
Detekteien	Know-how	2	3	3	3	2
Mitbewerber, Konkurrenz	Know-how, Sabotage	2	3	3	2	3
Industriespion	Know-how, Sabotage	3	4	3	3	3
Ehrgeizige Dienstleister	Know-how	4	1	5	5	3
Betrügerische Partner	Know-how	2	1	4	4	4
Unehrliche Kunden	Geld	1	1	3	4	1
Produktpiraten	Know-how, Geld	2	1	4	3	3
Modding-Szene	Know-how, Geld	4	3	4	3	2
Finanzakteure	Know-how, Sabotage	2	4	3	3	4
Eingeschleuste Mitarbeiter	Know-how, Sabotage	2	1	4	4	2
Instrumentalisierte Verbände	Know-how	1	3	2	2	4
Unterwanderte Dienstleister	Know-how	5	3	5	5	1
Ausländische Propaganda	Know-how, Sabotage	1	5	1	1	4
Klassische Nachrichtendienste	Know-how	3	5	3	3	5
Unvorsichtige Mitarbeiter	Versehen	3	1	5	5	0
Unachtsame Dienstleister	Versehen	4	1	5	5	0
Ermittlungsbehörden	Versehen	3	4	1	2	3
Entfernte Lokationen	Versehen	4	1	5	5	0

Die Priorisierung der Täter ist für jeden Entscheider möglich.

Als Nächstes werden mögliche Tätergruppen im Licht der Anwendung oder des Unternehmensteils priorisiert. Welche Täter sind relevant? Welche Täter sind gefährlich. Dabei werden sicherlich 50–80 Prozent der Täter und Motivationen aus dem Gesamtportfolio komplett aussortiert, die restlichen werden priorisiert. Der Vorteil dabei ist, dass die Bedro-

hungen auch von Kollegen verstanden werden, die sich mit IT-Sicherheit noch nie beschäftigt haben. Dementsprechend kann die Priorisierung leicht auf eine breite Basis gestellt werden. Die Priorisierung geschieht entweder im Umlaufverfahren (»in eine Reihenfolge der Gefährlichkeit bringen«) oder im Team (z. B. mittels Planning-Poker-Karten).

Danach wird überlegt, welche Angriffsvektoren ein Täter mit seinen Voraussetzungen wahrscheinlich verwenden würde. Eine komplette Bedrohungsanalyse könnte dann wie folgt aussehen (hier am Beispiel einer Bank, siehe Tab. 7–2).

Im letzten Schritt werden die Szenarien anhand der Einschätzung in drei Kategorien eingeteilt:

- **akut** (Szenarien, bei denen es wahrscheinlich ist, dass sie aktuell passieren können),
- **aufstrebend** (Szenarien, die aktuell im Feld beobachtet werden, die aber aufgrund der Situation derzeit eher unwahrscheinlich sind),
- **Außenseiter** (Szenarien, die aktuell noch nicht »in the wild« vorkommen oder derzeit nicht relevant sind, es aber zukünftig werden können).

Tab. 7–2 *Bedrohungsanalyse am Beispiel einer Bank*

Beispiel für eine Bedrohungsanalyse (Rohform)		
Täter bzw. Tätergruppe	**Motivation**	**Angriffsmöglichkeit bzw. Schwachstelle**
Ehemaliger Insider	Vergeltung/Rache	Von außen nutzbare Zugänge und Schwachpunkte in Geschäftsprozessen
Ermittlungsbehörden: ■ Staatsanwaltschaft ■ Polizei ■ Steuerfahndung	Auftrag	■ Observation ■ Verdeckte Ermittlungen (Social Engineering) ■ Telefonüberwachung ■ Wanzen ■ Lauschangriff
Hacker	■ Spielen mit Systemen ■ Aufdecken von Schwachstellen	Extern erreichbare Dienste/Systeme
Insider	Finanzieller Vorteil	Weitergabe vertraulicher Informationen an Behörden
Insider	■ Vergeltung/Rache ■ Finanzieller Vorteil	Legitime Zugriffsmöglichkeit auf Systeme oder Daten
Medien & investigative Journalistik	Schlagzeilen	Social Engineering

→

Beispiel für eine Bedrohungsanalyse (Rohform)		
Täter bzw. Tätergruppe	**Motivation**	**Angriffsmöglichkeit bzw. Schwachstelle**
Mitarbeiter	Finanzieller Vorteil	■ Geldüberweisungen tätigen bzw. umschreiben ■ Kredit ohne Vorprüfung anlegen und Überweisung tätigen
■ Mitarbeiter ■ Dienstleister	Unabsichtliche Fahrlässigkeit	Fehlbedienung von Systemen/Applikationen
Mitarbeiter/ehem. Mitarbeiter	■ Karrierevorteil ■ Finanzieller Vorteil	Missbrauch von externen Diensten
■ Mitarbeiter/ehem. Mitarbeiter ■ Organisierte Kriminalität ■ Terroristen	■ Erpressung ■ Rufschädigung ■ Finanzieller Vorteil	■ Ausspähen von Zugangsdaten ■ Manipulationen im Zahlungsverkehr
Mitbewerber	Wettbewerbsvorteil	Abwerben von Schlüssel-Mitarbeitern
Organisierte Kriminalität	Finanzieller Vorteil	■ Fake President o. Ä. ■ Social Engineering auf Firmenebene
Organisierte Kriminalität	Finanzieller Vorteil	■ Manuelle Prozessanpassung der Daueranweisungen (Login bekannt, erbeutet), um kleine Beträge abzuzweigen ■ SWIFT-Nachrichten (meist Text- bzw. XML-Dateien) anpassen (Geldtransfersysteme, Übertragungsweg) ■ Kredit ohne Vorprüfung anlegen und Überweisung tätigen (geht das?)
Organisierte Kriminalität	Finanzieller Vorteil	Androhung/Durchführung eines DoS-Angriffs
Organisierte Kriminalität	Geld erpressen	Ausspähen von vertraulichen Informationen
Unzufriedener Mitarbeiter/Ex-Mitarbeiter	Rufschädigung	Datenschutzverletzungen öffentlich machen
Whistleblower	Ethisch-moralische Beweggründe	Weitergabe vertraulicher Informationen an Behörden oder Journalisten

Inhaltsübersicht

Inhaltsverzeichnis