

Kapitel 2

Die veränderte Rolle der IT im Unternehmen

Auf dem Weg von der postmodernen Industriegesellschaft hin zur so genannten Informationsgesellschaft nimmt die Quantität und die Qualität von Informationen völlig neue Dimensionen an. Nie zuvor waren Informationen so umfangreich und gleichzeitig hoch konzentriert verfügbar, nie zuvor waren auch Geschwindigkeit und die Fähigkeit, Informationen gewinnbringend zu nutzen, so entscheidend im Wettbewerb.

Dennoch wird das Verständnis wirtschaftlicher Zusammenhänge, innerbetrieblicher Aktionsparameter und damit die Gestaltung der Aufbau- und Ablauforganisation auch heute noch weitgehend durch das von E. Gutenberg entwickelte System der Produktionsfaktoren geprägt.

2.1 Der verkannte Produktionsfaktor

Produktionsfaktoren sind laut Gutenberg alle Güter, die im Leistungserstellungsprozess eingesetzt werden. Hierbei unterscheidet er zwei Gruppen: Die Elementarfaktoren bilden die Grundbausteine, ohne die eine betriebliche Leistungserstellung nicht möglich wäre. Sie bestehen aus Werkstoffen, Betriebsmitteln und ausführender Arbeit. Die dispositiven Faktoren werden von allen Funktionen gebildet, die betriebliche Vorgänge koordinieren und lenken, also Leitung, Planung, Organisation und Kontrolle.

Im Zuge der Automatisierung von außer- und innerbetrieblichen Abläufen, der Entwicklung „intelligenter“ Produkte, Information als eigenständigem Produkt oder selbständigem Einsatzfaktor, wurde die Limitierung des gutenbergschen Modells schnell klar und die Information wurde als Erweiterung in das Modell eingebracht. Das geschah, indem man die Information als vierten Elementarfaktor, neben Werkstoffen, Betriebsmitteln und ausführender Arbeit, klassifizierte.

Unserer Ansicht nach springt man hier jedoch zu kurz. Die Information gewinnt als eigenständiger Werkstoff, als Betriebsmittel und immer wichtigere Grundlage und Arbeitsmittel der dispositiven Faktoren exponentiell an Bedeutung. Nimmt man die Entwicklung des Anteils der Beschäftigten in den vier Sektoren Landwirtschaft, Produktion, Dienstleistungen und Informationsverarbeitung als Indikator, so ist dieser Prozess auch noch längst nicht zu Ende.

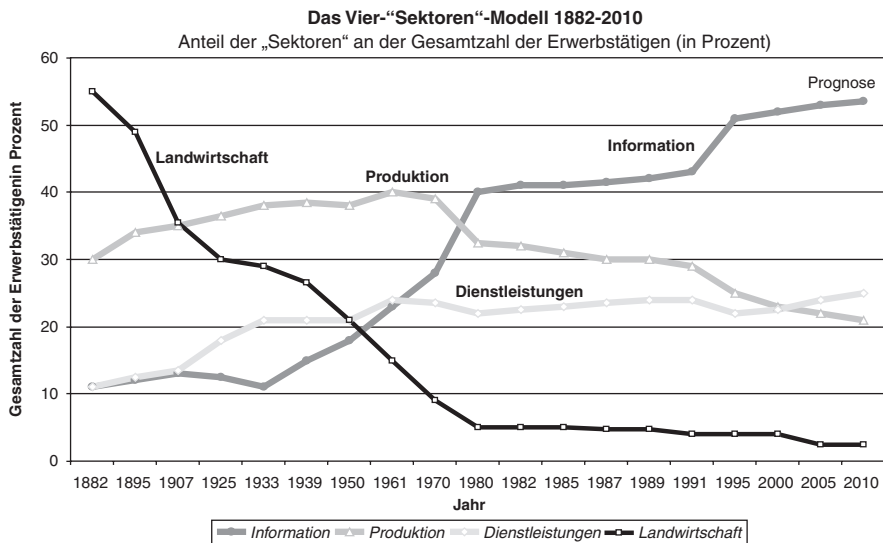


Abb. 2.1. Vier-„Sektoren“-Modell

Letztendlich bildet die Information und ihre Verarbeitung in der modernen Unternehmung das – im wahrsten Sinne des Wortes – unverzichtbare Bindeglied zwischen allen Elementen der gutenbergschen Darstellung. Daher auch die immer häufigere Auslegung des Kürzels IT als *Integrations-Technologie* an Stelle von *Informations-Technologie*.

Der veränderten Situation wird man jedoch weder durch Hilfskonstruktionen bzw. Erweiterungen von Modellen, noch durch das Festhalten an der klassischen Aufbauorganisation mit Reduktion der Informationstechnologie auf den Status einer Querschnitts-Funktion gerecht.

Wir denken, es bedarf einer grundlegenden Überarbeitung der bisherigen Annahmen und in der Folge auch der unternehmensinternen Mechanismen und Governance-Strukturen im Umgang mit Informationstechnologie.

2.2 Die Folgen der digitalen Revolution

Das Vertrauen in die IT, oder besser gesagt in die Fähigkeiten des in der IT tätigen Managements, ist wie bereits erwähnt während des Internet-Booms (E-Business) stark und mit anhaltender Wirkung gestört worden. In der Hype-Phase des Internet-Booms wurde der Versuch unternommen, die IT als eigenständigen Erfolgsfaktor neben den natürlichen Kernkompetenzen der Unternehmen zu etablieren. Die Informationstechnologie sollte nicht mehr „nur“ als Servicefunktion wahrgenommen

werden, sondern ihren Platz gleichberechtigt neben den klassischen Unternehmensfunktionen finden.

Im Sinne der oben geforderten Umorientierung in der Betrachtung der Rolle der IT im modernen Unternehmen ist das zwar durchaus nachvollziehbar. Allerdings wurde der Bogen, manchmal drastisch, überspannt und eine Informationstechnologie quasi als Selbstzweck und losgelöst von ihrer integrierenden und verbindenden Rolle als „Unternehmen im Unternehmen“ propagiert. Zudem wurden Erwartungen – die die Unternehmens-IT nicht erfüllen konnte, da die Zeit für die jeweilige Technologie noch nicht reif war oder unrealistische Annahmen getroffen wurden – insbesondere durch das Marketing geschürt.

Aber es ist müßig, über die Urheber dieses „Missverständnisses“ zu diskutieren. Tatsache ist, dass die Geschäftsmodelle diverser Anbieter von Produkten und Dienstleistungen rund um die Informationstechnologie diesen Trend zumindest nicht gebremst, sondern sogar erfunden und gefördert haben. In der Folge wurden wertvolle Zeit und Ressourcen in aus heutiger Sicht, im wahrsten Sinne des Wortes „abgeschriebene“ Investitionsruinen investiert. Der zu diesem Zeitpunkt jedoch dringend benötigte Wandel hin zu einer professionell aufgestellten und für die Zukunft gerüsteten firmeninternen IT-Organisation blieb dagegen weitgehend auf der Strecke.

2.3 Die Industrialisierung der Informationsverarbeitung

Am Ende des 20. Jahrhunderts ist erkennbar geworden, dass die vor etwa zwei Jahrhunderten entstandene Industriegesellschaft durch konsequente und rationelle Nutzung der Informationstechnologie ihren Charakter mehr und mehr verändert und zur Informationsgesellschaft wird. Zum Einen ermöglicht die Informationstechnologie durch das Entstehen so genannter Teleprozesse (Telearbeit, -banking, -learning, etc.) die Weiterentwicklung der Industriegesellschaft in eine neue Dimension.

Zum anderen erfährt die Informationsverarbeitung jedoch selbst auch einen tief greifenden Wandel, indem sie einen großen und wichtigen Entwicklungsschritt durchlaufen muss: die Bereitstellung ihrer Leistungen nach industriellen Maßstäben – qualitativ, quantitativ, effizient, effektiv und unter Wettbewerbsbedingungen.

Als Gradmesser und Seismograph für die Erwartungshaltung der Nutzer gegenüber den Betreibern von Informationssystemen mögen hier die Äußerungen in der Fachpresse dienen. Mit Formulierungen wie „IT aus der Steckdose“, „IT als Commodity“ (also Massenware), „das Web ist der Computer“, „Virtualisierung der Infrastruktur“ und „IT on demand“ wird ein Reifegrad gefordert, den die wenigsten Organisationen, egal ob unternehmensintern oder als externer Serviceprovider, bisher erreicht haben.

Die mit dieser Erwartungshaltung verknüpften Technologien und Serviceangebote wie Service oriented Architecture (SOA), Web-Services und Application Service

Providing (ASP), um nur einige zu nennen, setzen ganz auf die mit der industriellen Massenfertigung verknüpften Kennzeichen, nämlich Spezialisierung und Arbeitsteilung. Auf die „Serienfertigung“ in der Informationstechnologie übertragen heißt das, dass die Leistungstiefe der IT-Organisationen abnehmen wird und auf Grund der hiermit einhergehenden Spezialisierung wesentlich mehr Teilnehmer in die Wertschöpfungskette für IT-Produkte eingebunden werden müssen.

Ironischerweise entsteht, zugegebenermaßen auf höherem Niveau, genau das Szenario wieder auf, welches wir durch die Einführung von integrierter Software als „besiegt“ betrachtet hatten: eine Vielzahl von Schnittstellen! Diese und die zu übergebenden Teilprodukte müssen überwacht und qualitätsgesichert werden, Service Level Agreements müssen abgeschlossen und verwaltet werden.

Hier stellen sich eine Vielzahl von Fragen, die aus der Industrie wohl bekannt und untrennbar mit der Arbeitsteilung in der Wertschöpfung verbunden sind: Wie ist die verteilte Wertschöpfung organisiert? Welche Partner erbringen welchen Anteil an der Leistung? Handelt es sich um Lohnfertigung? Wie funktioniert die Abrechnung und die Qualitätssicherung? Wer kann zu welchem Zeitpunkt für was haftbar gemacht werden? Welche Governance-Strukturen herrschen zwischen den teilnehmenden Akteuren?

2.4 Der Druck zur permanenten Veränderung und Anpassung

In der neu entstandenen Informationsgesellschaft verlieren die klassischen Wettbewerbsfaktoren und die räumliche Distanz zu Kunden und Mitbewerbern zunehmend an Bedeutung. Der Wettbewerb wird immer mehr zum Zeitwettbewerb. Auf den Märkten der Informationsgesellschaft zählen nicht mehr Größe und Kosten, sondern vorrangig Kreativität und Flexibilität. Wurden früher die Kleinen von den Großen gefressen, so wird in der Zukunft der Schnelle den Langsamen überholen und letztendlich besiegen. Time-to-Market wird zur entscheidenden Größe, wenige Wochen entscheiden über Erfolg oder Misserfolg einer Produkteinführung.

In der Informationsgesellschaft sind daher, vor allen Dingen bei den Schöpfern digitaler Produkte, Phasen mit Arbeitszeiten von 100 Stunden/Woche und mehr durchaus nicht ungewöhnlich. Da inzwischen jedoch auch in den alten und reifen Industrien, wie der Autoindustrie, Software in allen Stadien der Wertschöpfung eine Schlüsselrolle spielt oder, wie schon ABB-Chef Percy Barnevik es formulierte, „alle Unternehmen heute Informationstechnologie-Unternehmen sind“, wird auch hier ebenfalls immer häufiger rund um die Uhr und rund um den Globus entwickelt.

Fast jede Veränderung im Unternehmen resultiert heute in der einen oder anderen Form in einem IT-Projekt. Gesetzliche Vorschriften, geänderte Geschäftsprozesse, Änderungen in den Organisationsstrukturen, Mergers & Acquisitions, Verkäufe von Unternehmensteilen – jede Veränderung im Unternehmen muss in den unterstützenden Systemen nachvollzogen werden. Kann die IT die immer schneller und grundlegenden Veränderungen auf Grund von ineffizienten Organisations-, d. h. Demand/Supply-, oder Managementstrukturen nicht zeitgerecht nachvollziehen, so

verstärkt sich bei den Business-Managern das Gefühl der Abhängigkeit und des Ausgeliefertseins. Die IT wird als Hemmschuh wahrgenommen.

Die Hebel, um diesen Missstand zu beseitigen, sind organisatorischer Natur. Effektive und klare Steuerungsprozesse unter Einbezug aller beteiligten Parteien wie Zulieferern, Partnern, Dienstleistern und Kunden sind genauso notwendig wie ein effektives Demand/Supply-Management. Ein weiteres Thema ist das effektive Managen des Projektportfolios: Das Einschränken der Anzahl von Projekten auf das notwendige Maß schafft Kapazität, um auf Veränderungen angemessen reagieren zu können, die Priorisierung des Projektportfolios hilft das Wichtige vom Unwichtigen zu unterscheiden. Änderungsprojekte können so zeitlich an der richtigen Stelle eingetaktet werden, ohne andere – für das Unternehmen wichtige – Maßnahmen zu kannibalisieren.

Aber nicht nur der sich immer schneller wandelnde Unternehmensalltag zwingt zur permanenten Anpassung. Die Halbwertszeit etablierter Technologien nimmt beständig ab. Durch das stetige Anwachsen der Komplexität müssen heute prozentual mehr Ressourcen in der IT für die Pflege der Systemlandschaft bereitgestellt werden (ein Faktor, der übrigens durch die anhaltenden, starken Kostenreduktionen der letzten Jahre verstärkt wird). Um die unterschiedlichen Technologieplattformen kompatibel zu halten, müssen immer häufiger Releasewechsel durchgeführt werden. Der Mehrwert dieser manchmal recht aufwändigen Aktivitäten erschließt sich dem Nutzer der Systeme nur selten direkt und der nicht erkennbare Mehrwert nährt die Zweifel am rationalen Handeln der Verantwortlichen in der IT.

Auch hier helfen nur Transparenz und die Einbeziehung der Systemnutzer in den Prozess der Steuerung und Priorisierung. Durch eine konsequente und inhaltlich saubere Strukturierung des Aufwands in der IT muss die Notwendigkeit einer permanenten Pflege der technologischen Basis („cost of doing business“) deutlich gemacht werden. Es ist für den Laien eben schwer zu verstehen, dass die immateriellen Produktionsanlagen für immaterielle Informationen genauso schnell veralten oder einem Verschleiß unterworfen sind wie die materiellen Produktionsanlagen zur Herstellung materieller Güter!

Software, auch die selbst erstellte, wird zwar abgeschrieben, jedoch ist damit noch längst nicht der Gedanke kontinuierlicher Wartung und periodischer Erneuerung als Konsequenz verknüpft.

2.5 Die digitale Identität

Geschäftserfolg ist heute mehr denn je abhängig vom schnellen und zuverlässigen Zugriff auf Informationen. Konsequenterweise rückt damit auch der Bedarf an nachhaltiger Sicherung dieser Informationen vor Verfälschung und Diebstahl in den Vordergrund. Obwohl auch heute noch der Zugang zu unseren Firmen über technisch mehr oder weniger raffiniert ausgestattete Firmenausweise die am ehesten wahrnehmbare Sicherheitskontrolle darstellt, verläuft die wirkliche Kampflinie um den berechtigten Zugang auf das „Firmengelände“ längst woanders: bei der Prüfung der Zugriffsberechtigung auf die Informationssysteme!

War die Zugangskontrolle über Passwörter vor einigen Jahren noch eine ungeliebte, häufig geradezu verhasste und umgangene Prozedur, so ist die Überprüfung der digitalen Identität mittlerweile auf der Prioritätenliste der Unternehmen ganz nach oben gerückt. Aber nicht nur der Zugang zu den Informationssystemen muss angemessen administriert und kontrolliert werden. Auch in Bezug auf die Nutzung der in den Systemen vorhandenen Daten muss je nach Wichtigkeit derselben für das Unternehmen unterschieden werden.

Ausschlaggebend hierfür ist nicht nur der frustrierte und rachsüchtige Mitarbeiter, der Informationen an die Konkurrenz oder die Presse weiterleitet. Die wachsende Komplexität der Beziehungen von Firmen untereinander, speziell die so genannte „Virtualisierung“ von Teilen des Unternehmens, verlangt nach klaren und eindeutigen Regeln, um die Identität von Mitarbeitern feststellen und administrieren zu können.

Wesentliche Voraussetzungen für eine funktionierende „Business Resilience“ sind klare und eindeutig definierte Steuerungsmechanismen, Berechtigungskonzepte und Entscheidungsstrukturen. Diese müssen sich in der IT-Governance niederschlagen.

2.6 Der Einfluss rechtlicher oder regulatorischer Anforderungen

Einer Umfrage von AMR Research zufolge (AMR Research 2005) werden alleine in den Vereinigten Staaten im Jahr 2005 ungefähr 15,5 Mrd. \$ dazu verwendet, mit den wachsenden gesetzlichen Anforderungen – wie Sarbanes–Oxley, dem Health Insurance Portability and Accountability Act sowie den Anforderungen der Securities and Exchange Commission und der Food and Drug Administration – Schritt zu halten. Es wird erwartet, dass diese Ausgaben bis 2009 eine Größenordnung von 80 Mrd. \$ erreichen können.

Die für diese Studie befragten Firmen gaben an, dass von den oben genannten Mitteln ca. ein Drittel in Informationstechnologie, also Hardware und Software, investiert werden. Zwei Drittel werden für die Beschäftigung von internen Mitarbeitern sowie externen Beratern und Auditoren aufgewendet. Es steht außer Frage, dass ein Großteil der Kosten im direkten Zusammenhang mit der Beseitigung ablauforganisatorischer Schwächen in den Geschäftsprozessen bzw. den zugrunde liegenden Systemen steht. Eindeutigkeit, Nachvollziehbarkeit und die saubere Dokumentation von Änderungen an Prozessen und Systemen stellen die wichtigsten und fast identischen Forderungen fast aller Gesetze mit normierender Kraft für die IT dar. Diese gesetzesspezifischen Anforderungen mit ihren Auswirkungen auf die jeweiligen Systeme sind aber wirtschaftlich nicht in einer Vielzahl voneinander unabhängiger Einzelprojekte zu bewältigen. Vielmehr ist hier die Entwicklung eines allgemein gültigen Regelwerks, eben in der Form einer IT-Governance, gefragt.

Im Nachfolgenden wird beispielhaft auf rechtliche und regulatorische Anforderungen an die IT Bezug genommen, um die Notwendigkeit einer praxisnahen

IT-Governance herauszuarbeiten. Unberücksichtigt bleiben hier Anforderungen an Unternehmen, die sich zwar mittelbar auch an die IT richten (wie zum Beispiel die Forderungen des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich KonTraG), jedoch durch geeignete Corporate-Governance-Strategien schon entsprechend berücksichtigt wurden. Hierzu würden auch das Transparenz- und Publizitätsgesetz (TransPuG), das Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG) oder die International Financial Reporting Standards (IFRS und IAS) zählen. Wegen der vielschichtigen externen Anforderungen gehen viele global agierende Unternehmen mit zusätzlichen branchenspezifischen Anforderungen, wie zum Beispiel der Pharmaindustrie (Compliance-Anforderungen der FDA), heute bereits so weit, eine diesbezügliche zentrale Anlaufstelle in Form eines Corporate Compliance Officers¹ einzurichten.

2.6.1 Die Verarbeitung personenbezogener Daten und Datenschutz

Gerade die Verarbeitung² personenbezogener (oder beziehbarer) Daten (Datenschutz) ist durch vielfältige Anforderungen betroffen und stellt global agierende Unternehmen vor besondere Herausforderungen. Vor ein paar Jahren wurde der Bereich Datenschutz noch als rein deutsches (erstes Datenschutzgesetz weltweit) und später als ein europäisches (EU-Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995) Problem angesehen. In anderen Rechtsstaaten stand schon immer das Recht auf Informationsfreiheit im Vordergrund (USA 1966 Freedom of Information Act). Informationsfreiheit beinhaltet jedoch nicht nur ein allumfassendes Recht auf Auskunft, sondern schließt auch staatliche und private Interessen an Geheimhaltung mit ein (Tinnefeld und Ehmann 1994). Datenschutz heißt informationelle Selbstbestimmung des Einzelnen und schützt zugleich seine privaten Interessen an Geheimhaltung. Erst in den letzten Jahren haben sich beide Grundsätze angenähert. Dies hat weltweit zu einer Stärkung des Datenschutzes geführt, ohne jedoch in einer internationalen Übereinkunft des Umganges mit dem Datenschutz zu enden, wie es in anderen Bereichen, zum Beispiel durch Basel II für das Kreditwesen, möglich wurde.

Möchte ein Unternehmen personenbezogene Daten wie zum Beispiel Mitarbeiterdaten, Gesundheitsdaten von Patienten oder Kundenstammdaten nur innerhalb der EU verarbeiten, dann gibt es diesbezüglich konkret einzuhaltende Vorgaben,

¹ The Corporate Compliance Officer oversees the Corporate Compliance Program, functioning as an independent and objective body that reviews and evaluates compliance issues/concerns within the organization. The position ensures the Board of Directors, management and employees are in compliance with the rules and regulations of regulatory agencies, that company policies and procedures are being followed, and that behavior in the organization meets the company's Standards of Conduct.

² Im Folgenden wird unter dem Oberbegriff Verarbeitung sowohl die Speicherung, wie auch Veränderung, Sperrung, Löschung und Übermittlung verstanden.

die durch die EU-Datenschutzrichtlinie innerhalb der Mitgliedsländer der EU auch vergleichbar geregelt sind.

Für Unternehmen, die personenbezogene Daten jedoch außerhalb der EU verarbeiten möchten, stellt sich die Frage, welche Datenschutzbestimmungen anzuwenden sind: die der EU, die des Empfängerlandes, die des Landes, in dem die personenbezogenen Daten verarbeitet werden sollen, alle Bestimmungen zusammen oder nur Teile daraus? Reicht eine vertragliche Regelung zwischen den verarbeitenden Unternehmen oder bedarf es der vorherigen Zustimmung jedes einzelnen Betroffenen zu der Verarbeitung seiner Daten? Diese oder ähnliche Fragestellungen dürften dazu geführt haben, dass gemäß einer weltweiten Umfrage unter 808 IT-Verantwortlichen 2004/2005 70% der in der USA, 55% der in Asia-Pacific und 48% der in EMEA befragten IT-Verantwortlichen Datenschutzbelange als größte Herausforderung für ihre Unternehmen bezeichnet haben (Mercury 2005). Hierbei wurde insbesondere festgestellt, dass nicht etwa Strafandrohungen der anzuwendenden Datenschutzbestimmungen die IT-Verantwortlichen zu dieser Einschätzung haben kommen lassen, sondern die Reputationsverluste betroffener Unternehmen bei Publikwerden von Datenschutzverstößen.

Im Gegensatz zur Datensicherheit (siehe unten) gibt es derzeit keine international anerkannte Möglichkeit eines Datenschutzzertifikates, das einem Unternehmen dessen Datenschutzniveau bescheinigt. Auch wurde bisher ein Konzernprivileg bei der Verarbeitung personenbezogener Daten von den Aufsichtsbehörden abgelehnt, so dass ein Unternehmen, das über weltweit verteilte Tochterunternehmen verfügt, eine eigenständige Lösung für die Datenschutzfragen finden muss. Diese Lösung muss jedoch unbedingt in einen Kontext mit den übrigen im Unternehmen existierenden Regelwerken zur Informationsverarbeitung gestellt werden und ihren Niederschlag in der IT-Governance finden.

2.6.2 Anforderungen an die Datensicherheit

Dass derzeit noch kein „Datensicherheitsgesetz“ existiert, sollte nicht den Eindruck erwecken, dass es keine externen Datensicherheitsanforderungen an die IT gibt. Leider trifft eher das Gegenteil zu. Im Gegensatz zu Datenschutzanforderungen finden sich diese Anforderungen mehr oder weniger deutlich ausgeprägt in jeder der im Folgenden beispielhaft behandelten Anforderungen wieder. Auch nur einen Teil dieser Anforderungen vertieft an dieser Stelle behandeln zu wollen, würde den Rahmen dieses Werkes sprengen.

Die *GoBS* (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme) stellt lediglich eine Präzisierung der Grundsätze ordnungsgemäßer Buchführung (GoB) im Hinblick auf die DV-Buchführung dar und bezieht sich auf alle Prozesse, in denen außerhalb des eigentlichen Buchhaltungsbereichs buchführungsrelevante Daten erfasst, erzeugt, verarbeitet oder übermittelt werden. Die *GoBS* führt aus, dass die starke Abhängigkeit der Unternehmen von ihren gespeicherten Informationen ein ausgeprägtes Datensicherheitskonzept für das Erfüllen der *GoBS* unabdingbar

macht und beschreibt recht detailliert Anforderungen an solch ein Datensicherheitskonzept. Insofern führt die GoBS Datensicherheitsanforderungen zum Schutz buchführungsrelevanter Daten innerhalb eines Unternehmens ein.

Operative Risiken und daraus abgeleitete Datensicherheitsanforderungen an die IT durch *Basel II*: 1988 legte der Baseler Ausschuss für Bankaufsicht (Vertreter der Zentralbanken und der nationalen Aufsichtsbehörden der führenden Industrieländer) mit Basel I Eigenkapitalrichtlinien in Abhängigkeit von vergebenen Krediten für Banken fest. Basel II (beschlossen im 2. Quartal 2004, geltend ab 1.1.2007) erweitert diese Richtlinien. Berücksichtigt bei der Absicherung mit Eigenkapital der Banken werden in Basel II auch die individuellen Ausfallrisiken von Krediten an Bankkunden sowie operative Risiken der Banken (z. B. IT-Ausfall, Naturkatastrophen).

Da die Banken ihre Erfahrungen mit ihren eigenen operativen Risiken bei der Berechnung der individuellen Ausfallrisiken von Krediten der Bankkunden mit einbeziehen werden, ergeben sich erhebliche Datensicherheitsanforderungen an die IT der Unternehmen, wenn diese nicht zukünftig mit schlechteren Kreditkonditionen leben möchten.

Datensicherheitsanforderungen des *Sarbanes–Oxley Act* von 2002 für in den USA börsennotierte Firmen für die Verarbeitung von Finanzdaten: Als Reaktion auf die Bilanzskandale in Konzernen wie Enron oder WorldCom, wo mittels gefälschter Bilanzen die eigentliche Schuldenlage verborgen wurde, wurde in den USA am 30. Juli 2002 der Sarbanes–Oxley Act (SOX) erlassen. Der Sarbanes–Oxley Act enthält elf Artikel – unter anderem die Pflicht zur Bestätigung der Richtigkeit der Jahresabschlüsse und Berichte sowie zur rechtzeitigen Offenlegung durch das Management (Section 302), wie auch die Pflicht zum Aufbau eines internen Kontrollsystems durch das Management und zur regelmässigen Überprüfung (Section 404). Insofern stellt SOX auch ganz erhebliche Anforderungen an die Datensicherheit bei der Verarbeitung der Finanzdaten, da die Pflicht zur Bestätigung der Richtigkeit der Jahresabschlüsse eine persönliche Haftung der CEOs und CFOs einschließt.

Eine mögliche Gegenstrategie gegen die aufgezeigten Anforderungen an die IT und die Datensicherheit kann in der Einführung und vor allem auch in der öffentlichen Darstellung einer Zertifizierung eines anerkannten Datensicherheitsstandards bestehen. Für nur in Deutschland operierende Unternehmen würde sich dort eine Zertifizierung nach dem IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) anbieten. Global agierende Unternehmen können ab Herbst 2005 durch eine Zertifizierung nach der ISO 27001 in Verbindung mit der ISO/IEC 17799: 2005 ihren aktuellen international anerkannten Datensicherheitsstandard darstellen.

Solch eine Zertifizierung entbindet die Unternehmen nicht davon, für besonders sensible Daten (zum Beispiel personenbezogene oder SOX-relevante Daten) zusätzliche Datensicherheitsmaßnahmen zu treffen. Eine Zertifizierung dokumentiert jedoch, dass ein Unternehmen den Schutz jeglicher Daten ernst nimmt. Für jegliche Art von Zertifizierung gilt aber auch, dass sowohl von der angewandten Methodik wie auch von den Zielen her eine Verzahnung erfolgen muss. Bei jeder Einzelmaßnahme muss „das Ganze“ im Auge behalten werden. Das bedeutet, dass man

einen „Bebauungsplan“ für die Einzelmaßnahmen entwickeln muss, um im Sinne einer proaktiven Lösung und einer ganzheitlichen IT-Governance keine regulatorischen „Silos“ entstehen zu lassen. Ein Return on Invest aus all diesen Bemühungen könnte sich spätestens unter Basel II-Aspekten hinsichtlich eines guten Ratings eigener operativer Risiken und somit besserer Kreditkonditionen ergeben.

2.6.3 Spezielle Anforderungen der Gesundheitsbehörden

Neben einem hohen Eigeninteresse an geregelten Abläufen gelten für die pharmazeutische Industrie, zusätzlich zu den für alle Unternehmen geltenden Anforderungen des KonTraG (Gesetz zur Kontrolle und Transparenz), der Buchprüfer (IDWERS, EPS³) und der Finanzbehörden (GDPdU⁴), gesetzliche und regulatorische Anforderungen der nationalen (GMP Annex 11⁵) und internationalen (FDA⁶) pharmazeutischen Überwachungsinstitutionen an qualitätsgesicherte Prozesse. Für europäische Inspektoren gilt die Pharmaceutical Inspection Convention / Scheme (PIC/S), die, wie auch Veröffentlichungen der FDA (21 CFR Part 11⁷), zur Umsetzung auf den GAMP-Leitfaden (GAMP 4⁸) als Industriestandard verweist.

Der Grund für diese spezielle Regulierung liegt natürlich in der Bedeutung der medizinischen und pharmazeutischen Produkte für das tägliche Leben und das Wohlbefinden einer Vielzahl von Patienten. In der Praxis sind eine Vielzahl von Prozessen in Forschung, Entwicklung, Fertigung sowie auch Marketing und Vertrieb betroffen. Das nachweisliche Einhalten dieser Anforderungen und Vorschriften (Compliance) ist letztendlich entscheidend für die Zulassung von Medikamenten und die Erlaubnis, diese dauerhaft zu vertreiben.

Compliance mit den Anforderungen und Vorschriften, wie auch das Einhalten des erreichten Niveaus in den betroffenen Prozessen, hat für die betroffenen Unternehmen eine existentielle Bedeutung; in diesem Sinne kann man Compliance also durchaus zu den Kernkompetenzen der betroffenen Unternehmen zählen. Dies gilt im Übrigen ähnlich für andere Industrien wie z. B. die Lebensmittelindustrie.

In pharmazeutischen Firmen werden natürlich fast alle Prozesse durch eine informationstechnische Infrastruktur unterstützt. Eine Vielzahl von Abläufen sind ohne

³ IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie (IDW ERS FAIT 1), IDW Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie (IDW EPS 330).

⁴ Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) des Bundesministeriums für Finanzen

⁵ Annex 11 des Guide to GMP, als europäisches Recht

⁶ manifestiert durch ausgeübte Inspektorenpraxis der Food and Drug Administration, FDA

⁷ 21 CFR Part 11 - Electronic Records: Electronic Signatures und Guidance for Industry Part 11, Electronic Records: Electronic Signatures - Scope and Application

⁸ Good Automated Manufacturing Practice (GAMP), Leitfaden zur Validierung automatisierter Systeme (GAMP 4)

den Einsatz von Informationstechnologie nicht mehr vorstellbar bzw. schlichtweg undurchführbar.

Deshalb sind bei der Ausrichtung der IT an den Unternehmenszielen und -prozessen diese Anforderungen durch das Etablieren eines Qualitätsmanagementsystems zu erfüllen, da hierdurch ein verantwortungsvoller und nachhaltiger Einsatz der IT-Ressourcen (Mitarbeiter, Systeme und finanzielle Mittel) gewährleistet ist. Denn durch dokumentierte, qualitätsgesteuerte Prozesse lassen sich die auf die Integrität der Daten einwirkenden IT-Risiken minimieren.

Die Infrastruktur im Fokus

Heißt es noch im §5 des Annex 11 des Guide to GMP: „Software ist eine kritische Komponente eines computergestützten Systems. Der Benutzer solcher Software sollte alle erforderlichen Maßnahmen treffen, um sicherzustellen, dass sie in Übereinstimmung mit einem Qualitätssicherungssystem erstellt worden ist“, so hat sich nach einem Jahrzehnt der Validierungen von Anwendungssystemen der Fokus der Inspektoren auf die Qualifizierung der Infrastruktur als Basis dieser Systeme verlagert, da validierte Applikationen eine qualifizierte Infrastruktur verlangen. Der Leitfaden führt hierzu aus: „Anwenderfirmen sollten Qualitätssysteme einrichten, die eine qualifizierte Infrastruktur bereitstellen, um die validierten Anwendungen zu unterstützen. Die Qualifizierung der Infrastruktur sollte den dokumentierten Nachweis erbringen, dass die Infrastruktur mit hoher Wahrscheinlichkeit dauerhaft und bestimmungsgemäß arbeitet sowie die Spezifikationen einhält.“

Das Qualitätsmanagementsystem für die Infrastruktur

Das Qualitätsmanagementsystem sollte strukturiert mit aufeinander aufbauenden Regeln, vom Allgemeinen zum Spezifischen, entwickelt sein und einem Außenstehenden eine Vorstellung von den qualitätssichernden Elementen im Betrieb der Infrastruktur vermitteln. Die Beschreibung des Systems geschieht in der Regel dadurch, dass übergeordnete Prinzipien, weiterführende Direktiven und abschließend wiederum detaillierte Handlungsanweisungen (Prozeduren) spezifiziert werden. Für die Arbeitsprozesse der betroffenen Mitarbeiter werden dann entsprechend auf die Tätigkeit des Mitarbeiters speziell abgestellte Handbücher und Arbeitsanweisungen verfasst. Diese Prozesse sollten einem internationalen Standard, wie zum Beispiel dem der ITIL (Information Technology Infrastructure Library), folgen.

Teil des Regelwerkes ist auch die Beschreibung von Zuständigkeiten und Aufgaben aller Beteiligten: vom Chief Information Officer (CIO) über die qualitätssichernde Funktion für die Infrastruktur bis hin zum Leiter der Rechenzentren und die jeweiligen Mitarbeiter (Qualitätsbeauftragte, Qualifizierungsverantwortliche, Qualifizierungskordinatoren). Teil des Regelwerkes ist auch die Beschreibung des Systems selbst. Die Verfahren zum Betrieb eines Qualitätsmanagementsystems, einschließlich der Überwachung der Qualitätskonformität der Abläufe und der Durchführung von Selbstaudits, und zum Erreichen der Qualifizierung der

IT-Infrastruktur werden betrachtet und detailliert festgeschrieben. Diese „Meta-sicht“, also eine Beschreibung der Beschreibung, ist jedoch ein charakterisierendes Element von Regelwerken der Kategorie „Governance“.

Ziel des Qualitätsmanagementsystems ist auch die Information der jeweiligen Leitungsebene mit dem Ziel, korrigierende Maßnahmen einleiten zu können. Neben der Transparenz über das Zusammenspiel der betrachteten Komponenten und Systeme, Informationen über die Wirksamkeit und Vollständigkeit der Qualifizierungsmaßnahmen muss das System hierzu auch über die von ihm gelieferten Informationen die Beurteilung sowie die zielgerichtete Weiterentwicklung des Qualitätsstandards ermöglichen. Unter dem Strich muss auch für das Themengebiet der hier behandelten speziellen Anforderungen festgestellt werden, dass der Betrieb einer globalen IT-Infrastruktur unter dem Aspekt des Qualitätsmanagements zum Zweck, den qualifizierten Betrieb zu sichern und nachzuweisen, ohne übergreifende Governance wirtschaftlich nicht möglich sein wird. Informationstechnologie als Querschnittsfunktion kann einfach nicht auf jede Anforderung regulatorischer Natur individuell reagieren, sondern muss die „Querschnittsforderungen“ durch ein einheitliches Vorgehen ganzheitlich und nachhaltig adressieren können.

2.7 Fazit

Die IT, bzw. das Management der IT, kann dem externen Druck ohne eine neutralisierende (Schutz-) Schicht nicht auf Dauer standhalten. Um im Bild zu bleiben: Mangels geeigneter Möglichkeiten, argumentativ und systematisch ausgleichenden Gegendruck aufzubauen zu können, wird sich die IT nicht aus ihrer Verteidigungshaltung befreien können. Es muss klar sein, dass es hierbei nicht um das Aufrüsten zweier Lager geht, sondern im Gegenteil um den Brückenschlag zwischen den Lagern.

Daher ist im Sinne des im Vorwort eingeführten Schaubildes eine vermittelnde und übersetzende Instanz in Form der IT-Governance vonnöten, damit alle Beteiligten in der Interaktion und Kommunikation miteinander auf ein neutrales Regelwerk zurückgreifen können.

Externen gesetzlichen, regulatorischen oder fremdmotivierten Anforderungen unterschiedlichster Ausprägung ausgesetzt, kann eine moderne IT durch eine geeignete IT-Governance-Strategie eine ihrer Wichtigkeit im Unternehmen angemessene Rolle ausfüllen und als Innovator wahrgenommen werden (Mercury 2004). Ohne diese dürfte sich eine Unternehmens-IT in kürzester Zeit in der Rolle eines „Geschäftsablaufbremsers“ wiederfinden, der bei dem Versuch, alle diesbezüglichen externen Anforderungen gleichberechtigt zu erfüllen, die Hauptaufgabe, eine das Business unterstützende IT-Dienstleistung anzubieten, nicht mehr erfüllen kann. Positiv betrachtet, kann die IT aber auch mal wieder eine Vorreiter-Rolle im Unternehmen spielen. Die Chance ist da und dieses Buch hat den Anspruch, das notwendige Rüstzeug hierfür zu liefern.

IT-Governance in der Praxis

Erfolgreiche Positionierung der IT im Unternehmen.

Anleitung zur erfolgreichen Umsetzung regulatorischer und wettbewerbsbedingter Anforderungen

(Eds.) A. Rüter; J. Schröder; A. Göldner; J. Niebuhr

2010, XXVII, 250 S. 200 Abb., 100 in Farbe., Hardcover

ISBN: 978-3-642-03504-3