UNIVERSITÄT DUISBURG-ESSEN

Risiko-orientierte Analyse, Bewertung und Ausgestaltung der Sicherheit von Informationssystemen

Revision und Controlling der IT-Security

Dissertation der Universität Duisburg-Essen
Institut für Informatik und Wirtschaftsinformatik
zur Erlangung des akademischen Grades eines

Doktors der Wirtschaftswissenschaften (Dr. rer. pol.)

vorgelegt von

Dipl.-Ing. Dipl.-Wirt.Inf. Thomas Collenberg

geboren in Essen

Disputation: 12.10.2007

Erstgutachter: Prof. Dr. Stefan Eicker

Zweitgutachter: Prof. Dr. Reinhard Voßbein

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

ADS	Administrations- und Dispositionssystem
AG	Aktiengesellschaft
AICPA	American Institute of Certified Public Accountants
ALE	Annulized Loss Expectance
ARIS	Architektur integrierter Informationssysteme);
AktG	Aktiengesetz
ATM	Asynchronous Transfer Mode
AVE	ARIS Value Engineering
B2C	Business-To-Consumer
Basel II	Eigenkapitalvorschriften des Basler Ausschusses für Bankenaufsicht
BDSG	Bundesdatenschutzgesetzes
BGB	Bürgerliches Gesetzbuch
BI	Business Intelligence
BilKoG	Bilanzkontrollgesetz
BilReG	Bilanzrechtsreformgesetz
BPM	Business Process Management
BS	British Standard
BSC	Balanced Scorecard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CEO	Chief Executive Officer
CMMI	Capability Maturity Model Integration
CPM	Corporate Performance Management
CFO	Chief Financial Officer
CISM	Certified Information Security Manager
CMDB	Configuration Management Database
CObIT	Control Objectives for Information and related Technology
COSO	Commitee of Sponsoring Organisations of the Treadway Commission
DCF	discounted cash flow
DHCP	Dynamic Host Configuration Protocol
DIN	Deutsches Institut für Normung e.V.
DNS	Domain Name System
DOS	Denial of Service
DRS	Deutscher Rechnungslegungsstandard
DV	Datenverarbeitung

EAL	Evaluation Assurance Level
EDI	Electronic Data Interchange,
EIS	Executive Information System
EN	Europäische Norm
ERM	Enterprise Risk Management Framework
ERP	Enterprise Ressource Planning
EIS	Executive Information System
EUS	Entscheidungsunterstützendes System
EDV	Elektronische Datenverarbeitung
ESB	Enterprise Service Bus
EJS	Enterprise Job Scheduling
FAIT	Fachausschusses für Informationstechnologie
FMEA	Fehlermöglichkeits- und -einflussanalyse
FTP	File Transfer Protocol
GenG	Gesetz betreffend die Erwerbs- und Wirtschaftsgenossenschaften
GLIB	Gramm-Leach-Billey-Act
Gmbh	Gesellschaft mit beschränkter Haftung
GmbhG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GMITS	Guidelines on the Management of IT-Security
GMX	Global Message eXchange
GoB	Grundsätze ordnungsgemäßer Buchführung
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
GoÜ	Grundsätze Risiko-orientierter Unternehmensüberwachung
GPSG	Geräte- und Produktsicherheitsgesetz:
GSHB	Grundschutzhandbuch
HFA	Hauptfachausschuss
HGB	Handelsgesetzbuch
HTTP	Hypertext Transfer Protocol
HW	Hardware
IAS	International Accounting Standards
IDS	Intrusion Detection/System
IDW	Institut der Wirtschaftsprüfer in Deutschland e. V.
IEC	International Electrotechnical Commission
IFAC	International Federation of Accountants
IKS	Internes Kontrollsystem
IMS	Integriertes Managementsystem
IP	Internet Protocol

IPsec	IP Security
IPT	IP-Telefonie
IPS	Intrusion Prevention System
IRB	Internal Ratings-Based
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Informationstechnologie
ITIL	IT Infrastructure Library
IuK	Informations- und Kommunikationstechnik
IV	Informationsverarbeitung
KapCoRiLiG	Kapitalgesellschaften- und Co-Richtliniengesetz
KG	Kommanditgesellschaft
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KWG	Kreditwesengesetz
LAN	Local Area Network
MaH	Mindestanforderungen an das Betreiben von Handelsgeschäften der Kreditinstitute
MaIR	Mindestanforderungen an die Ausgestaltung der Internen Revision der Kreditinstitute
MaK	Mindestanforderungen für das Kreditgeschäft der Kreditinstitute
MaRisk	Mindestanforderungen an das Risikomanagement
MICTS	Management of information and communications technology security
MIS	Management-Informations-System
MLS	Multiple Listing Service
NIR	Nettoinvestitionsrate
NOPLAT	Net operating profit less adjusted taxes
OASiS	Organization for the Advancement of Structured Information Standards
OHG	Offene Handelsgesellschaft
OLAP	Online Analytical Processing
OLTP	Online Transaction Processing
ÖNR	Österreichische Norm
OSI	Open Source Initiative
PCAOB	Public Company Oversight Board
PDA	Personal Digital Assistent
PDCA	Plan-Do-Check-Act
PET	Privacy Enhancing Technologies

PP	Protection Profile
PS	Prüfungsstandard
PublG	Publizitätsgesetz
RMA	Risk Management Association
RMIS	Risk Management Informationssystem
ROIC	Return on Invested Capital
RoSI	Return on Security Investment
RS	Rechnungslegungsstandard
SAML	Security Assertion Markup Language
SEC	U.S. Securities and Exchange Commission
SIC	Standing Interpretations Committee
SKM	strategisches Kontinuitätsmanagement
SLA	Service Level Agreement
SOA	Service-orientierten Architektur
SOAP	Simple Object Access Protokoll
SOP	Statement of Position
SOX	Sarbanes Oxley-Act
SREP	Supervisory Review and Evaluation Process
SSE-CMM	System Security Engineering – Capability Maturity Model
ST	Security Target
SW	Siftware
TR	Technical Report
TBO	Total Benefit of Ownership
TCO	Total Cost of Ownership
TR	Technical Report
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UMTS	Universal Mobile Telecommunications System
US-GAAP	Generally Accepted Accounting Principles in the United States
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAF	Web Application Firewall
WKN	Wertpapierkennnummer
WLAN	Wireless Local Area Network

WP	Wirtschaftsprüfer
WPG	Wirtschaftsprüfungsgesellschaft
WSDL	Web Services Description Language
XML	Extensible Markup Language

A Einführung

IT ist zur Unterstützung der Geschäftsprozesse eines Unternehmens unverzichtbar. Im Mittelpunkt derzeitiger Überlegungen stehen die Flexibilisierung der IT und die Harmonisierung der Prozesse. Von besonderer Bedeutung für die zukünftige Entwicklung ist die Nachfrage nach erhöhter IT-Security/IT-Sicherheit. Der schnelle, fehlerfreie Zugriff auf Informationen ist ein entscheidender Erfolgsfaktor. Wenn die IT-Infrastruktur das elektronische Abbild aller Geschäfts- und Entscheidungsfindungsprozesse darstellt, können Risiken der IT-Sicherheit den Regelbetrieb massiv gefährden. Dieser Regelbetrieb soll die größtmögliche Wertschöpfung mit einem akzeptablen Risiko erreichen.

Die Beherrschung von Risiken gehört zu den strategischen Feldern eines Unternehmens. Risiken zu erkennen und zu mindern oder zu vermeiden, sichert den mittel- und langfristigen Geschäftserfolg. Für jedes Unternehmen stehen neben Markterfolgen die Erkennung und Steuerung der vorhandenen Risiken im Vordergrund.

Im Mittelpunkt steht die Beherrschbarkeit der IT-Risiken. Technische Produkte sind dabei ein sehr wichtiger Bestandteil jeder modernen Sicherheitsarchitektur. Firewalls[1], Virenschutzsysteme, Zugangs- und Zugriffskontrollsysteme, Scanner oder Baseline Analyser sind in vielen Unternehmen Standard geworden. Neben den technischen Maßnahmen sind die benötigten generischen Richtlinien sowie Konzepte zum Umgang mit IT-Risiken zwecks Gewährleistung des Regelbetriebs mit größtmöglicher Wertschöpfung bei akzeptablem Risiko von Bedeutung.

Gerade bezüglich neuer bzw. sich etablierender Technologien wie z. B. VoIP kann dabei die erforderliche Sicherheit nur mit einem „professionellen Sicherheitskonzept, das dynamisch an technologische Weiterentwicklungen und neue potenzielle Angriffsziele anpassbar ist sowie einer unternehmensweiten Sicherheitspolitik“ angestrebt werden.[2]

Sicherheit muss das System – seine Komponenten und seine Verbindungen - durchdringen. Dabei hat Sicherheit neben vorbeugenden Technologien mit Prozessen, mit Erkennungs- und Reaktionsprozessen zu tun. Sicherheit ist kein Produkt, sie ist ein Prozess.[3]

Technische Lösungen sind eine notwendige, aber nicht hinreichende Bedingung für umfassende IT-Security/IT-Sicherheit. Ohne einen angemessenen organisatorischen Schutz, z. B. des internen Netzwerkes, verfügen weiterführende Maßnahmen nicht über das notwendige

[1] vgl. Strobel, Stefan (2003)
[2] vgl. Poels, Torsten. (2004b)
[3] vgl. Schneier, Bruce (2000), S.X

Fundament. Um das eigene Firmennetzwerk zu schützen, benötigt man aber weitaus mehr als eine Firewall. Um unerwünschte Zugriffe von außen zu unterbinden, ist der Einsatz einer Firewall eine notwendige, aber noch lange keine hinreichende Bedingung. Integritätsaspekte der Informationsverarbeitung erfordern eine genaue Analyse des Informationsflusses und den Schutz vor veralteten, unvollständigen, inkonsistenten Daten. Ebenso bedeutend sind organisatorische Vorkehrungen und die Sensibilisierung der Belegschaft: Die Bestellung eines betrieblichen Datenschutzbeauftragten ist eine notwendige, aber üblicherweise keinesfalls hinreichende Bedingung für die Umsetzung des Bundesdatenschutzgesetzes (BDSG) im Unternehmen. Von zentraler praktischer Bedeutung ist unter anderem eine auf das jeweilige Unternehmen zugeschnittene, verständliche Erläuterung aller für die Mitarbeiter relevanten Bestimmungen.

Für den Terminus „IT-Sicherheit“ gibt es eine gesetzliche Legaldefinition: § 2 Abs. 2 BSI-Errichtungsgesetz[1] sagt: „Sicherheit in der Informationstechnik…. bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen 1. in informationstechnischen Systemen oder Komponenten oder 2. bei der Anwendung von informationstechnischen Systemen oder Komponenten“. Diese Definition ist neutral in dem Sinne, dass sie erst konkret z. B. zur Bewertung angewandt werden kann, wenn die in Bezug genommenen „Sicherheitsstandards“ einbezogen werden. Diese müssen im konkreten Fall erst als maßgeblich bestimmt werden.[2]

Für die IT-Sicherheit ist neben Hard- und Software außerdem das IT-Personal von zentraler Bedeutung. Menschliches Fehlverhalten ist eine der häufigsten Ursachen für Sicherheitsverletzungen. Diesbezüglich sollte die unternehmensweite Sicherheitspolitik auf die interne bzw. externe Weiterbildung des Personals im Bereich von Kenntnissen zu Themen der IT-Sicherheit setzen. Beispielhaft sei hier die herstellerneutrale Qualifizierung zum Certified Information Security Manager (CISM) genannt. Diese Zertifizierung der Information Systems Audit and Control Association (ISACA) richtet sich an Führungskräfte/Manager, die die IT-Sicherheit auch bezüglich ihrer betriebswirtschaftlichen Notwendigkeit betrachten müssen.[3]

Das Ziel der IT-Security/IT-Sicherheit wird letztlich durch eine unternehmensweit fortlaufend auszuführende Abfolge von Tätigkeiten angestrebt, dem sog. IT-Sicherheits-/IT-Security-Prozess.

[1] Bundesgesetzblatt 1990 Teil I Seite 2834
[2] vgl. Sonntag, Matthias (2005), S.20,21
[3] vgl. Schmitz, Ulrich (2004)

IT-Security stellt die IT-Sicherheit bezüglich der Informationssicherheit dar. Vielfach werden auch IT-Security und IT-Sicherheit gleichgesetzt. Strategisch gesehen ist IT-Security Teil einer ganzheitlichen Sicherheitsstrategie. Bei der Ausprägung IT-Safetty geht es dagegen um die Funktions-, Zustands-, Betriebssicherheit von IT-Systemen und IT-Produkten.

Die internen und externen Gefährdungspotenziale der IT-Security/IT-Sicherheit müssen zunächst transparent gemacht und analysiert werden. Ansonsten kann ein angemessenes IT-Sicherheits-/IT-Security-Management nicht installiert werden. Dieses IT-Sicherheits-/IT-Security-Management muss sich kontinuierlich an Veränderungen im laufenden Geschäftsbetrieb anpassen. Im Zusammenhang mit der vorliegenden Thematik steht die Analyse der Bedeutung von Risiken der IT-Security für die Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse (mit Bezug auf die Anforderungen an die Informationssicherheit der von diesen benötigten Daten und die Sicherheit der sie unterstützenden IT-Systeme) im Mittelpunkt. Diese Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse hat die Unterstützung strategisch-operativer Handlungsspielräume zum Ziel.

Im Falle der E-Logistik müssen etwa die Möglichkeiten zur

- gezielten Informationsversorgung der Kunden durch einen geschützten elektronischen Zugang und strukturierte Recherchemöglichkeiten,
- Anbindung sämtlicher Abwicklungs- und Supportprozesse der beteiligten Geschäftspartner,
- Durchgängigkeit der Prozesse mit einem direkten Transfer von Aktionen und Reaktionen,
- Gewährleistung einer hohen Sicherheit und einer hohen Qualität bei Waren- und Informationstransporten

unterstützt werden.[1]

Der Ansatz der IT-Abteilung basiert darauf, bei der Entwicklung und Optimierung ihrer Systeme zunächst den „störungsfreien Betrieb“ sicherzustellen. Diese Forderung an das IT-Management ist zu erweitern um Potenziale für eine positive Auswirkung auf den Ertrag des Unternehmens.[2]

Der Unternehmenserfolg wird durch die Handlungsspielräume bzw. die durch die Umwelt vorgegebenen Strategiealternativen beeinflusst. Auf die Rahmenbedingungen, unter denen ein Unternehmen existiert, beziehen sich die externen Erfolgsfaktoren.[3] Die organisatorische Abwicklung der Geschäftsprozesse ist dagegen ein interner Erfolgsfaktor und bezieht sich auf

[1] vgl. Kirchner, Michael (2002), S.103
[2] vgl. Grawe, Tonio (2007), S.38
[3] vgl. Reichling, Peter (2003), S.208

die mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens.

Diese Handlungsspielräume zu analysieren und abzusichern, dies soll die zusätzliche Aufgabe des zu entwickelnden strategisch-operativen IT-Security-Managements sein, in das das klassische IT-Security-Management integriert werden kann, bzw. das das klassische IT-Security-Management lenkt und steuert.

Das IT-Sicherheits-/IT-Security-Management muss kontinuierlich an sich verändernde Umfeldbedingungen angepasst und weiterentwickelt werden. Dies sollte gezielt und nachvollziehbar gesteuert werden. Prüfungen im Sicherheitsmanagement beurteilen, ob das angestrebte Sicherheitsniveau erreicht, die kontinuierliche Anpassung und Weiterentwicklung sowie deren gezielte und nachweisbare Steuerung gewährleistet sind. Um den Untersuchungsgegenstand festzulegen, ist zu klären, was woraufhin in welchem Detaillierungsgrad von wem zu untersuchen ist. Das „was" betrifft die Untersuchungsobjekte: Geschäftsprozesse, sie unterstützende Informationssysteme und Infrastrukturen. Das „woraufhin" sind die betrachteten internen und externen Vorgaben, Sicherheitskriterien (z. B. Verfügbarkeit, Vertraulichkeit, Integrität) und Sicherheitsstandards. Der Detaillierungsgrad ist mitbestimmend für Aufwand und Dauer der Untersuchung. Für das „von wem" kommen der IT-Sicherheitsverantwortliche des Unternehmens, externe Berater oder die Revision in Betracht.

Aufgrund immer neu auftauchender Bedrohungen und Schwachstellen muss die Wirkung des Sicherheitsmanagements mit seinen Konzepten, Maßnahmen und deren Umsetzung zudem kontinuierlich geprüft werden. Dazu werden z. B. Penetrationstests [1] eingesetzt.

Im Kontext der vorliegenden Thematik wird die kontinuierliche Anpassung und Weiterentwicklung des IT-Sicherheits-/IT-Security-Managements, deren gezielte Steuerung zur Herstellung von Entscheidungsfreiheit/Flexibilitätspotenzialen bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens betrachtet, um sich ungewissen Umweltentwicklungen, wenn diese gewisser werden, anpassen zu können.

Steuerung bedeutet Bereitstellung aller für die Erreichung des Unternehmensziels notwendigen Informationen, laufende Beobachtungen der Planziele und Vergleich mit der Ist-Entwicklung.[2] Mit der Entwicklung eines umfassenden Modells zum Controlling der IT-Security soll die Effektivität und Effizienz der Strukturen und Prozesse des IT-Security-Managements im Sinne der strategischen und operativen Ausrichtung und Umsetzung sichergestellt werden. Gegenstand dieses Controllings sind die durch die IT-Security beeinflussten

[1] Glemser, Tobias (2006)
[2] Peemöller, Volker H. (2005), S.44

Informationsverarbeitungs- bzw. Technologierisiken, die entstehen, wenn die Informationstechnologie „die gegenwärtigen und zukünftigen Geschäftsbedürfnisse nicht ausreichend unterstützt sowie nicht wirtschaftlich und sicher genutzt werden kann“.[1] Management und Controlling sind untrennbar verbunden.[2] Das zu entwickelnde IT-Security-Management hat die gleichen Ziele wie das unternehmerische Risikomanagement-System es hat sicherzustellen, dass den unternehmerischen Erfolg gefährdende Risiken frühzeitig erkannt sowie adäquat gesteuert werden. Risiken resultieren hierbei aus der Ungewissheit der Zukunft, dass aufgrund von Störungen geplante Ziele verfehlt werden könnten.[3] Diese Ziele beziehen sich auf die zu unterstützenden und zu optimierenden bzw. abzusichernden Geschäftsprozesse und zu ermöglichenden Geschäftsmodelle des Unternehmens.

Im Zusammenhang mit neuen Geschäftsmodellen muss das Management eine ausreichende Flexibilität aufweisen, um Strategien im Bedarfsfall z. B. zwecks Ressourcenoptimierung zu überarbeiten und an neue Situationen anzupassen.[4] Die Durchsetzung/Umsetzung von Strategien erfordert (bei IT-gestützten Geschäftsmodellen) eine entsprechende IT-Security der für diese Geschäftsmöglichkeiten notwendigen (bzw. von der Durchsetzung/Umsetzung von Strategien betroffenen) IT-Systeme.

Die vorliegende Arbeit beinhaltet folgende neuen Aspekte bezüglich des IT-Security-Managements:

- Neben der Verlässlichkeit (beurteilt nach den Kriterien Verfügbarkeit, Integrität und Vertraulichkeit) und Beherrschbarkeit (beurteilt nach den Kriterien Nachprüfbarkeit, Rechtssicherheit ((Sicht der Anwender/Benutzer, Sicherheit vor dem Syystem) i. S v. externer Ordnungsmäßigkeit) wird eine dritte Sicht der (strategischen) Bewertbarkeit der IT-Security eines Systems eingeführt. Dies ist die Unterstützung der Strategie konformen und IT-Nutzenpotenzial absichernden Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume, und wird durch die von den Kriterien der beiden erstgenannten Sichten beeinflusste Handlungsbefähigung/Flexibilität/strategisch-operative Beweglichkeit bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und der Geschäftsprozesse/des IT-Security-Prozesses aufeinander modelliert. Diese Sicht beschränkt sich auf die von der Um-

[1] Kirchner, Michael (2002), S.98
[2] vgl. Kütz, Martin (2005), S.6
[3] vgl. Reichling, Peter (2003), S.218
[4] vgl. Kirchner, Michael (2002), S.102

setzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und der Geschäftsprozesse/des IT-Security-Prozesses aufeinander betroffenen IT-Systeme.

- Es wird einer Alternative zur Antizipation von Risiken (Voraussehen negativer Ereignisse und ihrer Folgen) auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen angegeben, die darauf basiert, alle potenziell ex-ante relevanten Anforderungen zu analysieren.
- Darauf aufbauend wird eine ex-ante Revision (bzw. Bewertung) der IT-Security in der Einsatzumgebung des IT-Systems konzipiert: Dazu kann zur Analyse der Bedeutung der IT-Security für das Erreichen der Unternehmensziele/strategisch-operativen Zielsetzungen des Unternehmens der Einfluss der IT-Security auf Handlungsbefähigung/Flexibilität/strategisch-operative Beweglichkeit (bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander) untersucht werden. Dies konkretisiert die ex-ante relevanten Anforderungen an die IT-Sicherheit entsprechender IT-Systeme.

1 Gegenstand der Revision [1] und des Controllings der IT-Security

Revision bezeichnet im Allgemeinen einen Prozess, der anfangend bei der Begutachtung z. B. von Systemen das Ziel verfolgt, diese zu aktualisieren und gegebenenfalls neuen Entwicklungen anzupassen. Z. B. wird auch die regelmäßige Überprüfung eines Ratingprozesses (etwa im Rahmen von Basel II) als Revision bezeichnet.[2] Revision kann als rein abschließende Prüfinstanz, aber auch als Projekt begleitende Aufgabe gesehen werden. Als abschließende Prüfinstanz kann Revision als Funktion interpretiert werden, welche in Form von Prüfungen, d. h. einzelnen Prüfungshandlungen oder einer Folge von Prüfungshandlungen ausgefüllt werden kann. Durch eine Prüfung sollen

- bestimmte Vorgänge nachvollzogen oder vergleichbare Größen gegenübergestellt werden, um ihre Konformität mit Vorgaben oder Normen objektiv zu beurteilen.

Dann handelt es sich zumeist jedoch nur um eine auf die Vergangenheit bezogene (ex-post) Revision. Prüfungen, die nicht das Finanz- und Rechnungswesen des Unternehmens betreffen, werden als „Operational Auditing“ bezeichnet. Dazu zählen etwa Wirtschaftlichkeitsanalysen in Informationssystemen. Audits werden in Form von Soll-Ist-Vergleichen durchgeführt.

[1] dieses Kapitel war Basis die Veröffentlichung: Vossbein, Reinhard/Collenberg, Thomas (2007)
[2] vgl. Reichling, Peter (2003), S.81

Aber auch als Projekt-begleitende Aufgabe (und Aspekt der Überwachung) stehen bei der Revision Soll-Ist-Vergleiche im Mittelpunkt: Revision wird im Hinblick auf den Prozessbezug definiert als

- Prozess unabhängiges (außerhalb des betrieblichen Ablaufs stehendes) Tätigwerden in Form von Soll-Ist-Vergleichen.

Die technische Revision hat aufgrund der Betriebssicherheitsverordnung und Genehmigungsauflagen die Aufgabe, wiederkehrende Prüfungen an Überwachungsbedürftigen und Gefahr geneigten Anlagen durchzuführen bzw. zu organisieren. Dazu gehören auch die sicherheitstechnische und fachspezifische Beratung des Arbeitgebers und der Betreiber von genehmigungs- bzw. prüfpflichtigen Anlagen und Komponenten. Dies dient nicht nur der Anlagensicherheit sondern auch der Verfügbarkeit und dem Werterhalt dieser Anlagen.

Damit die Lösung einer Aufgabe – hier Revision und Controlling der IT-Security – nicht scheitert oder zu einem mangelhaften Resultat führt, muss man wissen, was man tun will oder soll. Außerdem muss man verstehen, warum man es tun soll. Und man muss einen Plan, eine Vorstellung davon haben, wie man es tun kann.[1] Das „warum“ wird am sinnvollsten mit dem Nutzen durch einen zukünftigen Vorteil klar gemacht. Weniger motivierend ist es, einen möglichen Schaden in der Zukunft anzuführen [2]

Revision (wie auch Controlling) wird im Zusammenhang mit der IT-Security im Folgenden als Projekt begleitende Aufgabe bei der Risiko-orientierten Analyse, Bewertung und Ausgestaltung der Sicherheit von Informationssystemen untersucht. Dabei steht die Entwicklung entsprechender Konzepte im Vordergrund. Es geht dabei nicht oder nur am Rande um Aspekte der oben angesprochenen technischen Revision. Im Mittelpunkt steht der strategische Umgang mit Risiken der Informationsverarbeitung resultierend aus der Ungewissheit der zukünftigen Entwicklung im Umfeld des Unternehmens (zwecks Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume).

Revision wird des Weiteren unterteilt in Interne und Externe Revision. Seit KonTraG und verstärkt u. a. durch die Diskussion um den Deutschen Corporate Governance Kodex oder den Sarbanes-Oxley-Act„ prägt sich die Interne Revision als die zentrale, im ‚Querschnitt’

[1] vgl. Weigelt, Lutz (2005)
[2] vgl. Weigelt, Luttz (2005)

wirkende, interne Kontrollinstanz eines Unternehmens aus“.[1] Mit einem systematischen und zielgerichteten Ansatz soll die Effektivität des Risikomanagements, der Kontrollen sowie der Führungs- und Überwachungsprozesse bewertet und verbessert werden.[2] Dabei ist die Interne Revision ein wesentliches Element im Überwachungssystem und für das Risikomanagement-System.[3] Im Bereich Risikomanagement soll das Unternehmen bei der Identifizierung und Bewertung wesentlicher Risikopotenziale unterstützt werden.[4] Die Interne Revision beurteilt den gesamten Managementprozess, um festzustellen, ob ausreichende Sicherheit besteht, die Ziele und Vorgaben zu erreichen.[5] Die Interne Revision richtet sich dabei an Normen zur Ordnungsmäßigkeit, Sicherheit, Wirtschaftlichkeit und Zweckmäßigkeit aus. Dabei ist auch die Zweckmäßigkeit von Beurteilungsmaßstäben zu hinterfragen, indem diese auf Übereinstimmung mit höherwertigen Zielsetzungen untersucht werden.[6] Prüfungsziele betreffen die Ermittlung von Abweichungen und Schwachstellen. Beratungsziele betreffen die Verbesserung von Sachverhalten, Schaffung von Mehrwert.[7] Die Interne Revision beurteilt Effektivität und Effizienz des Kontrollsystems. Im Schwerpunkt des Operational Auditing finden Systemprüfungen von Aufbau- und Ablauforganisation statt. Aber auch die Validierung von Steuerungs- und Entscheidungsvorgängen (sog. Management Auditing) ist ein Gegenstand der Internen Revision. Dabei haben aufgrund der Umweltdynamik zukunftsorientierte Schwachstellenanalysen an Bedeutung gewonnen.[8]

Das interne Kontrollsystem (IKS) besteht nach herrschender Meinung aus dem internen Steuerungssystem, welchem insbesondere das Controlling zugeordnet wird, und dem internen Überwachungssystem, zu dem organisatorische Sicherungsmaßnahmen und die eingerichteten Kontrollen gehören.[9] Zusammengefasst summieren sich im IKS alle Sicherheitsregularien eines Unternehmens.[10] Auch die Interne Revision ist Teil des vom KonTraG geforderten internen Überwachungssystems. Aufgabe des IKS ist die Durchführung ziel- und ordnungsorientierter Kontrollen. Diese Überwachung beeinflusst die Sicherheit, Ordnungsmäßigkeit und Wirtschaftlichkeit betrieblicher Prozesse.[11]

Von der Internen Revision wird nicht mehr nur die Unterstützung der Unternehmensführung bei der Sicherung des Betriebsvermögens und der Überwachung des Einhaltens interner Vor-

[1] Schreiber, Ottokar (2006), S.5
[2] vgl. Förschle, Gerhart/Peemöller, Volker H. (2004), S.152,153
[3] vgl. Lück, Wolfgang (2000), S.14 TZ 36
[4] vgl. Förschle, Gerhart/Peemöller, Volker H. (2004), S.157
[5] vgl. Förschle, Gerhart/Peemöller, Volker H. (2004), S.157
[6] vgl. Förschle, Gerhart/Peemöller, Volker H. (2004), S.162.163
[7] vgl. Förschle, Gerhart/Peemöller, Volker H. (2004), S.154
[8] vgl. Wolf, Klaus (2003b), S.83
[9] vgl. Warncke, Markus (2006), S.61
[10] vgl. Schreiber, Ottokar (2006), S.7
[11] Wolf, Klaus (2003b), S.81

schriften, sondern eine „ständige Adaption an die Bedürfnisse einer modernen Management-Unterstützungsfunktion“ verlangt. Sie soll nunmehr durch ihre umfassenden Prüfungs- und Beratungsleistungen für das gesamte Unternehmen einen Beitrag zur Wertsteigerung und zur Verbesserung sämtlicher Geschäftsprozesse erbringen. Gefordert ist eine Funktion, welche die Unternehmensleitung unterstützt, die Unternehmensrisiken zu überwachen und zumindest indirekt zu steuern.[1] Das in dieser Arbeit zu entwickelnde Modell dient dem Zweck, Risiken der IT-Security indirekt, in Bezug auf ihre Bedeutung für das Erreichen der unternehmerischen Zielsetzungen, zu steuern.

Die Interne Revision soll u. a. eine systematische und anerkannte Vorgehensweise zur Bewertung und Steigerung der Effektivität des Risikomanagements bereitstellen.[2] Die Externe Revision kann z. B. in Form von sog. Risk Advisory bzw. Risk Assessment Services einen Beitrag zum Risikomanagement liefern. Diese beinhalten das Aufspüren potenzieller Risiken für das Unternehmen, die Überprüfung auf Vollständigkeit der vom Unternehmen identifizierten Risiken, die unabhängige Bewertung der entdeckten Risiken oder die Evaluation der unternehmenseigenen Systeme zur Risikoerkennung und -begrenzung.[3]:

Risk Assessment beurteilt zunächst alle externen und internen Unternehmensrisiken und identifiziert Bedrohungen und Angriffspunkte für zu schützende Informationen. Dabei werden alle internen und externen Einflussfaktoren wie Technologie, Personal, Sicherheitspolitik und in Anspruch zu nehmenden sicherheitsrelevanten Dienstleistungen einbezogen. Risk Assessment soll [4]

- das akzeptable Risikoniveau unter Berücksichtigung der Wichtigkeit der zu schützenden Informationen bestimmen. Dazu müssen die Unternehmensziele, die unternehmerische Risikopolitik und die Geschäftsabläufe einer näheren Betrachtung unterzogen werden.

Des Weiteren soll Risk Assessment

- bei der Auswahl von Kontrollmaßnahmen zum Management der Risiken potenzieller Schädigungen der Informationssysteme und Netzwerke unterstützen.

Die Aufgabe der Internen Revision besteht neben Zweckmäßigkeits-, Ordnungsmäßigkeits- und Wirtschaftlichkeitsprüfungen von Aufbau- und Ablaufsystemen, insbesondere des Internen Kontrollsystems aber auch in der Feststellung der Sicherheit (Assurance) bestimmter

[1] vgl. Schroff, Joachim (2006), S.7,8
[2] vgl. Allenspach, Marco (2001), S.97,98
[3] vgl. Allenspach, Marco (2001), S.96
[4] vgl. Collenberg, Thomas/Wolz Matthias (2005), S.139-141

Informationen. Assurance bildet den Oberbegriff für alle Prüfungstätigkeiten wie Audit, Review, Examination, die sich hinsichtlich der Prüfungssicherheit unterscheiden.[1]

Auch Wirtschaftsprüfer versuchen also, dem neben dem Informationsgehalt eines Jahresabschlusses bestehenden Bedarf nach entscheidungsrelevanten Informationen mit neuen Dienstleistungen entgegenzukommen. Diese sog. freiwilligen Prüfungsleistungen (Assurance Services) beruhen nicht auf einer gesetzlichen oder anderen zwingenden Verpflichtung und stellen einen Teilbereich der „assurance engagements“ gemäß IFAC (International Federation of Accountants) dar, die auch die Prüfung und Durchsicht historischer Finanzinformationen umfasst. Die. Assurance Services wurden von der US-amerikanischen Berufsorganisation der Wirtschaftsprüfer American Institute of Certified Public Accountants (AICPA) angestoßen und betreffen u. a. neben Risk Advisory den Bereich Information System Reliability (SysTrust).

Die Assurance Services sollen die Qualität von Information oder von deren Kontext erhöhen, was auch die Beschaffung und Aufbereitung von Informationen zur Steigerung der Zeitnähe (timeliness) und Verfügbarkeit (availability) von Daten einschließt. Qualität stützt sich auf das in den Regelwerken zur Rechnungslegung US-GAAP (Generally Accepted Accounting Principles in the United States) und IAS (International Accounting Standards) verwendete Konzept der „Decision Usefulness“ (Verständlichkeit, Relevanz, Verlässlichkeit, Vergleichbarkeit). „Kontext“ bezieht sich hier auf die Informationsgewinnungs-, Informationsverarbeitungs- und Kommunikationsprozesse. Ziel der Assurance Services nach US-amerikanischem Vorbild ist damit nicht in erster Linie die Abgabe eines Prüfungsurteils, sondern die Qualitätserhöhung von Informationen, Informationsbeschaffungs-, Informationsverarbeitungssystemen oder -prozessen, welche der Entscheidungsfindung des Mandanten dienen.[2] [3]

Im Bereich Finanz- und Rechnungswesen ist die Interne Revision weitgehend mit dem gleichen Gegenstand beschäftigt wie der Wirtschaftsprüfer bei der handelsrechtlichen Abschlussprüfung. Aber auch die Prüfungshandlungen der Internen Revision bei der Prüfung des Internen Kontrollsystems (IKS) und die des Abschlussprüfers bei der Prüfung des internen Überwachungssystems sind vergleichbar.[4]: Die interne Revision hat auch Abschluss-bezogene Informationen zu untersuchen und z. B. Regelungen zu beurteilen, nach denen Informationen aus betrieblichen Prozessen erkannt, gemessen und zugeordnet werden. Von daher stützt sich

[1] vgl. Förschle, Gerhart/Peemöller, Volker.H. (2004), S.153
[2] vgl. Marten, Kai-Uwe/Köhler, Annette G. (2001)
[3] vgl. Collenberg, Thomas/Wolz Matthias (2005), S.104
[4] vgl. IIR (2001): Revisionsstandard Nr. 1,5-7

der Abschlussprüfer regelmäßig auf Feststellungen der Internen Revision.[1] Die Interne Revision hat für ein angemessenes und funktionsfähiges IKS zu sorgen. Sie reduziert dadurch das Risiko, dass durch Mängel im IKS, Fehler oder Unregelmäßigkeiten nicht oder nicht rechtzeitig entdeckt und verhindert werden (Kontrollrisiko). Auf Umfang der Prüfungshandlungen des Abschlussprüfers wirken sich immanente Risiken des entsprechenden Prüfungsgebiets, Kontrollrisiken und Erkennungsrisiken aus. Wenn bei der Abschlussprüfung das Kontrollrisiko aufgrund der Prüfung des internen Überwachungssystems und der Arbeit der Internen Revision als gering eingeschätzt wird, werden bei den immanenten Risiken des Prüfungsgebiets und gleich bleibendem Gesamt-Prüfungsrisiko die Anforderungen an das Erkennungsrisiko des Abschlussprüfers geringer.

Aber auch umgekehrt kann die Externe Revision der Internen Revision zuarbeiten: Als Beispiel sei eine Softwareprüfung zur Beurteilung der Verarbeitungsfunktionen der Software zur Einhaltung der Grundsätze ordnungsmäßiger Buchführung, nach dem Prüfungsstandard „Erteilung und Verwendung von Softwarebescheinigungen“ (PS 880) des IDW (Institut der Wirtschaftsprüfer in Deutschland e. V.) betrachtet. Wenn die Software und das Informationssystem, auf der die Software ablauffähig ist, als Einheit betrachtet wird, kann diese Prüfung dem Bereich „Information System Reliability“ (Beurteilung bestehender Informationssysteme hinsichtlich der Aktualität, zeitnahen Verfügbarkeit, Korrektheit und Zugänglichkeit elektronisch erzeugter Informationen) zugeordnet werden. Es werden die Anforderungen aufgezeigt, die bei der Prüfung von Softwareprodukten und der Erteilung von Bescheinigungen zu Softwareprodukten zu beachten sind.

Beurteilt werden müssen neben den[2]

- für die Einhaltung der Grundsätze ordnungsmäßiger Buchführung bedeutsamen Verarbeitungsfunktionen

auch

- Umfang und Wirksamkeit maschineninterner Plausibilitätskontrollen (Eingabekontrollen, maschinelle Kontroll- und Abstimmverfahren im Verarbeitungsablauf) zur Sicherstellung der Verarbeitung vollständiger und richtiger Daten und
- die Softwaresicherheit (Zugriffsschutz, Datensicherungs- und Wiederanlaufverfahren), welche auch durch Programmentwicklung, -wartung und -freigabe beeinflusst wird.

Der Bericht zur Testatvergabe kann für spätere Prüfungen der Software durch die Interne Revision oder beispielsweise den Wirtschaftsprüfer bei der handelsrechtlichen Jahresabschlussprüfung in der Einsatzumgebung verwendet werden. Die Ergebnisse der Software-

[1] vgl. IDW (2002d): PS 321,2-9
[2] vgl. IDW (1998): PS 880

prüfung sind dabei auf die besonderen Gegebenheiten und Anforderungen des Internen Kontrollsystems im geprüften Unternehmen zu beziehen: Eine Softwareprüfung kann eine DV-Systemprüfung im Bereich der Ablauforganisation (zur Sicherstellung der optimalen Auslastung der Arbeitskräfte und Betriebsmittel sowie Durchlaufzeit für die Bearbeitungsobjekte) des Datenverarbeitungs-Bereichs aber nicht ersetzen. In der Regel wird die mit einem Testat versehene Softwareversion erst nach einem sog. Customizing beim Kunden eingesetzt. Customizing bezeichnet die Anpassung eines Serienprodukts wie etwa Software an die Bedürfnisse eines Kunden. Die Anpassung kann durch Programmänderungen (Individualprogrammierung) oder durch das Setzen von Parametern erfolgen. Dadurch werden Umfang und Aussehen einerseits oder das Verhalten und die Ergebnisse einer Standardsoftware verändert. Durch das Setzen von Parametern erfolgt die Änderung von Softwareparametern aufgrund spezifischer Kundenwünsche, damit die konfigurierbaren Eigenschaften der Software anhand der Ablauforganisation/Einsatzumgebung im zukünftigen Einsatzgebiet der Software optimiert bzw. an die Ablauforganisation/Einsatzumgebung angepasst werden. Es ist dann zu beurteilen, ob die für die mit einem Testat versehene Softwareversion getroffene Aussage auch auf die im Einsatz befindliche (an die Ablauforganisation/Einsatzumgebung angepasste) Software zutrifft.

Diese Ausführungen verdeutlichen, dass Interne und Externe Revision nicht isoliert voneinander betrachtet werden können. Insofern spielen auch die Stellungnahmen und Standards des IDW für die Interne Revision, insoweit diese der Externen Revision zuarbeitet und diese vorbereitet, eine Rolle. So werden im Folgenden – wo sie in den Zusammenhang passen - auch Ausführungen der Stellungnahmen und Standards des IDW, als Auffassung des Berufsstands der Wirtschaftsprüfer, angeführt und verwendet.

Im Bereich der Informationsverarbeitung (IV) und Informationstechnologie (IT) kennt man eine Datenverarbeitung(DV)s- und eine IT-Revision: Gegenstand der DV-Revision im engeren Sinne (als Bestandteil der Internen Revision) sind gemäß den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) „DV-gestützte Buchführungssysteme“ oder gemäß IDW Rechnungslegungsstandard des Fachausschusses für Informationstechnologie (RS FAIT 1) „IT-Systeme mit Rechnungslegungsbezug“. Im Zentrum stehen dabei die Kriterien Ordnungsmäßigkeit der DV-gestützten Buchführungsprozesse und anderer DV-Prozesse im Geltungsbereich der GoB (Grundsätze ordnungsgemäßer Buchführung) und GoBS sowie Sicherheit und Wirtschaftlichkeit in ihrer wechselseitigen Durchdringung. Bei dem Kriterium Sicherheit geht es um die Gewährleistung der Betriebsbereitschaft der EDV-Systeme und der zu ihrem Betrieb erforderlichen IT-Infrastruktur, Gewährleistung der Integri-

tät der Datenbestände, Gewährleistung der Wiederherstellbarkeit von Software und Datenbeständen im Bedarfsfall, Schutz personenbezogener Daten gemäß BDSG (Bundesdatenschutzgesetz).[1]

IT-Revision ist weitergehender als DV-Revision, insofern Ordnungsmäßigkeit allgemeiner als „Übereinstimmung der Aufgabenerfüllung mit internen und externen Vorschriften“ definiert wird und als Betrachtungskriterium die Funktionsfähigkeit (derartige Gestaltung der organisatorischen Abläufe, dass sie im Sinne der abgestimmten Ziele termingerecht zu richtigen und vollständigen Ergebnissen führen) hinzukommt.[2] Dies kommt der Sicht der im Folgenden angestrebten Konzeption entgegen: Untersucht wird u. a. die Bedeutung der IT-Security für die Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume.

Die IT-Revision im Speziellen hat ihre Begründung darin, dass der Geschäftsverkehr und Geschäftsprozesse mehr und mehr digital abgewickelt werden: dies beginnt bereits bei Anfragen, Angeboten bis hin zu rechtlich verbindlichen Verträgen mit den daraus resultierenden Ansprüchen und Verpflichtungen.[3]

Betriebliche Informationssysteme werden in Prozess-unterstützende und Prozess-neutrale Anwendungen unterteilt. Prozess-neutrale Anwendungen unterstützen alle Geschäftsprozesse unabhängig von der Art der jeweils auszuführenden Tätigkeit (z. B. Workflowsysteme). Sie bilden das Rückgrat des Unternehmens, indem sie den Informationsaustausch sicherstellen. Sie werden grundsätzlich unternehmens- oder konzernweit eingesetzt. Fehleinschätzungen von Rahmendaten, z. B. durch neue Technologien, können diverse Geschäftsprozesse beeinträchtigen. (z. B. durch einen nicht rechtzeitig entdeckten und beseitigten Virenangriff). Sie sind von strategischer Bedeutung und erfordern entsprechende Konzepte für Planung, Einführung und Betrieb.[4] Im Zusammenhang mit der vorliegenden Thematik geht es um solche Prozess-neutralen Anwendungen.

Mit zunehmender Abhängigkeit der Unternehmen von der Ordnungsmäßigkeit und Sicherheit ihrer IV und IT hat sich das Interesse an der Wirtschaftlichkeit (optimaler Ressourceneinsatz), Zweckmäßigkeit, Ordnungsmäßigkeit und Sicherheit auch im Bereich der Informationsverarbeitung und -technologie erhöht, wobei eine ex-ante (Zukunft bezogene) Revision im Mittelpunkt steht. Revisionsarten dieses Bereichs gliedern sich in:

[1] vgl. Wähner Gerd W. (2002), S.24-52
[2] vgl. IIR (2002), S.4
[3] vgl. Foth, Michael (2006c), S.136
[4] vgl. Gadatsch, Andreas (2004), S.95,96

- Untersuchungen institutioneller Einheiten (z. B. die Abteilungen Buchhaltung oder Programmierung), die insbesondere den Steuerungs- und Kontrollprozess innerhalb dieser Einheiten betreffen sowie
- Verfahrensprüfungen, bei denen Ordnungsmäßigkeit und Funktionalität der Verfahren im Mittelpunkt stehen, und bei denen sowohl ex-post als auch ex-ante Prüfungen sinnvoll sind.

Die Tätigkeit der Revisoren reicht hierbei von Teilprüfungen bis hin zu Beratung und Gutachten. Revisorisches Mitwirken bezweckt hier auch das Einbringen von Erfahrungen zum Sachgebiet und über Schwachstellen in Abläufen.

Eine adäquate Revisionstechnik in diesem Zusammenhang ist die Systemprüfung. Damit werden z. B. umfassende Datenmengen auf ihre ordnungsgemäße Verarbeitung hin beurteilt.

Das Systemkonzept erlaubt es, aus einem komplexen Gebilde ein Teilsystem herauszugreifen, ohne den Bezug zum übergeordneten Ganzen zu verlieren. Im Gegensatz zum Controlling (als zweitem Aspekt der Überwachung) ist die Revision von Personen wahrzunehmen.

Bei ex-ante Prüfungen ist sehr genau zu hinterfragen, ob die Unabhängigkeit des Prüfers durch diese Tätigkeit leiden könnte. Danach darf der Revisor z. B. Grundsätze für die Kontrollen von Systemen empfehlen. Wenn er allerdings die Konzeption, Installation und den Betrieb derartiger Systeme durchführt, gilt seine Objektivität als beeinträchtigt.[1]

IT-Risk-Assessment beurteilt zunächst IT-Bedrohungen, die auf zu kontrollierende Ergebnisse und Vorgänge einwirken und über Schwachstellen z. B. der IT-Infrastruktur IT-Risiken auslösen und ein Risikomanagement notwendig werden lassen.

IT-Risk-Assessment betrachtet Risiken, welche von der IT-Infrastruktur, den IT-Anwendungen und den IT-Geschäftsprozessen her begründet sind. Durch gesetzliche Rahmenbedingungen wie KonTraG ist ein extern induzierter Handlungsbedarf gegeben, Operational Risks und somit auch solche IT-Risiken hinreichend zu messen und zu managen.

Bei der Identifikation und angemessenen Behebung von Sicherheitsrisiken der IT-Infrastruktur geht es darum, Präventivmaßnahmen zum physischen Schutz von Installationen durchzuführen. Ziel ist eine Infrastruktur, die den Anforderungen auf Basis von vorhandenen Normen und Bewertungskriterien genügt und eine möglichst hohe System- und Datenverfügbarkeit sowie den Schutz der Informationen, Geräte und möglicherweise Lager- und Archivbestände sicherstellt.

[1] vgl. Förschle, Gerhart/Peemöller, Volker H. (2004), S.159

Sicherheitsanforderungen sollen sich an den Geschäftsprozessen des Unternehmens orientieren. Geschäftsprozesse bestehen aus einer Folge von zusammenhängenden, abgeschlossenen Tätigkeiten/Aktivitäten, die von den betrieblichen Aufgabenträgern unter kombinatorischer Nutzung betrieblicher Produktionsfaktoren (menschliche Arbeitsleistung, Betriebsmittel, Be- und Verarbeitungsobjekte, Zusatzfaktoren, Information) erbracht werden. Sie dienen der Leistungserstellung von Produkten oder Dienstleistungen (Services) für unternehmensexterne oder –interne Empfänger/Kunden nach explizit oder implizit vorgegebenen Zielsetzungen. Im Zusammenhang mit dem Gegenstand der vorliegenden Untersuchung geht es um die IT-Ressourcen in den Produktionsfaktoren, vor allem um den Produktionsfaktor Information. Dieser steht in verschiedenster Ausprägung vor allem bei der Planung von Geschäftsprozessen im Vordergrund. So sollen die Computer-gestützten Informationssysteme eines Unternehmens gewährleisten, dass die Geschäftsprozesse ordnungsgemäß ablaufen.[1]

Die abstrakten Sicherheitsanforderungen ergeben sich aus der Schutzbedürftigkeit der durch die IT-Systeme unterstützten Geschäftsprozesse. Die konkreten Sicherheitsanforderungen an die IT-Systeme und Daten, die Teil dieser Geschäftsprozesse sind, leiten sich aus der Wichtigkeit und Kritikalität dieser Geschäftsprozesse ab.[2]

Im Zentrum der Revision der IT-Sicherheit steht das IT-Sicherheitsmanagement.[3] Eine ständige und fortlaufende Sicherheitsrevision wird im Sinne einer ständigen Verbesserung des Sicherheitsmanagements verstanden. Bei der IT-Sicherheitsrevision wird die planungsgemäße Umsetzung und Wirksamkeit der Maßnahmen (Standards und Best Practices) überprüft.[4] Dabei wird nicht nur die Einhaltung bestehender Maßnahmen überprüft, sondern auch deren Relevanz.[5] In der vorliegenden Untersuchung wird dieser Gegenstand im Rahmen der Überprüfung von Entwicklung und Umsetzung der IT-Security-Strategie betrachtet.

Controlling ist ein Begriff aus der englischsprachigen Managementliteratur, der im deutschsprachigen Raum ohne Übersetzung verwendet wird. Die im deutschsprachigen Raum im Bereich des Controllings behandelten Probleme sind in Bezug auf die internationale wissenschaftliche Diskussion am ehesten dem Management Accounting bzw. Managerial

[1] vgl. Rosenkranz, Friedrich (2006), S.3,4
[2] vgl. Rieger Holger (2005a), S.26
[3] vgl. Kamlah, Bernd (2005)
[4] Rudholzer, Gerhard (2005), S.43
[5] vgl. Humpert, Frederik (2005), S.8

Accounting zuzuordnen.[1] Zentrale Fragestellungen des Management Accounting sind auf die Probleme und die Struktur innerbetrieblicher Koordinations- und Steuerungssysteme ausgerichtet.[2]

Nach der jeweiligen Definition des Aufgabenbereichs werden Controlling-Konzeptionen entweder als „Universalzielorientierte Metaführungskonzeption“ oder als „Ergebniszielorientierte Führungsunterstützungskonzeption“ typologisiert. Die Unternehmensziele bilden die Deduktionsbasis für die Controllingziele, die sich also an den Unternehmenszielen ausrichten sollten. Aus diesen Oberzielen können die zentralen Controllingziele aber formal betrachtet als Unterstützung der Planung und Koordination der einzelnen Unternehmens-Teilbereiche sowie Kontrolle der wirtschaftlichen Ergebnisse betrachtet werden.[3] Controlling gilt als gut geeignet, die Handlungs- und Entscheidungsprozesse im Unternehmen zu koordinieren und zu integrieren.[4]

Controlling bedeutet ein umfassendes Steuerungs- und Koordinationskonzept. Es ist insgesamt der Prozess von Zielsetzung, Planung, Steuerung und Kontrolle.[5] Aufgabe ist die Unterstützung der Geschäftsleitung und der führungsverantwortlichen Stellen bei der Planung und Umsetzung der unternehmerischen Aktivitäten (Unterstützung der strategischen Planung, Umsetzung der strategischen in die operative Planung sowie Aufbau und Durchführung einer strategischen Kontrolle)[6], wozu insbesondere [7]

- Ausrichtung des Informationssystems auf Planung, Steuerung und Kontrolle sowie
- Koordination von Planung, Kontrolle und Informationssystem mit der Organisation

gehören.[8]

Im Mittelpunkt des Controllings stehen die Konzeption und der Betrieb von qualitativen und quantitativen Steuerungsinstrumenten. Das Controlling kann dementsprechend als Management-unterstützende Funktion gesehen werden, die sicherstellen soll, dass die vom Management vorgegebenen Zielsetzungen und Strategien u. a. [9]

- durch ein adäquates Vorgehen realisiert werden können und
- so effizient wie möglich erfüllt werden.

[1] vgl. Küpper, Hans-Ulrich (2005), S.6
[2] Küpper, Hans-Ulrich (2005), S.49
[3] vgl. Diederichs, Marc (2004), S.19-21
[4] Peemöller, Volker H. (2005), S.118
[5] Peemöller, Volker H. (2005), S.37
[6] vgl. Peemöller, Volker H. (2005), S.118-212
[7] vgl. Horváth, Péter (2006), S.147-639
[8] vgl. Küpper, Hans-Ulrich (2005), S.38,39
[9] vgl. Diederichs, Marc (2004), S.22

Die ständige und fortlaufende Überprüfung der Relevanz und der Einhaltung bestehender Standards und Best Practices durch die IT-Security-Revision kann auf die Überprüfung der Entwicklung und Umsetzung der IT-Security-Strategie verallgemeinert werden. In diesem Sinne überprüft die IT-Security-Revision Effektivität und Effizienz des IT-Security-Controllings.

Metaaufgabe des Controllings ist sowohl die Problemerfassung und -bewertung als auch die damit verbundene Informationsbeschaffung, um die mit der Problemerkennung einhergehende Unsicherheit zu reduzieren.[1] Kontrollen im Sinne des Controllings betreffen eher Prognoseunsicherheiten - betrachtet werden vor allem Tendenzen, die zukünftiges Handeln beeinflussen. Die Prüfungen der Internen Revision beziehen sich auf die vom Controlling er- und verarbeiteten Informationen. Gemeinsamkeiten zwischen Interner Revision und Controlling ergeben sich u. a. insbesondere bei den Indikatoren für die zukünftige Entwicklung: Beide versuchen, die Prognoseunsicherheit aufgrund zunehmender Komplexität und Dynamik der Unternehmensumwelt durch adäquate Instrumente zu begrenzen.[2]

Aus der Koordinationsfunktion des Controllings lässt sich des Weiteren u. a. die Anpassungsfunktion als Koordination der Führungsaufgabe mit der Umwelt ableiten.[3] Sie bezieht sich auf die Gestaltung von Systemen insbesondere der Informationsbereitstellung (z. B. Früherkennungssysteme) und Kontrolle.[4] Teile der Aufgaben des Controllings stimmen mit denen des Risikomanagements überein.[5]

Die Controlling-Konzeption kann als dreidimensionaler Bezugsrahmen dargestellt werden: Die erste Dimension basiert auf der Einteilung der Unternehmensfunktionen und -prozesse in Primär- und Sekundärfunktionen, die zweite Dimension auf der Informationskategorisierung (insbesondere qualitativ vs. quantitativ, intern vs. extern) und die dritte auf der Unterteilung in eine operative und eine strategische Ebene.[6]

Das operative Controlling befasst sich mit dem laufenden Nachweis der operativen Geschäftstätigkeit. Die operativen Ist-Größen werden dabei periodisch mit den operationalisierten Zielgrößen aus der strategischen Planung auf Zieleinhaltung und -abweichung überprüft.

Das strategische Controlling befasst sich mit der strategischen Planung und der Festlegung der unternehmensweiten Zielvorgaben, z. B. innerhalb einer Balanced Scorecard. Es ist

[1] vgl. Diederichs, Marc (2004), S.21
[2] vgl. Peemöller, Volker H. (2005), S.64-66
[3] vgl. Horváth, Péter (2006), S.1-68
[4] vgl. Küpper, Hans-Ulrich (2005), S.32,33
[5] vgl. Diederichs, Marc (2004), S. 18
[6] vgl. Reichmann, Thomas (2006), S.6-8

primär extern, d. h. auf das Umfeld des Unternehmens orientiert, während das operative Controlling intern, d. h. auf das Unternehmen selber ausgerichtet ist, und z. B. die Wirtschaftlichkeit der betrieblichen Prozesse sicherzustellen hat. Das strategische Controlling soll die Unzulänglichkeiten der strategischen Planung (d. h. die Auswirkungen mangelnder Prognostizierbarkeit zukünftiger Umfeldentwicklungen) überwinden.[1] Es unterstützt den Prozess des strategischen Managements und setzt sich aus den drei Teilaspekten Prämissenkontrolle, strategische Durchführungskontrolle und strategische Überwachung zusammen: Wesentliche Aufgabe ist die Unterstützung des Managements bei der Strategieentwicklung und bei der Strategieumsetzung. Ziel ist die langfristige Existenzsicherung der Unternehmung.

Dabei sollen operative Controlling-Werkzeuge und die strategische Planung mit strategischen Controlling-Werkzeugen ergänzt und miteinander vernetzt werden.[2]

Im Kontext der vorliegenden Thematik geht es um die Umsetzung der angesprochenen Konzepte am Beispiel der IT-Security. Das zu entwickelnde Modell soll die erwähnten Aufgaben der IT-Security-Revision und des Controllings abdecken.

Theoretisch wissenschaftlicher Steuerungsansatz hinsichtlich eines zu konzeptionierenden Frameworks[3] ist dabei die Perspektive der Organisationsentwicklung, die dazu benutzt werden kann, „strategische Veränderungsprozesse in Organisationen wissenschaftlich fundiert und systematisch zielgerichtet zu gestalten“, und auf Ansätze zurückgeht, die „Veränderungen der Umwelt und entsprechende Anpassungsleistungen der internen Systeme“ berücksichtigen wollen.[4]

Strategische IT-Controlling-Werkzeuge sollen das IT-Management bei der Formulierung, Umsetzung und laufenden Überwachung der IT-Strategie des Unternehmens unterstützen.[5] Strategisches Controlling der IT-Security wird im Folgenden dahin gehend entwickelt, dass es das IT-Security-Management in ein strategisches Rahmenkonzept einbetten, die kontinuierliche Anpassung und Weiterentwicklung des IT-Sicherheits-/IT-Security-Managements koordinieren und das IT-Security-Management so steuern und (im Sinne strategischer IT-Controlling-Werkzeuge) unterstützen soll.

[1] Peemöller, Volker H. (2005), S.118
[2] vgl. Gadatsch, Andreas (2006), S.15
[3] Hanke, Thomas (2006), S.213-226
[4] vgl. Hanke, Thomas (2006), S.93-117
[5] vgl. Gadatsch, Andreas (2006) S.45

2 Gang der Untersuchung und weitere Vorgehensweise

Im Hauptteil wird ein Modell zur Revision bzw. zum Controlling (der Geschäftsprozess-orientierten Ausgestaltung) des IT-Security-Managements entwickelt. Geschäftsprozesse ziehen sich über viele Bereiche und Systeme der IT hinweg und dürfen nicht Technik orientiert betrachtet werden. Die IT wird nicht alleine aus der Perspektive der Technologie betrachtet, sondern z. B. auch aus der Perspektive der IT-Dienstleistungen.

Bei der Revision und dem Controlling der IT-Security im Sinne einer Projekt--begleitenden Aufgabe des Managements (z. B. im IT-Service-Management) geht es um die Lösung eines Problems. Dieses besteht darin, die Effektivität und Effizienz des IT-Security-Managements so zu gestalten, dass diese notwendige und gleichzeitig hinreichende Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security ist. Die notwendige Bedingung wird hauptsächlich von der Revision der IT-Security, die hinreichende Bedingung im Wesentlichen vom Controlling der IT-Security zu erfüllen sein.

Ein Problem ergibt sich für ein Wirtschaftssubjekt aus einer als negativ empfundenen, nicht tolerierbaren Diskrepanz zwischen dem aktuell bestehenden oder für die Zukunft erwarteten Ist-Zustand und dem Soll-Zustand eines Betrachtungsobjekts aus dem Verfügungsbereich des Wirtschaftssubjekts.[1] Betrachtungsobjekt ist das IT-Security-Management. Eine Problemlösung besteht in einem veränderten Ist-Zustand des Betrachtungsobjekts und/oder einer veränderten Vorstellung des Wirtschaftssubjekts über den Soll-Zustand, wobei die Diskrepanz zwischen dem aktuell bestehenden oder für die Zukunft erwarteten Ist-Zustand und dem Soll-Zustand auf ein tolerierbares Maß verringert wird.[2] Für das IT-Security-Management ist also ein kontinuierlicher Verbesserungsprozess zu initiieren, der auf die Anpassung von Ist ans Soll abzielt. Dazu sollen Systeme zur Unterstützung der Strategieformulierung und -umsetzung in ein entsprechendes Lösungsmodell integriert werden. Unterstützung der Strategieformulierung betrifft dann den Aspekt der Veränderung der Vorstellung des Wirtschaftssubjekts über den Soll-Zustand, Unterstützung der Strategieumsetzung betrifft den Aspekt der Veränderung des Ist-Zustands.

Zunächst wird dargestellt, welche Gegenstände/Objekte der Revision und des Controllings der IT-Security betrachtet werden und Ansatzpunkte zur Bewertung der IT-Security liefern. Zu orientieren hat sich die Revision und Risiko-orientierte Ausgestaltung der IT-Security

[1] vgl. Gössinger, Ralf (2005), S.87
[2] vgl. Gössinger, Ralf (2005), S.88

darüber hinaus an gesetzlichen Anforderungsgrundlagen. Auch wenn die Revision der IT-Security im Sinne einer Prüfung keine Pflichtveranstaltung ist, so ergibt sich doch durch entsprechende Haftungsprobleme ein obligatorischer Charakter. Aus den gesetzlichen Anforderungsgrundlagen wird aber im Wesentlichen nur deutlich, dass die auf die Risiko-orientierte Ausgestaltung abzielende Revision der IT-Security auf entsprechende Schnittstellen zum Risikomanagement basiert. Im weiteren Verlauf wird daher ein operativer Rahmen zur Analyse und Risiko-orientierten Ausgestaltung der IT-Security konzeptioniert. Klassische Konzepte haben dabei ihre Schwächen vor allem in der Einbeziehung nicht-antizipierbarer Risiken. Alternativen zur Risikoprognose werden entwickelt, basierend auf Risikokontext und Risikoakzeptanz. Darauf aufbauend werden Methoden für ein Gefährdungspotenzial-orientiertes Management der IT-Security zum Erreichen und Aufrechterhalten eines angemessenen, wirtschaftlich vertretbaren IT-Security-Niveaus erörtert. Zudem wird ein strategisch-operatives IT-Security-Management entwickelt. Dieses soll strategische Handlungsspielräume (bezüglich der mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens) bei der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse unterstützen.

Das Aufzeigen von Handlungsspielräumen gelingt Softwarelösungen, die speziell für das Risikomanagement entwickelt wurden, mittels einer integrierten Chancenbetrachtung.[1] In Bezug auf die IT-Sicherheit sind Risiken normalerweise reine Verlustgefahren und damit ist eine Chancenbetrachtung nicht möglich. Allerdings bieten Technologien wie das Internet Chancen, die mit entsprechenden Risiken verbunden sind.[2] Ob bewusst eingegangene Risiken der IT-Sicherheit Chancenpotenziale eröffnen, soll jedoch keine Fragestellung im Zusammenhang mit der vorliegenden Thematik sein. Es sollen die Möglichkeiten bewertet, kontrolliert und gesteuert werden, dass sich Erwartungen des Systems Unternehmung aufgrund mangelnder IT-Security nicht erfüllen. Es geht in diesem Zusammenhang darum, welche Anforderungskriterien an die IT-Security, für die Handlungsbefähigung bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens auf welcher Ebene der Unternehmensplanung wichtig sind.

Danach geht es um Anwendungen der entwickelten Konzepte. Das ist zunächst die ex-ante Bewertung und Optimierung der IT-Security. Unterschieden werden dabei ein strukturierter und ein strategischer Ansatz. Es wird hier ein strukturiert-strategischer Ansatz entwickelt.

[1] vgl. Giefer, Katrin (2006), S.21
[2] vgl. Parthier, Ulrich/Lamm, Andreas (2006)

Dabei soll das entwickelte strategische Controlling/strategische IT-Security-Management Formulierung und Umsetzung der (mithilfe geeigneter IT-Projekte umzusetzenden) strategisch-operativen Zielsetzung des Unternehmens koordinieren und steuern, um neue Geschäftsmöglichkeiten und entsprechende Geschäftsmodelle mit zugehörigen Erfolgspotenzialen zu unterstützen bzw. abzusichern. Dann wird das (darauf basierende) Nutzenpotenzial der IT-Security diskutiert und ein Vorgehensmodell zur Sicherheitsstandardunabhängigen, Geschäftsprozess-orientierten Ausgestaltung der Sicherheit von Informationssystemen skizziert.

B Entwicklung eines Modells zur Revision und zum Controlling der IT-Security

Das Modell zur Revision und zum Controlling der IT-Security soll auf den wesentlichen Normelementen einer Qualitätspolitik[1], welche mit den Normelementen der Sicherheits-/Securitypolitik gleichgesetzt werden, aufsetzen:

- Security umfasst sowohl technisch-funktionale als auch normative und wirtschaftliche Anforderungen
- Security als strategisches Unternehmensziel bedeutet, dass der Security-Gedanke bereits in den Zielbildungsprozess und die Zielfindung mit einfließt
- Security als unternehmensweite Aufgabe bedeutet die Verinnerlichung und Umsetzung des Security-Gedankens im gesamten Unternehmen
- Prävention als wichtiger Leitgedanke verschiebt den Fokus weg von der reinen Fehlerbehebungsmentalität hin zu vorbeugenden Maßnahmen und zur Eigenkontrolle

Im Rahmen des Controllings stehen die Struktur und die Eigenschaften von Risiken im Vordergrund.[2] In diesem Sinne geht es um qualitative (nicht quantifizierbare) Aspekte im Rahmen des Managements von Risiken der IT-Security/des IT-Security-Managements. Als quantitative Größen wären vor allem. Eintrittswahrscheinlichkeit und finanzielle Konsequenzen von Interesse. Von der Quantifizierbarkeit der Risiken wird auch der Einsatz verschiedener Erfassungs-, Analyse- und Steuerungsmethoden, und insbesondere verschiedener Instrumente zur Bewertung abhängig gemacht.[3] Es wird zu zeigen sein, wie aus der Ungewissheit von zukünftigen Entwicklungen im Umfeld des Unternehmens entspringende qualitative Risiken analysiert und gesteuert werden können. Durch Modellierung eines entsprechenden strategisch-operativen IT-Security-Managements wird ein Ansatz für eine strukturiert-strategische ex-ante Bewertung der IT-Security hergeleitet. Dies wird dadurch ermöglicht werden, dass auf sinnvollen Bewertungsebenen die Zielerreichung als abhängig von den Anforderungskriterien an die IT-Sicherheit analysiert wird. Die Bewertung ist nicht mehr von der Quantifizierbarkeit der Risiken abhängig, da letztlich nicht mehr direkt die Risiken, sondern die Anforderungskriterien an die IT-Sicherheit analysiert werden.

[1] vgl. Mieschke, Lutz (2003), S.81
[2] vgl. Burger, Anton/Buchhart, Anton (2002), S.3
[3] vgl. Burger, Anton/Buchhart, Anton (2002), S.4

1 Bestimmungsobjekte/Betrachtungsobjekte der Revision und des Controllings der IT-Security

Die Revision, das Controlling und die Bewertung der als Informationssicherheit verstandenen IT-Security erfordert zunächst die Identifikation konkreter Bestimmungs-/Ausgestaltungsobjekte, welche in Verbindung zu den Geschäftsprozessen des Unternehmens stehen. Als Betrachtungsobjekte der Revision und des Controllings der IT-Security lassen sich neben den Anforderungen und Maßnahmen an die IT-Sicherheit (abgeleitet aus externen und internen Ordnungsmäßigkeitsvorgaben, den Korrektheitsbedürfnissen der im Unternehmen durchlaufenden und von den Geschäftsprozessen benötigten Informationen und den potenziellen IT-Bedrohungen), die IT-Sicherheitsstrategie des Unternehmens sowie der IT-Security-Prozess untersuchen.

Die Ziele einer Sicherheitsstrategie orientieren sich in der Regel an Fragestellungen zur Abwägung wie [1]

- maximale Anzahl zugänglicher Dienste und Services vs. maximale Sicherheit,
- Benutzerfreundlichkeit vs. Sicherheit,
- Kosten der Sicherheit vs. Risiko eines Schadens.

Die Sicherheitsstrategie versucht, den IT-Risiken zu begegnen. Häufig bedient man sich dabei des klassischen Outsourcings, d. h. Risiken zumeist des Systembetriebs werden auf externe Dienstleister übergewälzt.[2]

Der Regelkreis von der Sicherheitsstrategie über die Planung zur Umsetzung und Überwachung wird als IT-Sicherheitsprozess bezeichnet.[3] Dieser Regelkreis ist im Plan-Do-Check-Act (PDCA)-Zyklus der ISO 27001/BS7799-2 wiederzufinden.

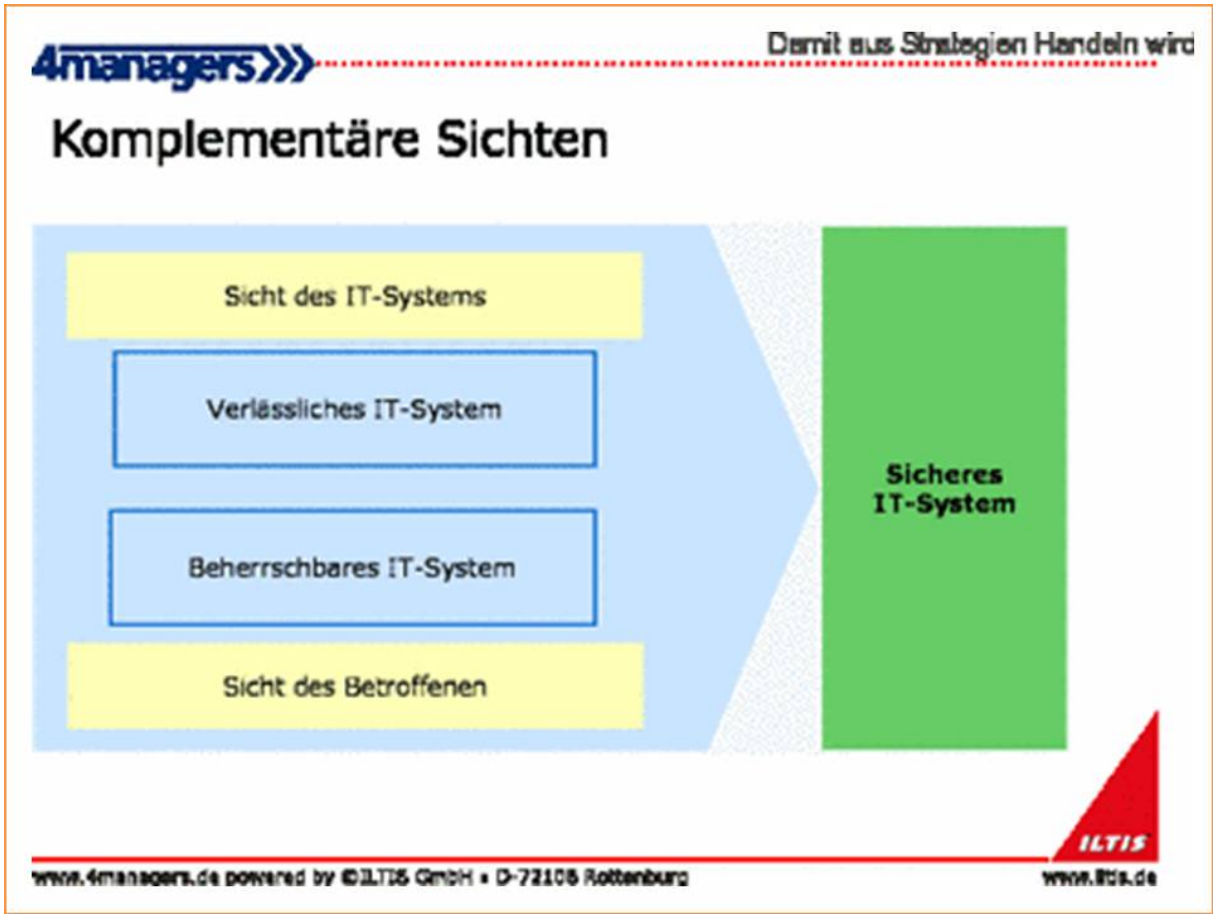
Ein auf die Bedürfnisse des individuellen Unternehmens angepasster und gesteuerter IT-Security-Prozess ist Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von IT-Security-Maßnahmen und somit der Revision der IT-Security. Maßnahmen sind in diesem Zusammenhang Aktivitäten, die sich auf den Inhalt und die Umsetzung der IT-Security-Strategie beziehen.

[1] vgl. Poels, Torsten. (2005)
[2] vgl. Kamlah, Bernd (2004b)
[3] vgl. Kamlah, Bernd (2005), S.24

Der IT-Security-Prozess ist das Kernstück eines IT-Security-Managements, welches eine angemessene und steuerbare Sicherheit gewährleisten soll. Als IT-Security-Management wird die Planungs- und Lenkungsaufgabe bezüglich dieses IT-Security-Prozesses bezeichnet.

Im weiteren Verlauf wird ein strategisch-operatives (Risiko-)Controlling entwickelt, das das (operative) IT-Security-Management zu einem strategisch-operativen IT-Security-Management erweitert. Dieses strategisch-operative (Risiko-)Controlling liefert Vorgaben für das operative IT-Security-Management. Zunächst werden die üblichen Gegenstände/Objekte des IT-Security-Managements beschrieben, die einen Teil der Gegenstände/Objekte des strategisch-operativen IT-Security-Managements darstellen. Die zusätzlichen Gegenstände/Objekte des strategisch-operativen IT-Security-Managements sind die aus dem strategischen und operativen Performance Management im weiteren Verlauf auf das strategisch-operative (Risiko-)Controlling der IT-Security übertragenen Komponenten.

1.1 Anforderungen und Maßnahmen der IT-Security



(Quelle: ILTIS GmbH (2005))

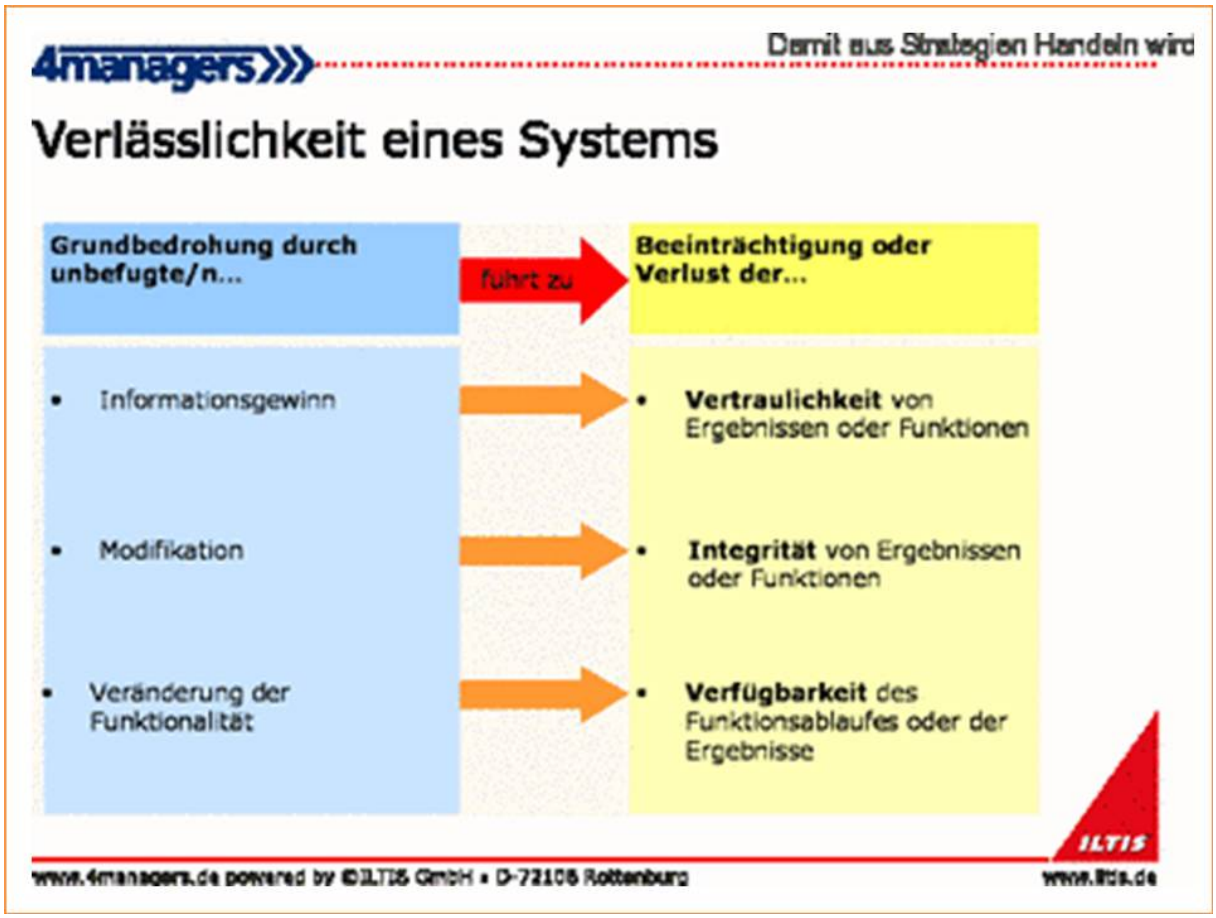
Abb. 1 Die zwei grundlegenden Sichten auf die IT-Sicherheit eines Systems

Die IT-Sicherheit eines Systems kann aus zwei komplementären, sich einander ergänzenden Sichten betrachtet werden:[1]

- Sicherheit des Systems (bezeichnet als Verlässlichkeit)
- Sicherheit vor dem System (bezeichnet als Beherrschbarkeit)

Verlässlichkeit kann definiert werden als Sicherheit des Systems in technischer Sicht, „bei der weder die Systeme, die mit ihnen verarbeiteten Daten noch die Form der Verarbeitung in ihrem Bestand, ihrer Nutzung oder in der Verfügbarkeit unzulässig beeinträchtigt werden.“[2]

Notwendige Eigenschaften, die ein System aufweisen muss, um als verlässlich bezeichnet zu werden, ergeben sich aus einer Analyse möglicher Beeinträchtigungen der Verlässlichkeit.



(Quelle: ILTIS GmbH (2005))

Abb. 2 *Notwendige Eigenschaften der Verlässlichkeit eines IT-Systems*

Vertraulichkeit, Integrität und Verfügbarkeit des Systems beziehen sich dabei auf alle seine Komponenten, d. h. Geräte, Daten, Programme und Personen. Erwähnt sei z. B. das Problem, dass ein fehlerhaftes Programm die Verfügbarkeit bestimmter Geräte und Services beein-

[1] vgl. ILTIS GmbH (2005)
[2] ILTIS GmbH (2005)

trächtigen kann. Wenn der Fehler unerkannt bleibt, kann dies zudem zu einer ungewollt veränderten Funktionalität und somit zu ungewollten Ergebnissen führen. Mithin wird neben der Verfügbarkeit bestimmter Services auch die Integrität der verarbeiteten bzw. erzeugten Daten beeinträchtigt.

Ein verlässliches IT-System muss alle im Anforderungskatalog definierten Aktionen ausführen, alle nicht definierten Aktionen zurückweisen (z. B. im Hinblick auf datenschutzrechtliche Anforderungen) und das alles in den geforderten zeitlichen Rahmenbedingungen. Es kann diesbezüglich auch als ordnungsgemäß bezeichnet werden. Höchste Aufmerksamkeit auf die Anwendungen/Programme zu lenken ist ein wesentlicher Bestandteil bei der Betrachtung der IT-Sicherheit und eine oft vernachlässigte Aufgabe, sowohl bei den Anwendern wie bei den Herstellern.

Aus Vertraulichkeit, Integrität und Verfügbarkeit leiten sich weitere Aspekte ab wie Privacy (Vertraulichkeit und Integrität einer auf eine natürliche Person zurückzuführenden Information) und Anonymität (Vertraulichkeit der Identität einer Person).

Im Bereich Datenschutz können des Weiteren Kriterien und Grundsätze zur Ausgestaltung der Datenschutz-Funktionalitäten und Vertrauenswürdigkeit von IT-Produkten/Systemen aufgestellt werden; Maßnahmen und Datenschutz-Funktionen müssen folgenden Kriterien und Grundsätze genügen:

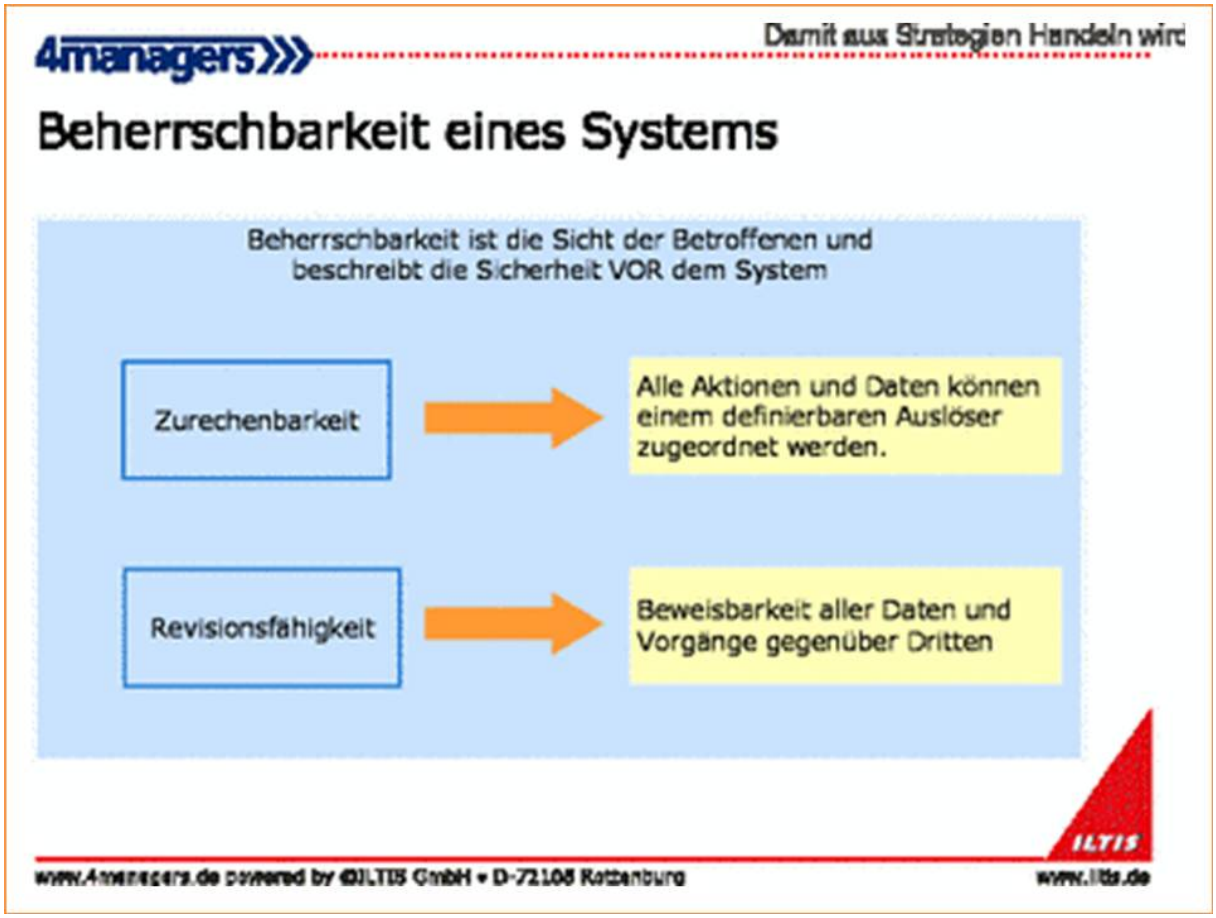
- Datenvermeidung und Datensparsamkeit (Reduktion personenbezogener Daten in einem IT-System),
- Systemdatenschutz (bereits technisch im System implementierte und organisatorisch verankerte Datenschutzmaßnahmen),
- Selbstdatenschutz (Maximum an Steuerungsmöglichkeiten durch den Nutzer) sowie
- Transparenz und andere vertrauensbildende Maßnahmen.

Diese Kriterien und Grundsätze manifestieren sich weitgehend auch in den technischen und organisatorischen Maßnahmen nach BDSG (Bundesdatenschutzgesetz) bzw. technischen und organisatorischen Maßnahmen nach TMG (Telemediengesetz).

Der Zustand IT-Sicherheit muss für jedes Unternehmen und jedes verwendete IT-System spezifisch festgelegt werden. Ob ein System in einer bestimmten Hinsicht als sicher gelten kann, hängt von den zu erfüllenden Anforderungen (z. B. bezüglich der Verfügbarkeit) ab.[1]

[1] vgl. Rieger Holger (2005a), S.26

Die Verlässlichkeit eines Systems gewährleistet grundsätzlich aber noch nicht, dass das System/die Anwendung im Sinne der Betroffenen/Anwender funktioniert, ihre Belange berücksichtigt und für sie nachvollziehbar ist. Dem Anwender/Betroffenen fehlt zumeist die Möglichkeit zur unmittelbaren Wahrnehmung dessen, was in einem IT-System passiert. Daher müssen weitere Eigenschaften definiert werden, um ein IT-System aus Sicht des Betroffenen sicher/beherrschbar zu machen:



(Quelle: ILTIS GmbH (2005))

Abb. 3 Eigenschaften für die Beherrschbarkeit eines IT-Systems

Um die Nachprüfbarkeit aller Daten, Prozesse oder Ereignisse in einem IT-System sicherzustellen, müssen alle Vorgänge und Ergebnisse (d. h. alle Aktionen und Daten) definierbaren Auslösern zugeordnet werden können (Authentizität/Zurechenbarkeit). Es genügt aber nicht, nur die Zurechenbarkeit festzustellen. Diese Zuordnung muss auch gegenüber unbeteiligten Dritten beweisbar sein (Revisionssicherheit bzw. Rechtsverbindlichkeit). Die Abläufe und Daten müssen aktuell und vollständig so dokumentiert sein, dass sie Dritten gegenüber beweiskräftig sind.

Zurechenbarkeit und Revisionsfähigkeit sind nicht notwendigerweise in einem System vorhanden, sondern müssen explizit implementiert werden. Sie erfordern, den Blick auf die einzelnen Programmfunktionen eines Systems zu richten: Kann z. B. jedes Abrechnungssystem beweisen, wie Abrechnungsdaten zustande kommen? Prozesse gegen Telekommunikationsunternehmen zeigen hier oftmals die Grenzen der Betroffenen auf: So argumentieren die Unternehmen, es läge eine umgekehrte Beweispflicht vor: Nicht sie müssten die Korrektheit ihrer Systeme beweisen, sondern der Betroffene die Unkorrektheit. Die Betroffenen sind mangels Kenntnis der IT-Systeme und mangelnder Möglichkeit zur unmittelbaren Wahrnehmung dazu meist nicht in der Lage.

Die Eigenschaften eines Systems Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit, Revisionsfähigkeit sind als grundlegend zu betrachten, wenn vernünftige Sicherheitskonzepte für IT-Systeme behandelt werden. Hilfreich ist jedoch auch die Erweiterung oder Verfeinerung dieser Eigenschaften, sie gibt Hinweise auf mögliche Lücken im Sicherheitskonzept.

So können z. B. Eigenschaften wie Wartbarkeit, Flexibilität, Stabilität, Robustheit aufzeigen, wie verlässlich ein System sein kann: Fehlende Stabilität führt schnell zu fehlender Verfügbarkeit und ggf. zu fehlerhaften Daten. Fehlende Wartbarkeit und Flexibilität können dazu führen, dass veränderte Anforderungen nicht oder nicht nachvollziehbar umgesetzt werden, hier wären die Eigenschaften Zurechenbarkeit oder gar Revisionsfähigkeit gefährdet.[1]

IT-Sicherheit ist ein Zustand, in dem der Schutz vor (bekannten) Gefährdungen gegeben ist.[2] Aufgrund der rasanten technologischen Entwicklung mit gleichzeitig raffinierteren Methoden der Angreifer entstehen immer neue Bedrohungspotenziale. Da also nicht alle Gefährdungen bekannt sind, ist jedes IT-System (ob z. B. Desktop-PC, Laptop oder Handy) potenziell unsicher und z. B. von Hackern angreifbar. Das Eindringen in Unternehmensnetze (als Voraussetzung für einen Angriff auf ein an das Netz angeschlossenes IT-System) ist sogar mobil (über öffentliche Hot-Spots, die ein kabelloses Einloggen ins Internet erlauben) möglich, wenn das Unternehmensnetz ans Internet angeschlossen ist.

IT-Sicherheit ist ein Zustand, dessen Stabilität/Dauerhaftigkeit angestrebt wird. Stabilität/Dauerhaftigkeit bedeutet, dass er im Idealfall durch kein Ereignis (als Realisierung eines Risikos), d. h. nur durch ein Ereignis, welches nie eintreten soll, verlassen werden kann. Da ein nie eintretendes Ereignis nicht beobachtet werden kann, kann auch nicht objektiv beurteilt

[1] vgl. ILTIS GmbH (2004)
[2] vgl. Riieger Holger (2005), S.23

werden, ob dieses Ziel erreicht ist. Notwendige Bedingung zur Erreichung der Stabilität/Dauerhaftigkeit ist aber, dass zunächst einmal Sicherheitsanforderungen aufgestellt und diese mit entsprechenden Sicherheitsmaßnahmen abgedeckt werden. Sicherheitsmaßnahmen stellen die konkrete Implementierung der spezifischen Sicherheitskonzepte in Form spezieller Technologien, Verfahren, Mechanismen, Prozeduren, organisatorischer oder personeller Maßnahmen dar.

Die notwendige Bedingung zur Erreichung der Stabilität/Dauerhaftigkeit erfordert ein geeignetes operatives Sicherheitsmanagement auf Basis der Analyse der potenziellen IT-Bedrohungen. Des Weiteren sind (auf die IT-Security bezogene) externe und interne Ordnungsmäßigkeitsvorgaben sowie Korrektheitsbedürfnisse bezüglich der im Unternehmen durchlaufenden Daten/Informationen zu erfüllen. Aus den Anforderungen an die IT-Security ergeben sich so als Hilfsmittel die Maßnahmen zur Erfüllung dieser Anforderungen.

Als strategischer Aspekt kommt im Zusammenhang mit der hier behandelten Thematik die organisatorische Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume hinzu. Für diesen Aspekt wird ein das operative IT-Security-Management zu einem strategisch-operativen IT-Security-Management erweitert. Eine Bewertung der IT-Security kann dann im Sinne einer Analyse der Bedeutung von Risiken der IT-Security für die Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume angegangen werden.

1.1.1 … abgeleitet aus den potenziellen IT-Bedrohungen

Informationssysteme haben im Unternehmen eine übergreifende Querschnittsfunktion. Dabei steigen im Bereich der Informations- und Kommunikationstechnik die Sicherheitsrisiken durch die stetig und rasant wachsende Komplexität überproportional an. Die Bedrohungen der IT- und IV-Sicherheit richten sich auf geistiges Eigentum, Know-how, Wissen sowie physisches Eigentum und das Leistungsvermögen von Einrichtungen.[1]

Die Ziele, mit denen Sicherheit erreicht werden soll (Schutzziele), sind Vertraulichkeit, Integrität, Verfügbarkeit, Verbindlichkeit, Authentizität und die Möglichkeit zur Anonym-/Pseudonymisierung[2]. Diese Ziele sind oder weniger die Kriterien für einen verlässlichen, störungsfreien Betrieb bzw. Betriebssicherheit entsprechender IT-Systeme. Auf das Ziel der Erreichung von Sicherheit ist das Sicherheitsmanagement ausgerichtet. Bedrohungen der

[1] vgl. Pietsch, Thomas (2004), S.261
[2] vgl. Eckert, Claudia (2003), S.6-12

Ziele der IT-Sicherheit lassen sich in unabsichtliche Bedrohungen wie Höhere Gewalt, menschliches Versagen, technisches Versagen und absichtliche Bedrohungen wie Spionage, Sabotage usw. einteilen.

Zu den wichtigsten Ausprägungen aktueller Bedrohungsszenarien zählen gezielte Angriffe auf Webanwendungen und Webbrowser. Diese bilden nämlich die Schnittstelle zwischen Internet und vertraulicher Unternehmensinformation, die die Kommunikation zwischen Kunde und Backend-Systemen vermitteln.

Immer mehr Unternehmen verlagern ihre geschäftskritischen Anwendungen und Daten auf Web-Oberflächen. Browser basierte Anwendungen sind bedienerfreundlicher, Browser und deren Skript-Sprachen werden immer leistungsfähiger und Internet-Services zum Standard. Sog. Web-Applikationen sind daher leichter in Betrieb zu nehmen, zu unterstützen und zu warten. Die Kehrseite ist, dass herkömmliche, auf die unteren Schichten des ISO/OSI-Referenzmodells beschränkte Schutzmechanismen hier versagen.[1]

Die Sicherheit in Datennetzen darf aber nicht auf die untersten Schichten des ISO/OSI-Referenzmodells beschränkt bleiben, da Sicherheit immer an Prozeduren und klar vorgegebene Abläufe auf der Applikations-Schicht gebunden ist. [2] Traditionelle IT-Sicherheitssysteme wie Firewalls und Intrusion Detection/Prevention Systeme entstanden als Reaktion auf Angriffe auf den unteren Ebenen des ISO/OSI-Sieben-Schichten-Modells. Angriffe auf diesen Ebenen wurden historisch gesehen zuerst „ausprobiert“ und hatten auch große Wirkung. Mit zunehmender Absicherung bis zur Transportschicht, wachsendem Angreifer-Interesse an vertraulichen Daten sowie der mittlerweile fast unbegrenzten Anzahl von Sicherheitslücken (durch die Vielfalt der angebotenen Web-Script-Sprachen, Application Frameworks und Webtechnologien) müssen IT-Sicherheitssysteme auch die Applikationsebene selber einbeziehen. Die typischen zusätzlichen Angriffspunkte von Webapplikationen resultieren dabei im Kern aus der Netzwerk basierten Natur der Webapplikationen.[3]

Das Internet eröffnet gegenüber herkömmlichen Straftaten neue Möglichkeiten zur Ausführung von Angriffen: Technisch versierte Täter können aufgrund der Anonymität im Internet nahezu spurlos agieren. Es gibt zudem keine geografische Begrenzung, wodurch sich für den Täter der Kreis der Unternehmen vergrößert, die er von einem Ort aus schädigen kann.

[1] vgl. Frohn, Michael/Parthier, Ulrich (2005)
[2] vgl. Voß, Antje (2003), S.12
[3] vgl. Meisel, Alexander (2005):

Einige Täter veröffentlichen gefundene Sicherheitslöcher über das Internet, wodurch sich der potenzielle Täterkreis vergrößert.[1]

Mit Internetanbindungen und Einführung mobiler Technologien werden bidirektionale Zugangstüren geöffnet. Aus dem organisatorisch-technischen Zusammenspiel von Mitarbeitern, Partnern und Kunden, beruhend auf der Nutzung dieser Zugangstüren, entstehen über alle geschäftlichen Kernprozesse hinweg Sicherheitsrisiken. Besondere Angriffsflächen bieten Unternehmen, deren Produkte digitalisiert sind. Neben den einzelnen konkret gefährdeten Prozessbestandteilen sind die durch das Zusammenspiel von Menschen, Soft-/Hardware und Netzen sich ergebenden möglichen Bedrohungen zu berücksichtigen.[2]

Die „digitalen Bedrohungen“[3] sind ein Spiegelbild der Bedrohungen der physischen Welt. Wie in der physischen Welt muss daher auch in der virtuellen Welt dafür gesorgt werden, dass Systeme spezielle Eigenschaften möglichst unter allen Umständen bewahren. Bei diesen Eigenschaften handelt es sich im Wesentlichen um Vertraulichkeit, Integrität und Verfügbarkeit. Interaktionen mit dem System müssen daher autorisiert sein, Benutzern müssen Privilegien zugeordnet werden, Angriffe müssen erkannt und abgewehrt werden. Es geht somit im weitesten Sinne um Maßnahmen der Erkennung/Behandlung/Vorbeugung unautorisierter Aktionen, um Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

1.1.2 … abgeleitet aus externen und internen Ordnungsmäßigkeitsvorgaben

Externe Ordnungsmäßigkeitsanforderungen in Form von gesetzlichen Vorgaben, z. B. dem KonTraG, mit dem Ziel, Gefahren für das Unternehmen zu minimieren bzw. frühzeitig zu erkennen, fordern – auf die IT-Sicherheit übertragen – den Aufbau einer IT-Sicherheitsinfrastruktur. Dazu ist es u. a. notwendig zu bestimmen, woraus sich rechtliche Risiken (d. h. Risiken der vorsätzlichen oder fahrlässigen Nichtbeachtung gesetzlicher Vorschriften) beim Einsatz von Informations- und Kommunikationstechnologie ergeben können. Zu nennen sind hier vor allem die nicht ausreichende Beachtung datenschutzrechtlicher Vorgaben, die Verletzung des Fernmeldegeheimnisses durch möglicherweise zu weit gehende Überwachungsmaßnahmen und das Übersehen relevanter Strafvorschriften.[4]

Insbesondere beim Einsatz mobiler Geräte und Kommunikationsmedien muss im Rahmen von Prüfungen bzw. Revisionen auf die Regelungen und Weisungen zum Umgang mit diesen

[1] vgl. Pietsch, Thomas (2004), S.257
[2] vgl. Brewing, Josef (2005)
[3] vgl. Schneier, Bruce (2000), S.11-20
[4] vgl. Knupfer, Jörg (2005)

Systemen fokussiert werden. Denn mobile Geräte und Kommunikationsmedien sind nicht permanent in eine zentrale Infrastruktur eingebunden und unterliegen somit keiner ständigen Kontrolle.[1] Interne Ordnungsmäßigkeitsanforderungen für den IT-Bereich zielen darauf ab, ein Höchstmaß an Effizienz und Effektivität bei der Nutzung moderner Informations- und Kommunikationstechnik zu erreichen. So erfordert z. B. die effektive Steuerung Unternehmens übergreifender Wertschöpfungsketten einen fehlerfreien Informationsaustausch zwischen den Partnern. Durch die mangelnde Datenintegration der übergreifenden Wertschöpfungskette entsteht Intransparenz (über Bestände und ein- und abgehende Lieferungen). Um die heterogenen IT-Strukturen der Partner einer Wertschöpfungskette in einer schlanken, stabilen Lieferkette zu integrieren, ist eine neutrale Integrationsplattform erforderlich, die eine strukturierte Kommunikation zwischen den Gliedern der Wertschöpfungskette ermöglicht. Der Anwender reduziert durch eine zentrale Schnittstelle zur Integrationsplattform die Komplexität des Datenaustausches. Da es an der Datenqualität der integrierten Partner oft mangelt, werden Systeme zwischengeschaltet, die die ausgetauschten Daten semantisch, syntaktisch und nach logischen Plausibilitätskriterien prüfen. Falsch eingestellte IT-Systeme werden erkannt und fehlerhafte Datensätze an den Sender zurück übermittelt. Der eigentliche logistische Prozess kann von der IT, ausgehend von Statusdaten durch einen Abgleich zwischen Soll (etwa geplanter Zustellungszeit) und Ist (Zustellstatus) vorgenommen werden. Bleibt der Zustellstatus aus, werden die am Prozess beteiligten Partner informiert und können entsprechend eingreifen. Zur weiteren Optimierung der Logistikkette werden übergreifende Managementinformationssysteme eingesetzt. Diese sollen die unternehmensübergreifende Prozesssteuerung und die Performancemessung über einen längeren Zeitraum hinweg ermöglichen. Unternehmensübergreifend sollen die Logistikpartner auf die gleichen Informationen zugreifen können. Auf dieser Basis lassen sich dann weitere Prozess-optimierende (kundenspezifische) Applikationen (z. B. „elektronische Abrechnung von Leistungen“ oder „Behältermanagement“ (Steuerung, Disposition und Verwaltung von Ladungsträgern)) einsetzen.

Es ist offensichtlich, dass die IT-Sicherheit in einer solchen Logistikkette eine entscheidende Rolle spielt. Im Kontext der zu behandelnden Thematik geht es um die Bedeutung der IT-Security allgemein für die Gestaltung der organisatorischen Abwicklung von Geschäftsprozessen. Dabei bildet die Berücksichtigung der Ungewissheit bezüglich zukünftiger Entwicklungen (rechtlich, organisatorisch, technisch) im Umfeld des Unternehmens den Ansatzpunkt zur Entwicklung eines entsprechenden Modells.

[1] vgl. Foth, Michael (2006a), S.35

1.1.3 … abgeleitet aus den Korrektheitsbedürfnissen der im Unternehmen durchlaufenden Informationen

Mit Korrektheitsbedürfnissen der im Unternehmen durchlaufenden Informationen ist gemeint, dass die richtigen Informationen zum richtigen Zeitpunkt mit dem notwendigen Genauigkeits- und Verdichtungsgrad am richtigen Ort zur Verfügung stehen. Die „rechtzeitige Versorgung der Handlungs- und Entscheidungsträger mit allen notwendigen und relevanten Informationen in wirtschaftlich sinnvoller Weise“ ist ganz allgemein die Aufgabe eines Informationssystems.[1] Ein wirksames Management-Informations-System (MIS), das die wesentlichen Informationen in der erforderlichen Form rechtzeitig sowohl top-down vom Top-Management zur operativen Ebene als auch bottom-up von der operativen Ebene zum Top-Management vermittelt, ist Voraussetzung für ein wirksames Risikomanagement-System. Dies betrifft nicht nur den unternehmensinternen Informationsfluss, sondern auch die Beschaffung externer Informationen, z. B. im Rahmen der Unternehmensplanung zur Vorbereitung strategischer Entscheidungen.[2] Zu den Tätigkeiten des Informationssystems im Zusammenhang mit der Bereitstellung der für Entscheidungsprozesse notwendigen Informationen gehört die Gewinnung aller relevanten, richtigen, vollständigen und aktuellen Informationen über die Unternehmung und die Umwelt. Dazu gehören auch entsprechende Prozesse der Beschaffung, Verarbeitung, Speicherung und Übermittlung, wobei Qualität von Planung und Kontrolle von der Qualität der vom Informationssystem bereitgestellten Informationen abhängt.[3]

Informationssysteme bilden damit die Basis für alle Managementprozesse und lassen sich im Wesentlichen in Administrations- und Dispositionssysteme (ADS) und Entscheidungsunterstützende Systeme (EUS) unterteilen. ADS werden vorwiegend in den operativen Bereichen eines Unternehmens eingesetzt und unterstützen die laufende Abwicklung der Geschäftsvorfälle. Wichtige Aufgabe eines EUS (z. B. Executive Information System (EIS) oder Controlling Support System) ist die Unterstützung des Informationsaustausches und der Kommunikation zwischen der Unternehmensleitung und den Entscheidungsvorbereitern (z. B. Controllern und Risk Managern) durch Verwendung entsprechender Daten, Methoden und Modelle.[4]

Aus dem Einsatz eines EUS sollen so u. a. folgende positive Effekte resultieren:[5]

- durch effizientere und schnellere Informationsbereitstellung steigt das Angebot an Informationen,

[1] vgl. Romeike, Frank (2004), S.279
[2] vgl. PwC (2000):, S.13,14
[3] vgl. Kimmig, Jens M. (2001), S.31
[4] vgl. Romeike, Frank (2004), S.279-281
[5] vgl. Romeike, Frank (2004), S.277-279

- die Komplexität einer Entscheidungssituation wird transparenter, der Entscheider kann das Ausmaß eines Problems besser erfassen,
- Wirkungs- und Bewertungsdefekte können (aufgrund der hohen Verarbeitungsgeschwindigkeit und Kapazität mittels Durchspielen mehrerer Alternativszenarien in umfangreichen Simulationsläufen) verringert oder zumindest analysiert werden.

Unter Zuhilfenahme verschiedener formaler Verfahren versucht man, Einfluss auf die Unvollständigkeit von Informationen zu nehmen. Dabei wird die Unschärfe der Informationen in Betracht gezogen, indem sie einerseits die Konsistenz überprüft und andererseits notfalls mit unvollständigen Informationen auszukommen versucht.[1]

Auch ein Risk Management Informationssystem (RMIS) ist ein EUS. Es erfasst und verarbeitet in der Regel sowohl interne Daten aus den betrieblichen ADS als auch externe Daten (z. B. Informationen aus öffentlich zugänglichen Datenbanken, dem Internet oder von Versicherern). Ein RMIS soll die Planung, Steuerung, Durchführung und Kontrolle der unternehmerischen Risikopolitik unterstützen. Eine wesentliche Anforderung an ein RMIS besteht dabei darin, „einen reibungslosen Informations- und Kommunikationsaustausch zwischen den am Risk Management beteiligten Organisationseinheiten und betrieblichen Funktionsträgern zu gewährleisten“. Zusätzlich soll das RMIS den Risk Manager bei der Aufbereitung und Bereitstellung der gesammelten Daten unterstützen. Von zentraler Bedeutung ist dabei ein flexibler Aufbau, um das RMIS den kontinuierlichen Unternehmensveränderungen anpassen zu können. Die vom RMIS bereitgestellten Module dienen insbesondere einer effizienteren und schnelleren Informationsbeschaffung und -verarbeitung.[2]

Im Geschäftsleben stellen Informationen Unternehmenswerte dar, deren Verlust oder Missbrauch Unternehmen und Behörden aller Größenordnungen empfindlich treffen können. Informationen sind daher Werte, die wie jedes andere Vermögen des Unternehmens, gemäß der ihnen zukommenden Bedeutung angemessen gemanagt und geschützt werden müssen. Um besser vorhersehbare Geschäftsprozesse zu ermöglichen, müssen Unternehmen jederzeit und an jedem Ort relevante und präzise Informationen liefern können. Veränderungen, Risiken und Chancen sollen zum Zeitpunkt ihres Auftretens wahrgenommen, verstanden und darauf reagiert werden können. Dies erfordert die Nutzung von Echtzeitereignissen und -services.[3]

[1] vgl. Kremin-Buch, Beate/Unger, Fritz/Walz, Hartmut (2004), S.27
[2] vgl. Romeike, Frank (2004), S.281-287
[3] vgl. Fischer, Bettina (2005)

Und auch die effektive Steuerung Unternehmens-übergreifender Wertschöpfungsprozesse setzt den fehlerfreien Informationsaustausch zwischen den Partnern voraus. Die Abteilung des Unternehmens, die dafür die Verantwortung trägt, ist das Controlling. Der Unternehmensführung alle für die Planung, Durchführung und Kontrolle erforderlichen Ergebnisziel orientierten Informationen bereitzustellen, ist Aufgabe des sog. Informationsversorgungssystems.[1] Aufgabe im Zusammenhang mit IT-Sicherheit ist es, den laufenden Betrieb dieses IV-Systems sicherzustellen.

Man unterscheidet einen objektiven und einen subjektiven Informationsbedarf. Der objektive Informationsbedarf erfordert Informationen ausreichender Qualität und Quantität „um eine vorgegebene Aufgabenstellung erfüllen bzw. eine bestimmte Entscheidung treffen zu können und dabei die systemimmanente Gefahr von Fehleinschätzungen zu vermeiden bzw. weit möglichst zu minimieren“. Der subjektive Informationsbedarf des Entscheiders umfasst nur all jene Informationen, „die er aus seiner spezifischen (subjektiven) Sicht als relevant für die vorliegende Problemstellung erachtet“.[2]

Aufgrund der Bedeutung von Informationen für das Überleben und den wirtschaftlichen Erfolg von Unternehmen muss ein strategisches Informationsmanagement dabei auch Regelungen zu den Strukturen, Verantwortlichkeiten und Verfahren der IT-/IV-Sicherheit beinhalten. Die IT-/IV-Sicherheit muss die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität derjenigen Daten gewährleisten, aus denen die für die Entscheidungen des Unternehmensmanagements notwendigen Informationen generiert werden. Hierzu ist ein IT-/IV-Sicherheitsmanagement erforderlich, das sämtliche informationellen Ressourcen des Unternehmens vor jeglicher Art von Angriff, Zerstörung oder Diebstahl schützt. Dieses IT-/IV-Sicherheitsmanagement muss IT-/IV-Sicherheitsziele definieren, im Rahmen eines IT-/IV-Sicherheitskonzepts umsetzen und die aus dem IT-/IV-Sicherheitskonzept abgeleiteten Aufgaben steuern.[3] Unterschieden werden generische Sicherheitskonzepte und spezifische Sicherheitskonzepte. Generische Sicherheitskonzepte enthalten alle Sicherheitsregeln, -richtlinien und -standards eines Unternehmens. Spezifische Sicherheitskonzepte setzen die generischen Sicherheitskonzepte auf system- und plattformspezifischer Ebene um.[4]

[1] vgl. Stoi, Roman (2002), S.160
[2] vgl. Romeike, Frank (2004), S.277
[3] vgl. Pietsch, Thomas. (2004), S.257,258
[4] vgl. Müller, Klaus-Rainer (2003), S.20

Informationsmanagement als Teil der Unternehmensführung hat für den nutzbringenden Einsatz der Möglichkeiten der Informations- und Kommunikationstechnologien im Unternehmen zu sorgen. [1] Strategisches Informationsmanagement kommt dabei ohne dezentrale Informationsverarbeitungsstrukturen nicht mehr aus.[2] Risiken der Beeinträchtigung oder des Ausfalls von Informations-/Datennetzen sind sehr kritisch einzustufen, da diese für nahezu jedes Unternehmen einen strategischen Faktor mit existenzieller Bedeutung darstellen. Eine ähnliche Bedeutung hat die Datenintegrität innerhalb des Unternehmens: Leistungsfähige Server stellen enorme Konzentrationen von Datenmengen an einer einzigen Stelle dar. Der potenzielle Schaden im Fall von Verlust oder Beschädigung steigt mit der Konzentration der Daten. Der Zugriff auf diese Systeme per LAN erfordert die sichere Identifikation der jeweiligen Benutzer zur Sicherstellung, dass diese nur auf jene Daten zugreifen, für die sie autorisiert sind. Die heutzutage verwendeten Datentransferkonzepte beruhen auf veralteten Systemen, in denen sensible Daten über ein Netz, zumeist einfach über das Internet, Standort übergreifend ausgetauscht werden. Dies erhöht das Risiko eines Schadens durch Hacker, Saboteure, Spione usw. enorm.[3] Potenzielle Angreifer können, wenn es ihnen einmal gelingt, ins Unternehmensnetz einzudringen, nicht abschätzbaren Schaden anrichten.

Security ist eine Managementaufgabe, die die Erarbeitung klarer Sicherheitskonzepte erfordert, welche auf der IT-Sicherheits-/IT-Security-Strategie basieren. Bei der Beschaffung von Informationen zur Analyse und Prognose von Umwelt und Unternehmung für die strategische Planung (vernetzt mit strategischen Controlling-Werkzeugen[4]) kommt dabei dem Aufbau von Früherkennungssystemen eine zentrale Bedeutung zu.

1.2 IT-Sicherheitsstrategie

Strategie ist ein „Problemfindungs- und Problemlösungspfad in komplexen Situationen“. Sie versucht, die Komplexität vielschichtiger Probleme mit organisatorischen Mitteln zu reduzieren und so die Beherrschbarkeit der Komplexität herzustellen[5] und beinhaltet die Planung, wie Organisationen oder Individuen ihre Ziele erreichen wollen.[6] Bezüglich der strategischen Ziele von Unternehmen ist die Steigerung der Wirtschaftlichkeit bei einer

[1] vgl. Zarnekow, Rüdiger (2005)
[2] vgl. Pietsch, Thomas (2004), S.253,54
[3] vgl. Pietsch, Thomas (2004), S.254,55
[4] vgl. Gadatsch, Andreas (2006), S.12-15
[5] vgl. Hinterhuber, Hans H. (2004b), S.141-146
[6] Ehrmann, Thomas (2006, S.6

gleichzeitigen Reduzierung der Reaktionszeiten und einer Erhöhung des Kundennutzens von größter Bedeutung.[1]

Die IT-Strategie soll sicherstellen, dass der „gesamte Bereich der Informationstechnik mit zur Erreichung der Unternehmensziele beiträgt“ , d. h., sie soll innovative Projekte identifizieren, die langfristig die Wettbewerbsfähigkeit des Unternehmens stärken und den Unternehmenswert erhöhen[2] und sicherstellen, dass „die IT-Budgets durch Priorisierung in die Projekte fließen, die den höchsten ROI/Nutzenbeitrag versprechen und die Geschäftsprozesse eines Unternehmens bezüglich deren strategischer Ausrichtung ideal unterstützt werden“.[3] Die IT muss neue Geschäftsprozesse, interne und externe Vorgaben, z. B. in Form gesetzlicher Änderungen und durch die Dynamik des Marktes vorgegebene kürzere Produktzyklen, unterstützen.

Bei der Operationalisierung der IT-Strategie, d. h. der auf die Teilsysteme der Unternehmens-IT bezogenen Konkretisierung, geht es vor allem darum, für jedes Teilsystem der Unternehmens-IT eine „individuelle Ausrichtung der eingesetzten Technologie zu bestimmen“.[4]

Um das Vertrauen der Kunden zu stärken, und die Reputation des Unternehmens nicht zu gefährden, rücken Werte wie Vertrauen und Zuverlässigkeit in den Mittelpunkt. Zunehmend werden dabei Service-Technologien attraktiver, die Eigenschaften wie Flexibilität und Skalierbarkeit versprechen. Als Beispiel sei der Ersatz von Netzwerk-Technologien wie Frame Relay (datenpaketorientierte Übertragungstechnik) und Asynchronous Transfer Mode (ATM) durch Internet Protocol Virtual Private Network (IP-VPN) genannt. Interne wie externe Netzwerke und Geschäftsprozesse müssen geschützt werden. Dieser Schutz bezieht sich auf Qualität, Effizienz und Sicherheit. Technische, organisatorische und strategische Maßnahmen bezüglich Qualität, Effizienz und Sicherheit sind dazu in einer ganzheitlichen Lösung geeignet zu kombinieren. Um die notwendige IT-Sicherheit zu gewährleisten, müssen zunächst die betroffenen Geschäftsprozesse analysiert werden. Die Optimierung und der Schutz der abgebildeten Prozesse einerseits und der IT-Infrastrukturen andererseits, sollen die Sicherheit der internen wie externen Netzwerke und Geschäftsprozesse sowie deren Qualität und Effizienz gewährleisten.[5]

[1] vgl. Hofmann, Ralf (2003), S.42
[2] vgl. Buchta, Dirk Uwe (2004):, S.13
[3] vgl. Scheer, August.-W (2004), S.359
[4] vgl. Haug, Andreas (2005)
[5] vgl. Henze, Detlev/Parthier, Ulrich. (2005)

Um solche ganzheitlichen, neuen und innovativen Lösungen abzuleiten, soll im Kontext der gegebenen Thematik ein IT-Security-Framework entwickelt werden, das die strategische Ebene mit der technisch-organisatorischen IT-Sicherheits-/IT-Security-Ebene verbindet.

Dazu wird von der Konkretisierung des Strategiebegriffs im Sinne der strategischen Unternehmensführung als „langfristige, nicht unmittelbar erkennbare Führung eines Systems“[1] mit dem Ziel, (operative) Erfolgspotenziale aufzubauen und zu sichern[2], ausgegangen. „Nicht unmittelbar erkennbar“ bedeutet, dass die Strategie für mögliche Konkurrenten in der Regel nicht ersichtlich sein soll.

Unter dem Begriff Management oder Unternehmensführung wird die Gesamtheit aller Handlungen verstanden, welche die Gestaltung und Koordination der Interaktionen mit der Unternehmensumwelt im Rahmen der Wertschöpfungsprozesse zum Gegenstand haben und grundlegend beeinflussen.[3]

Strategische Ziele markieren Zwischenschritte bei der Realisierung der unternehmerischen Vision, der generellen Leitidee für die zukünftige Entwicklung des Unternehmens. Sie beziehen sich zumeist auf die finanzielle, die Kunden- und Markt-, die Performance- und die infrastrukturelle Perspektive.[4] In der risikopolitischen Vision werden die grundlegenden Vorstellungen über die Zwecke des Risikomanagements und die entsprechenden Verhaltensweisen der Mitarbeiter in knapper Form zusammengefasst.[5] Die Risikobereitschaft eines Unternehmens drückt sich in der risikopolitischen Strategie (risikofreudig, risikoneutral, risikoscheu) aus. Hinsichtlich finanzieller Risiken bedeutet eine risikoneutrale Strategie, bezüglich rein monetär zu bewertender Risiken, einen wirtschaftlich optimalen Grad an Sicherheit anzustreben.[6] Die risikopolitische Strategie unterliegt nicht in vollem Umfang der unternehmerischen Gestaltungsfreiheit, sie ist insbesondere in Form von Gesetzen, behördlichen Verordnungen, Erlassen und Richtlinien zum Teil gravierenden Einschränkungen unterworfen. Eine Präzisierung der Risikopolitik erfolgt durch die Festlegung konkreter, messbarer operativer Ziele, die Grundlage für Kontrolle und Steuerung des Risikomanagements bilden.[7]

[1] vgl. Oetinger, Bolko von (2000), S.15
[2] vgl. Eschenbach, Rolf (2003):, S.10
[3] Diederichs, Marc (2004), S.11
[4] vgl. Seidenschwarz, Werner/Huber, Christian (2002), S.133
[5] vgl. Dahmen, Jörn (2002), S.49
[6] vgl. Dahmen, Jörn (2002), S.50,51
[7] vgl. Dahmen, Jörn (2002), S.53

Die Vision beinhaltet keine konkreten Ziele und Handlungsanweisungen. Ausdruck der Vision sind vielmehr zunächst die unternehmungspolitischen Grundsätze.[1] Eine Strategie wird aus diesen unternehmungspolitischen Grundsätzen abgleitet, in spezifische Handlungsrichtlinien übersetzt, eine entsprechende Organisationsstruktur abgeleitet und in Form angemessener Ausführungsschritte umgesetzt.

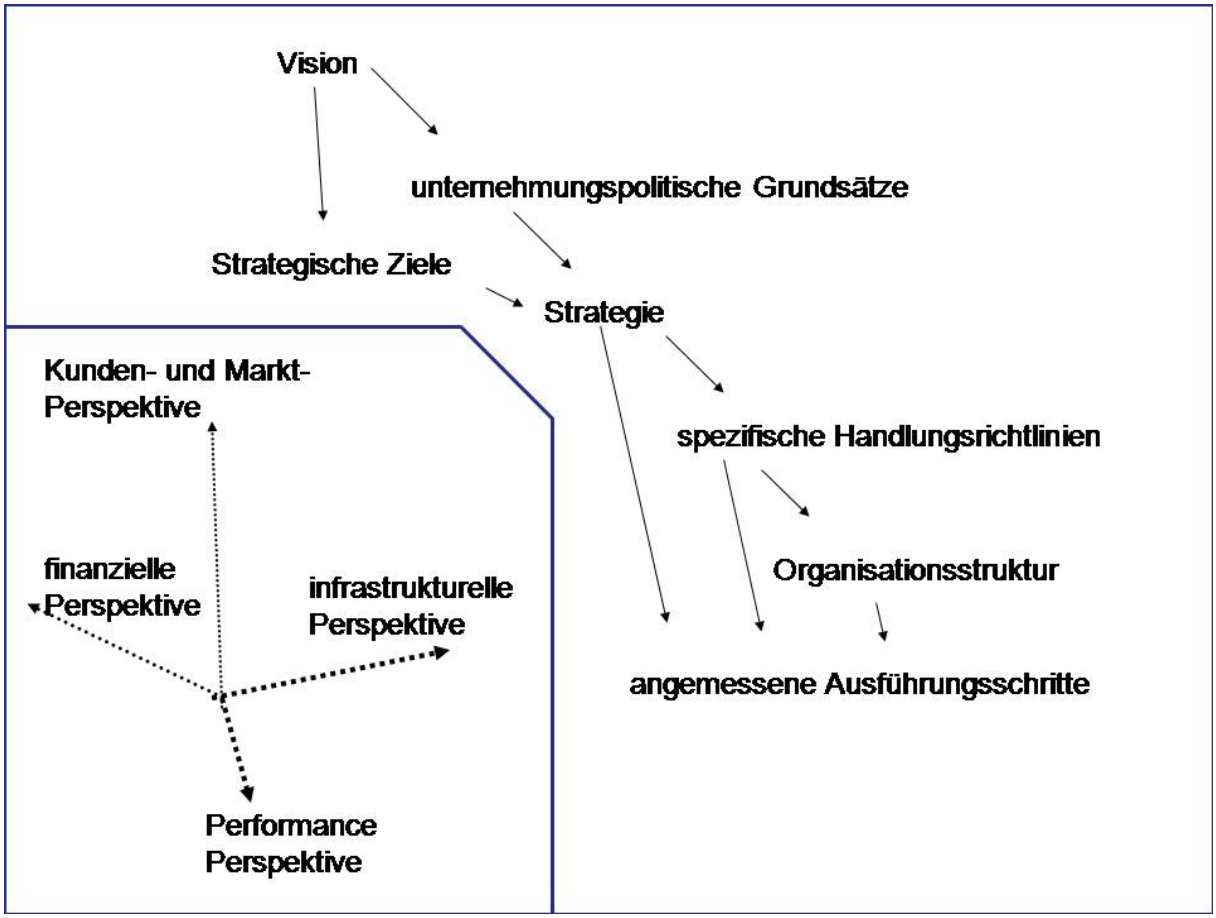


Abb. 4 Zusammenhang zwischen Vision, Strategie und Ausführungsschritten

Mit einer Sicherheitsstrategie werden Sicherheitsprinzipien/-richtlinien umgesetzt.[2] Sicherheitsrichtlinien sollen dem Unternehmen helfen, Risiken zu minimieren und Vorsorge für den Notfall zu treffen.[3] Diese Richtlinien können auf einem Sicherheitsmodell basieren. Dieses definiert die Methode, wie die Richtlinien und die dazu verwendeten Technologien implementiert und umgesetzt werden.[4]

Auf technischer Ebene gehört zu solchen Sicherheitsstrategien der Einsatz von Virenscannern, richtig konfigurierten Firewalls und Intrusion Detection/Prevention Systemen[5] (IDS/IPS).

[1] vgl. Hinterhuber, Hans H. (2004a), S. V,VI
[2] vgl. Mühlenbrock, Frank (2003), S.82
[3] vgl. Mühlenbrock, Frank (2003), S.23
[4] vgl. Mühlenbrock, Frank (2003), S.32,33
[5] vgl. Poels, Torsten. (2004a)

Standardisierte Firewalls und einzelne technische Ad-hoc Lösungen sind jedoch unzureichend, wichtig sind ganzheitliche Lösungen und Strategien.

Sicherheitsstrategien auf dieser Ebene können aus der Denkweise und der Vorgehensweise von Hackern abgeleitet werden.[1] Das Nachvollziehen der Methoden und Vorgehensweisen von Hackern ist ein Weg, Risiken eigener IT-Systeme und IT-Infrastrukturen zu erkennen. Dies soll dann zu Strategien führen, um die erkannten Risiken abzusichern.[2]

Für die IT-Security-Strategie sind strategische Ziele vor allem in der Performance- und in der infrastrukturellen Perspektive relevant. Performance meint die Qualität und Effizienz der Umsetzung von Vorgaben. Die Umsetzung der IT-Sicherheitsstrategie in Form angemessener Ausführungsschritte setzt die Evaluierung geeigneter Sicherheitsmaßnahmen voraus. Dies ist eine zentrale Aufgabe des Risikomanagements. Risk-Assessment betrifft dagegen vor allem die infrastrukturelle Perspektive.

Im Zusammenhang mit der gegebenen Thematik wird darüber hinaus davon ausgegangen, dass die IT-Security-Strategie aus der IT-Strategie abgleitet wird und diese unterstützen soll. Dies hat zur Folge, dass einer der wichtigsten Zielgegenstände des strategischen IT-Security-Managements mit dem Gegenstand des strategischen IT-Managements übereinstimmt. Dies sind die mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens.

1.3 IT-Security-Prozess

1.3.1 Modellierung und Aufgabenstellung/Einordnung in übergeordnete Unternehmensprozesse und -aktivitäten

Informationen und deren nicht manipulierbarer, schneller und verlässlicher Austausch sind ein zentraler Faktor unseres Wirtschaftslebens geworden. Dies, und die zugrunde liegende IT-Infrastruktur mit ihren Komponenten und IT-Systemen ist mit gemanagter IT-Sicherheit zu schützen. Die Minimierung von Risiken, die sich z. B. aus der IT-Infrastruktur ergeben, muss im Rahmen geeigneter Prozesse umgesetzt werden. Dabei geht es nicht allein darum, Anforderungen an die IT-Sicherheit punktuell mit entsprechenden Maßnahmen abzudecken und Bedrohungen z. B. aus öffentlichen Netzen, wie dem Internet, zu begegnen. Der Ausgangs-

[1] vgl. Poels, Torsten. (2004a)
[2] vgl. Ernst & Young (2005)

punkt zur Etablierung gemanagter IT-Sicherheit ist eine gute Security Policy (Sicherheitsvorgaben/-richtlinien). Zur Umsetzung dieser gemanagten IT-Sicherheit sind entsprechende Prozesse im Bereich der Informationssicherheit zu implementieren (etwa Incident Handling, Reporting oder Change Management). Incident Handling oder auch Behandlung von Sicherheitsvorfällen ist ein Prozess der Informationssicherheit, durch den Verletzungen der Sicherheitsvorgaben erkannt werden, koordinierte Reaktionen erfolgen und Auswertungen stattfinden. Gemanagte IT-Sicherheit muss dies mit gesetzlichen Bestimmungen, internationalen Standards, wirtschaftlichen IT-Lösungen sowie der Sicherung des Unternehmenserfolgs verknüpfen.[1]

Als wichtigste Geschäftsprozesse, die die Wertschöpfung in einem Unternehmen bestimmen, werden zumeist der Innovationsprozess, der Kundenmanagement-Prozess, operative Prozesse sowie gesetzliche- und Umweltprozesse angesehen. Mit den gesetzlichen Prozessen und Umweltprozessen passt sich das Unternehmen – mehr oder weniger gut und schnell – den sich wandelnden gesetzlichen, sozialen und ökologischen Entwicklungen an. Wirkungszusammenhänge zur Wertschöpfung im Unternehmen werden zumeist in den vier Dimensionen Finanzperspektive, Kundenperspektive, interne Prozessperspektive sowie Lern- und Entwicklungsperspektive abgebildet. In der Lern- und Entwicklungsperspektive wird Ausbildung und Motivation der Mitarbeiter betrachtet. Gut ausgebildete und hoch motivierte Mitarbeiter führen zumeist zu hoher Innovationskraft, zum intensiven Einsatz moderner Informations- und Kommunikationstechnologien sowie effizienteren und hochwertigeren Geschäftsprozessen. Über die Erhöhung der Produktivität und die Verbesserung der Kundenbeziehungen beeinflussen diese den Unternehmenswert und die finanzielle Perspektive.[2]

IT-Sicherheit muss alle internen und externen Unternehmensprozesse umfassen, die in Beziehung zu den IT-Systemen stehen. Dies kann prinzipiell alle der oben aufgeführten wichtigsten Geschäftsprozesse umfassen, die die Wertschöpfung in einem Unternehmen bestimmen.

Der IT-Sicherheitsprozess ist nicht als konkreter Kernprozess eines Unternehmens zu verstehen. Vielmehr soll er das grundsätzliche unternehmensweite Vorgehen beschreiben, um für alle Prozesse und IT-Systeme geeignete IT-Sicherheitskonzepte zu entwickeln, zielgerichtet

[1] vgl. Henze, Detlef/Parthier, Ulrich. (2005)
[2] vgl. Rosenkranz, Friedrich (2006), S.11,12

umzusetzen und regelmäßig zu überprüfen. Er muss dazu alle relevanten IT-gestützten Abläufe im Unternehmen durchdringen.[1]

Dabei müssen IT-Sicherheitsmaßnahmen in gegebenenfalls bestehende ganzheitliche Sicherheitskonzepte (wie Werkschutz, Produktionssicherheit, Datenschutz, Arbeitssicherheit) und der notwendige IT-Sicherheitsprozess in alle IT-gestützten Geschäftsprozesse integriert werden. Beispielsweise müssen Maßnahmen der Gebäudesicherheit Kabelwege schützen, damit der Datenverkehr nicht abgehört oder unterbrochen werden kann. IT-Sicherheit muss alle Prozesse (Kern- und unterstützende Prozesse) sowie alle Funktionsbereiche des Unternehmens (Personalwesen, Einkauf, Organisation, Qualitätsmanagement, Changemanagement, Datenschutz, Unternehmenskommunikation …) durchdringen. So kann etwa der Einkauf durch sicherheitsorientierte Auswahl von Lieferanten mit verhindern, dass Informationen über die Infrastruktur oder die IT-Sicherheitsmaßnahmen des Unternehmens in falsche Hände geraten. Und die Organisationsabteilung des Unternehmens sollte proaktiv daran mitwirken, Prozessrisiken zu vermeiden. Weitere unterstützende Prozesse/Arbeitsmethodiken stellen die Basis für die Implementierung der IT-Sicherheit dar: Dokumentation aller Prozesse und Systeme, konzeptorientierte Arbeitsweise, verantwortungsvoller Umgang mit den Daten und Systemen des Unternehmens usw.[2]

Damit wird deutlich, dass das zu entwickelnde IT-Security-Framework, das die strategische Ebene mit der technisch-organisatorischen IT-Sicherheits-/IT-Security-Ebene verbindet, einen entsprechenden IT-Sicherheits-/IT-Security-Prozess integrieren sollte.

Vor allem wenn Geschäftsprozesse internetbasiert ablaufen, sind sichere IT-Systeme Voraussetzung für den Erfolg der entsprechenden Geschäftsmodelle. Geschäftsmodelle geben in abstrakter Form Hauptcharakteristiken von Geschäftsprozessen wieder, sind eine aggregierte Darstellung von Geschäftsprozessen, wobei die Veranschaulichung kreativer Prozessideen oft für innovative Produkte und Leistungen im Vordergrund steht.[3] Um bei hoher Dynamik technologischer, organisatorischer und geschäftlicher Veränderungen die erforderliche Sicherheit zu erreichen, ist ein in die Geschäftsabläufe integrierter IT-Security-Management-Prozess unverzichtbar.[4]

Zudem ist ein Security-Audit zu etablieren, welches beginnend mit einem Security-Review, – das Sicherheitspolitik und -konzept einer kritischen Prüfung auf Konsistenz und Ange-

[1] vgl. Rieger, Holger (2005b), S.64
[2] vgl. Rieger, Holger (2005b), S.54-62
[3] vgl. Rosenkranz, Friedrich (2006), S.2,3
[4] vgl. Horster, Patrick (2002b), S.81-89

messenheit von Maßnahmen und Richtlinien unterzieht, - die korrekte Umsetzung von Maßnahmen und Richtlinien kontrolliert, nach technischen Sicherheitslücken sucht, und die Ergebnisse auf Sicherheitspolitik und -konzept zurückkoppelt.[1]

1.3.2 Strukturierung der Unbestimmtheit der Zielvorgabe und -erreichung/der operativen Bestandteile einer ganzheitlichen IT-Security-Strategie

Die planerische Vorbereitung und Unterstützung von (strategisch relevanten) Aktivitäten im Zusammenhang mit der Gewährleistung der unternehmerischen Handlungsfähigkeit setzt die (gedankliche) Bewältigung neuer Anforderungen voraus. Dazu werden Strukturierungshilfen benötigt, mit deren Hilfe möglichst handhabbare Modelle erarbeitet und angewandt werden können.[2]

Der IT-Sicherheits-/IT-Security-Prozess ist nicht nur auf gegenwärtige Anforderungen an die IT-Sicherheit/IT-Security beschränkt, sondern muss vor allem mit ungewissen zukünftigen Anforderungen umgehen können, wobei Security als strategisches Unternehmensziel betrachtet wird. Diese Ungewissheit wird zunächst hingenommen, um in einem weiteren Schritt ihre Struktur verstehen zu lernen und sie schließlich in die Strategieüberlegungen zu integrieren. Dieser gedankliche Ansatz bildet die Basis für die benötigten Strukturierungshilfen, mit deren Hilfe ein Modell zum Controlling der IT-Security erarbeitet wird.

Die Zielvereinbarung und -formulierung fragt nach dem Sinn des Unternehmens und seinen Verpflichtungen in seinem Umfeld.[3] In Zusammenhang mit Zielen versteht man unter Effektivität die Zielauswahl und unter Effizienz die Zielerreichung. Vereinfacht ausgedrückt bedeutet Effektivität „die richtigen Dinge tun“, und Effizienz „die Dinge richtig tun“.[4] Ob der IT-Sicherheits-/IT-Security-Prozess die im Hinblick auf ungenaue gegenwärtige und ungewisse zukünftige Anforderungen benötigte Effektivität und Effizienz aufweist, ist im Allgemeinen unbestimmt.

Das Risiko, dass der IT-Sicherheits-/IT-Security-Prozess nicht die benötigte Effektivität und Effizienz aufweist, ist das eigentliche zu managende Risiko. Dies soll als eine Aufgabe des IT-Security-Managements definiert werden. Dabei geht es um das Risiko ungültiger oder falscher Zielvorgaben aufgrund falscher Annahmen und das Risiko mangelnder Umsetzung,

[1] vgl. Bursch, Daniel (2005), S.117
[2] vgl. Ehrmann, Thomas (2006), S.1
[3] vgl. Gadatsch, Andreas (2004), S.37
[4] vgl. Stahlknecht, Peter (2003), S.13

was auch zu Zielverfehlungen führt. Weitere Aufgabe des operativen IT-Security-Managements ist die Bestimmung von den Zielvorgaben angemessenen Sicherheitsmaßnahmen. Die Zielerfüllung ist dann abhängig vom Umsetzungsvermögen des operativen Managements und seiner Mitarbeiter.

Der Aufbau eines IT-Security-Managements, bei dem es um die Effektivität und Effizienz des IT-Security-Prozesses geht, erfordert die detaillierte Untersuchung der Gründe für die Unbestimmtheit der Zielvorgabe und Zielerreichung des IT-Security-Prozesses, welche abstrakt mit ungenauen gegenwärtigen und ungewissen zukünftigen Anforderungen an die IT-Sicherheit/IT-Security angegeben wurden.

Für eine geschäftsübergreifende Unternehmensstrategie bieten sich fünf eng miteinander verzahnte Planungsebenen an: Ressourcenebene, sozio-technische Ebene, Organisationsebene, Geschäftsebene und Unternehmensebene. Auf der Ressourcenebene erfolgt die ganzheitliche Planung der Ressourcen, um Engpässe zu vermeiden. Ziel bezüglich der IT-Vermögenswerte ist ihr optimaler Einsatz zur Umsetzung der Unternehmensstrategie. Auf der sozio-technischen Ebene werden die systemimmanenten Erfolgspotenziale im operativen Geschäft erschlossen. Auf der Organisationsebene werden die strategischen Geschäftsziele durch Organisation optimierter Prozesse umgesetzt. Auf der Geschäftsebene erfolgt die Identifikation und Erschließung von Marktpotenzialen im Rahmen strategischer Geschäftsfelder. Auf der Unternehmensebene erfolgt die Führung der Geschäftsfelder sowie Entwicklung und Pflege der Unternehmensstrategie.

Security wird als strategisches Unternehmensziel, die IT-Security-Strategie als geschäftsübergreifende Unternehmensstrategie gesehen. Der IT-Security-Prozess enthält eine Planungskomponente bezüglich der IT-Security-Strategie. Demzufolge können die ungenauen gegenwärtigen und ungewissen zukünftigen Anforderungen an die IT-Sicherheit/IT-Security als Grund für die Unbestimmtheit der Zielvorgabe und Zielerreichung des IT-Security-Prozesses auf den obigen Planungsebenen untersucht werden.

Auf den Ebenen der Gründe für die Unbestimmtheit der Zielvorgabe und Zielerreichung des IT-Security-Prozesses können die operativen Bestandteile einer ganzheitlichen IT-Security-Strategie des Unternehmens identifiziert werden. Diese beziehen sich auf die physischen Objekte Hardware, Software, Netze und Personal und logischen Objekte wie Informationssysteme, Datenbanken, Kommunikationsbeziehungen sowie Konzepte wie Vorgehensmodelle, Systementwicklungsmethoden und Richtlinien für den Werkzeugeinsatz.

Diese können jeweils aus den Perspektiven betrachtet werden, auf die sich strategische Ziele im Allgemeinen beziehen: der finanziellen, der Kunden- und Markt-, der Performance- und der infrastrukturellen Perspektive.

Auf der Ressourcenebene ist bei der ganzheitlichen Planung der von den Geschäftsprozessen benötigten Ressourcen zu berücksichtigen, dass Aktivitäten eines Geschäftsprozesses bei ihrer Ausführung nicht nur zeitlichen und sachlich/logischen, sondern durch nicht oder nicht genügende Produktionsfaktoren/Ressourcen anderweitigen Restriktionen unterliegen.[1]

Auch Restriktionen bezüglich des IT-Personals spielen hier eine wichtige Rolle. Damit der optimale Einsatz der zur Verfügung stehenden IT-Security-Technologie zur Umsetzung der IT-Security-Strategie gewährleistet ist, muss auch entsprechendes Know-how vorhanden sein.

Auf der sozio-technischen Ebene geht es vor allem um das Management von Risiken, um die systemimmanenten Erfolgspotenziale im operativen Geschäft nicht zu gefährden. Dazu ist eine geeignete Sicherheitsinfrastruktur aufzubauen.

Die Sicherheitsarchitektur legt fest, in welchen Bereichen der Technik welche Elemente/Komponenten zur Realisierung/Umsetzung von Sicherheitsanforderungen aus Sicht der Anwender/Kunden der Informationsverarbeitung zur Verfügung stehen.[2]

Die IT-Sicherheitsarchitektur ist das technische Abbild, die technische Realisierung der Sicherheitspolitik und der -richtlinien. Sie bildet die Basis zur Auswahl von Sicherheitsprodukten, die in die IT-Infrastruktur implementiert werden. Die zielgerichtete Nutzung der Sicherheitsprodukte und -komponenten soll die IT-Sicherheitsorganisation gewährleisten. Dazu sind organisatorische Aspekte der IT-Sicherheit in die Organisation des Geschäftsbetriebs einzubeziehen.[3]

Auf der Organisationsebene geht es dann um die Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume. Diese Ebene setzt auf die beiden Ebenen darunter (sozio-technische und Ressourcenebene) auf. Während diese drei Ebenen aus der Performance- und der infrastrukturellen Perspektive betrachtet wurden, wird die Geschäftsebene aus der Kunden- und Markt-Perspektive betrachtet. Von Bedeutung im Zusammenhang mit der IT-Security ist hier die Bereitstellung von IT-Dienstleistungen,

[1] vgl. Rosenkranz, Friedrich (2006), S.26
[2] vgl. Müller, Klaus-Rainer (2003), S.19
[3] vgl. Gadatsch, Andreas (2003), Kap.6.6.2

Wichtig für jede Form von bedarfsorientierter Bereitstellung beliebiger IT-Dienstleistungen ist die Service-Orientierung der IT-Architektur. Gefordert werden IT-Services mit nachvollziehbarem Wertbeitrag, die die geschäftlichen Anforderungen der einzelnen Unternehmensbereiche optimal unterstützen.[1]

Auf der Unternehmensebene geht es im Zusammenhang mit der IT-Security um Entwicklung und Pflege der IT-Security-Strategie. Aus der Geschäftsstrategie des Unternehmens leiten sich die Sicherheitspolitik und -richtlinien ab. Diese bilden die Grundlage für das IT-Sicherheitskonzept.[2]

Risiken ungültiger oder falscher Zielvorgaben ergeben sich vor allem aufgrund falscher Annahmen über Restriktionen der Geschäftsprozesse bei ihrer Ausführung sowie der Bereitstellung von IT-Dienstleistungen.

Der IT-Security-Prozess ist mit den Unternehmenszielen abzustimmen. Bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander benötigt das Unternehmen eine entsprechende strategisch-operative Beweglichkeit/Handlungsbefähigung. Die Bedeutung der IT-Security für Formulierung und Umsetzung der strategisch-operativen Zielsetzungen des Unternehmens liegt also auch darin begründet, dass die als Voraussetzung zum Erreichen der strategisch-operativen Zielsetzungen des Unternehmens angesehene strategisch-operative Beweglichkeit/Handlungsbefähigung auch von der IT-Sicherheit entsprechender IT-Systeme abhängt.

[1] vgl. Lautenbach, Annette (2005)
[2] vgl. Gadatsch, Andreas (2003), Kap.6.6.2

2 Anforderungsgrundlagen zur Revision, zum Controlling und zur Risiko-orientierten Ausgestaltung der IT-Security

In der Diskussion um Unternehmensführung und -kontrolle tauchte der Begriff Corporate Governance auf. Darunter versteht man alle Regeln, die zwischen den Eigentümern des Unternehmens (z. B. Aktionären) und den Verantwortlichen für die Geschäftstätigkeit des Unternehmens vereinbart werden.[1] Ein zentraler Gesichtspunkt dabei ist die Forderung der Eigentümer nach einem verantwortungsvollen Umgang der Geschäftsführung mit den der Geschäftstätigkeit inhärenten Risiken. Entscheidungsrelevante Risikoinformationen müssen jederzeit rechtzeitig zur Verfügung stehen. In einem umfassenden Sinn bezeichnet Corporate Governance die rechtlichen und institutionellen Rahmenbedingungen sowie die unternehmensinternen Instrumente, die Leitung und Kontrolle eines Unternehmens beeinflussen.[2]

Zunächst geht es um die sorgfältige strategische Analyse des Markts, der Stellung des eigenen Unternehmens im Mark (strategische Planung) und damit zusammenhängende Chancen und Risiken. Im Rahmen von Revisionen beginnt bereits bei der Prüfungsplanung und -vorbereitung die Berücksichtigung relevanter Gesetze. Aber auch das Controlling sollte die Zielsetzungen der gesetzlich fixierten Anforderungen unterstützen. Im Rahmen des strategischen Controllings (an die strategische Planung anschließend) ist die „Anfälligkeit des Unternehmens gegenüber externen und internen negativen Einflüssen“ genauer zu analysieren. Im Hinblick auf die Analyse interner Einflussfaktoren geht es um umfangreiche Untersuchungen, die unter dem Begriff Risk Management zusammengefasst werden.[3]

Alle relevanten Unternehmensrisiken (extern und intern) sollen durch die Elemente der Corporate Control als Bereich der Corporate Governance vollständig abgedeckt werden. Corporate Control hat (im Sinne von Compliance) nichtkonforme (d. h. mit nicht auf Regelbefolgung ausgerichteten Maßnahmen[4]) bzw. (im Sinne von Effektivität und Effizienz) nicht optimal funktionierende Teilsysteme des Unternehmens zu identifizieren und zu überwachen. Sie stützt sich dabei auf die wesentlichen Elemente unternehmensweites Risikomanagement, interne Revision und externe Revision.[5]

[1] vgl. Wallmüller, Ernest (2004), S.3
[2] vgl. Warncke, Markus (2006), S.48
[3] vgl. Reichmann, Thomas (2006), S.5661-63
[4] vgl. Fassbender, Pantaleon. (2001), S.78
[5] vgl. Wallmüller, Ernest (2004), S.14

Die Diskussion um Corporate Governance führte in den USA zu dem Report des Commitee of Sponsoring Organisations of the Treadway Commission (COSO-Report) und in Deutschland zum Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG).[1]

Im gegebenen Kontext geht es um die Analyse und Bewertung operativer und im Zusammenhang mit der IT-Security stehender strategischer Unternehmensrisiken und darum, welche IT-Werkzeuge, Maßnahmen und Konzepte zur Risikosteuerung eingesetzt werden können.

2.1 Gesetzliche Anforderungsgrundlagen

Es existieren keine regulatorischen Vorgaben, welche Informationssicherheit explizit vorschreiben. Spezielle gesetzliche Sicherheitsanforderungen bezüglich der IT müssen aus den vorhandenen Gesetzen und allgemeineren Normen (z. B. Haftungsnormen oder Verlautbarungen anerkannter Organisationen) abgeleitet werden.

Gesetzlich fixierte Anforderungen an die IT-Sicherheit sollen – zumindest im Zusammenspiel verschiedener Normen untereinander – die vier Einflussbereiche

- technische Sicherheit (d. h. die Eigenschaft der eingesetzten Hard- und Softwaresysteme, absichtliche und unabsichtliche Angriffe auf ihre IT-Sicherheit verlässlich zu erkennen, abzuwehren und nachvollziehbar machen zu können),
- Anwendungssicherheit (d. h. verlässliche Nutzung der Systemkomponenten),
- Organisatorische Sicherheit (d. h. die an Sicherheit orientierte organisatorische Ausgestaltung der Informations- und Datenflüsse in der Organisation) und
- Personelle Sicherheit (d. h., die Fähigkeit und Bereitschaft der beteiligten Personen, entsprechend den Sicherheitsanforderungen zu handeln)

berücksichtigen. IT-sicherheitsbezogene ordnungsrechtliche Verhaltenspflichten werden unterteilt in:

- Vorsorgepflichten (Überwachung und Sicherung von Anlagen),
- Organisationspflichten zur Eigensicherung (Bestellung eines Sicherheitsbeauftragten, Erarbeitung eines Sicherheitskonzepts) und
- überwachungserleichternde Pflichten (Auskunfts-, Mitteilungs-, sonstige Mitwirkungspflichten).

Zur Einbindung von technischen Sicherheitsstandards (welche die materiell rechtlichen Anforderungen umschreiben und praktisch handhabbar machen, die zum Schutz der IT-Sicherheit eingehalten werden müssen) in die Gesetze macht der Gesetzgeber abstrakte Vor-

[1] vgl. Wallmüller, Ernest (2004), S.14

gaben in Form der unbestimmten Rechtsbegriffe „allgemein anerkannte Regeln der Technik“, „Stand der Technik“ oder „Stand von Technik und Wissenschaft“.[1] So wird etwa im Geräte- und Produktsicherheitsgesetz: (GPSG) § 14 Abs. 2 bestimmt, dass „Ausschüsse die Bundesregierung oder das zuständige Bundesministerium in technischen Fragen beraten sollen. Sie schlagen dem Stand der Technik entsprechende Regeln (technische Regeln) unter Berücksichtigung der für andere Schutzziele vorhandenen Regeln … vor“. Mit dem GPSG wird das präventive Ziel verfolgt, dass der Verbraucher nur „sichere“ Produkte zur privaten Nutzung erhält. Eine Ausweitung der dem Gesetz zugrunde liegenden EU-Produktsicherheitsrichtlinie ist möglich auf Produkte, die im Rahmen von Dienstleistungen verwendet werden. Das GPSG verpflichtet den Hersteller über den ganzen Lebenszyklus des Produkts hinweg zur Information des Verbrauchers über mögliche vom Produkt ausgehende Gefahren, geeignete Schutzmaßnahmen sowie für bereits in Verkehr gebrachte Produkte zu Maßnahmen, um mögliche Gefahren zu erkennen und abzuwehren. Zu den europäischen Rechtsvorschriften für spezielle Produktgruppen zählen u. a. die Niederspannungsrichtlinie und die Maschinenrichtlinie, welche durch das GPSG und die zugehörigen Verordnungen ins deutsche Recht umgesetzt wurden.[2]

Die gesetzlichen Mindeststandards für die IT-Security sind zwar insgesamt unpräzise definiert, aus Spezialvorschriften (z. B. § 9 BDSG) ergibt sich dennoch ein von Unternehmen zu beachtendes Mindestniveau an Sicherheitsvorschriften. Für Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste gilt mit der EU-Datenschutzrichtlinie für elektronische Kommunikation eine explizite Regelung für die Ausgestaltung der IT-Sicherheit: Nach Art. 4 Abs. 1 sind unter Berücksichtigung des Stands der Technik technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit der Dienste zu gewährleisten. Diese Maßnahmen müssen den bestehenden Risiken „angemessen“ sein. Wenn ein besonderes Risiko der Verletzung der Netzsicherheit besteht, muss der Betreiber die Teilnehmer über dieses Risiko und - wenn das Risiko nicht vom Dienstleister mit entsprechenden. Maßnahmen abgesichert werden muss – über mögliche Abhilfen einschließlich der dafür voraussichtlich entstehenden Kosten, informieren.[3]

Das deutsche KonTraG und internationale Regelungen wie Basel II oder der amerikanische Sarbanes-Oxley-Act (SOX) sollen für mehr Transparenz in den Unternehmen sorgen und fordern ein aktives Risikomanagement. Es geht um die Wiedererlangung des öffentlichen Vertrauens in Kapitalmarktinformationen. Es wird massiv nach besseren internen Kontroll-

[1] vgl. Holznagel Bernd (2003): S.35,36
[2] vgl. Dahmen, Jörn (2002), S.13-14
[3] vgl. Coester, Ursula/Hein, Matthias (2005), S.94,95

systemen (IKS) verlangt, wie sie nur mit Unterstützung der Informationstechnologie erreicht werden.[1] Zentrale Aufgabe bezogen auf die IT ist der Aufbau, die Überwachung und Steuerung transparenter IT-Strukturen für definierte und kontrollierte Prozesse (ein Enterprise Change und Configuration Management) zur Gewährleistung eines wirksamen IKS.[2] Ein angemessenes und wirksames IT-Kontrollsystem soll die Umsetzung der IT-Strategie überwachen.[3] Verlangt wird auch die Revisionssicherheit der fachlichen Prozesse (Nachweis der Qualität der Prozessabwicklung). Sämtliche IT-Prozesse müssen nachvollziehbar sein.

Die gesetzlichen Mindeststandards sind für Unternehmen zur Risikoprävention aber in keinem Fall ausreichend. IT-Security ist im Kern ein unternehmerisches bzw. technisch-organisatorisches Problem. Gesetzliche Grundlagen, die explizit Maßnahmen zur Sicherung von IT-Systemen fordern, verfügen insgesamt über wenig Detailtiefe. Sie müssen in eigenen Sicherheitsprozessen und -richtlinien spezifiziert werden. Dabei kann man sich an existierenden IT-Sicherheitsstandards orientieren, mit deren Hilfe sich ein entsprechendes Sicherheitsmanagement-System sowie detaillierte Sicherheitsrichtlinien entwickeln lassen. Für die IT-Systeme werden so Sicherheitsrichtlinien mit konkreten Umsetzungsvorgaben entwickelt mit dem Ziel, einen vorab in einer Schutzbedarfsanalyse festgestellten Schutzbedarf zu erreichen. Rechtliche Maßnahmen müssen die technischen und organisatorischen Maßnahmen zur Risikominimierung zwingend unterstützen. Denn das beste technische und organisatorische Konzept nützt nichts, wenn nicht die Mitarbeiter und Externe vertraglich zur Einhaltung verpflichtet sind.[4]

Als technisches und organisatorisches Konzept wird etwa ein ISMS-Rahmenwerk zum Management der IT-Sicherheit als stetiger, sich immer wieder neu definierender Prozess geschaffen. So im Rahmen des PDCA-Zyklus der ISO 27001, mit der sich als Ergebnis der Verbesserungsphase eine erweiterte bzw. entsprechend ergänzte Fassung der Sicherheitsvorgaben ergeben kann. Die Beurteilung der Einhaltung der gesetzlichen Regelungen sowie der Angemessenheit der umgesetzten Maßnahmen erfolgt extern durch speziell dafür ausgebildete Wirtschaftsprüfer und intern durch die IT-Revision bzw. IT-Sicherheitsbeauftragte.[5]

[1] vgl. Rentschler, Peter (2005a)
[2] vgl. Stahl, Christoph (2005)
[3] vgl. IDW (2002a): RS FAIT 1,78
[4] vgl. Schröder, Georg F. (2006), S.16,17
[5] vgl. Hirch, Axel/Rahmel, Jürgen (2005), S.10-11

Zum Umfeld der rechtlichen Problematik gehören auch die steuerlichen Aspekte des Unternehmens, insbesondere umsatzsteuerliche Fragen oder z. B. die steuerliche Belastung des privaten Internetgebrauchs während der Arbeitszeit im Unternehmen.[1]

Insbesondere KonTraG und Basel II muss in der Praxis durch die Implementierung eines (operativen) "(IT-)Risikomanagements" konkretisiert werden. Die gesetzlichen Vorschriften zur Informationspflicht gegenüber Anteilseignern bezüglich Risiken im Unternehmen schließt die Informationstechnik mit ein. Gesetzen wie KonTraG und SOX kann diesbezüglich nur entsprochen werden, wenn ein angemessener IT-Sicherheitsprozess mit Schnittpunkten zu den Risikomanagementprozessen im Tagesgeschäft des Unternehmens verankert ist.[2]

2.1.1 KonTraG

Ziel der Corporate Governance ist eine gute, vertrauensvolle, auf langfristige Wertschöpfung ausgerichtete Unternehmensführung und Kontrolle. Im Fokus steht insbesondere der sorgfältige Umgang mit Risiken, von der Erkennung bis zur Bewältigung.[3] Viele Elemente der Corporate Governance waren in Deutschland jedoch auch vor KonTraG bereits gesetzlich kodifiziert. In unterschiedlichen Gesetzen des Handels- und Gesellschaftsrechts sowie des Kapitalmarktrechts finden sich rechtliche Parameter. Nach § 317 Abs. 4 HGB z. B. muss auch der Geschäftsführer einer GmbH auf die in § 91 Abs. 2 AktG beschriebenen Maßnahmen zur Risikoüberwachung hinwirken.

Bereits vor dem Inkrafttreten des KonTraG gehörte es zu den Aufgaben des Vorstands (vgl. § 76 Abs. 1 AktG (allgemeine Leitungsaufgabe des Vorstands)), für die Einrichtung eines Kontroll- und Risikomanagement-Systems zu sorgen und Entwicklungen, die den Fortbestand der Gesellschaft gefährden könnten, zu erkennen sowie die entsprechenden organisatorischen Maßnahmen zu treffen.[4] Das Gebot, ein Risikofrüherkennungs- und Überwachungssystem zu unterhalten, ist Teil der umfassenden Sorgfaltspflicht einer jeden Geschäftsführung, sodass das KonTraG eigentlich nur die allgemeine Sorgfaltspflicht der §§ 93 AktG, 43 GmbhG, 34 GenG näher konkretisiert.[5]

[1] vgl. Kirchner, Michael (2002), S.100,101
[2] vgl. Rieger, Holger/Schoolmann Jürgen (2005), S.438
[3] Romeike, Frank (2004), S.72
[4] vgl. Romeike, Frank (2004), S.69
[5] vgl. Diederichs, Marc (2004), S.31

Das KonTraG verfolgt zwei Ziele: Zum einen die „Verminderung von unternehmerischen Risiken“ und Stärkung der Kontrollsysteme in den Unternehmen. Zum anderen sollen Transparenz und Information gegenüber Anlegern, Anteilseignern und der Öffentlichkeit verbessert werden.[1] Das Ziel, mehr Transparenz im Unternehmen zu erreichen, ist schon aus dem Namen des Gesetzes ableitbar. Qualitativ hochwertige Informationen und vor allem ein schneller, sicherer Informationsfluss sind notwendige Voraussetzung der Risikoüberwachung und -steuerung. Nur dann haben die Verantwortlichen einen Zeitgewinn, um Maßnahmen zur Risikobekämpfung einzuleiten.[2]

Das KonTraG trifft Festlegungen für börsennotierte Aktiengesellschaften, Kapitalgesellschaften bzw. Unternehmen, die den Vorschriften für Kapitalgesellschaften unterliegen, und Gesellschaften mit einem Aufsichtsrat. Das KonTraG verpflichtet nun noch stärker zur Durchführung eines angemessenen Risikomanagements und im Falle einer börsennotierten Gesellschaft, künftig zu erwartende Risiken im Lagebericht zu dokumentieren. Nicht nur für Dokumentation und Berichterstattung sind dabei IT-Systeme zur Unterstützung notwendig, die auch eine entsprechende Datensicherheit gewährleisten müssen.

Die gesetzliche Verpflichtung zur Einrichtung eines Überwachungssystems zur Risikofrüherkennung wurde direkt zwar nur ins Aktiengesetz aufgenommen. Obwohl das GmbH-Gesetz nicht in analoger Weise erweitert wurde[3], wird allgemein jedoch von einer Ausstrahlungswirkung vor allem auf alle Unternehmen ausgegangen, die die Größenkriterien gemäß § 5 Abs. 2 Publizitätsgesetz (PublG) erfüllen und deren Belange deshalb von öffentlichem Interesse sind.[4]

Die Verpflichtung gemäß § 91 Abs. 2 AktG ist im Sinne von § 290 HGB bei Mutterunternehmen konzernweit zu verstehen, bei einer strategischen Holding als AG mit operativen Tochtergesellschaften einer beliebigen Rechtsform schlägt die Anwendung auf die Tochtergesellschaft durch.[5] Zusätzlich kann das KonTraG auch Offene Handelsgesellschaften (OHG) und Kommanditgesellschaften (KG) betreffen, die keine natürliche Person als persönlich haftenden Gesellschafter haben, denn dadurch sind sie nach dem Kapitalgesellschaften- und Co-Richtliniengesetz (KapCoRiLiG) mit Kapitalgesellschaften gleichzusetzen: Hauptzweck des KapCoRiLiG ist es, Personengesellschaften, bei denen nicht wenigstens eine natürliche Person unmittelbar oder mittelbar (über eine andere Personengesellschaft) als persönlich

[1] vgl. Reichling, Peter (2003), S.92
[2] vgl. Kirchner, Michael (2002), S.71
[3] vgl. Hölscher, Reinhold (2002), S.94
[4] vgl. Ibers, Tobias (2005), S.19
[5] vgl. Diederichs, Marc (2004), S.33

haftender Gesellschafter beteiligt ist, den strengeren Pflichten zur Erstellung, Prüfung und Offenlegung der Jahresabschüsse der Kapitalgesellschaften zu unterwerfen. Nach herrschender Meinung und Auffassung des IDW ist dies auf den Anwendungsbereich des KonTraG zu übertragen.

Der Gesetzgeber fordert im Rahmen von KonTraG ein Risikomanagement-System, internes Überwachungssystem, Controlling und Frühwarnsystem. Jedoch wird keine Auskunft darüber gegeben, wie die geforderten Elemente konkret zu gestalten oder welche Mindest-anforderungen einzuhalten sind. Maßgeblich dafür sind betriebswirtschaftliche Aspekte und das Gebot der Zweckmäßigkeit.[1]

Das Risikomanagement gemäß KonTraG muss nicht nur die Sicherheit der IT-Infrastruktur im Allgemeinen, sondern auch die der eingesetzten Anwendungen berücksichtigen. Um der Sorgfaltspflicht hier zu entsprechen, sind für „kritische Entwicklungen“ adäquate Früherkennungs- und Steuerungssysteme zu implementieren. Eine solche kritische Entwicklung kann bereits durch das Auftreten von Sicherheitslücken unmittelbar eingeleitet werden.[2] Im Rahmen der Risikominimierung ergibt sich die Verpflichtung, Maßnahmen auch zum Schutz gegen IT-Sicherheitsrisiken zu ergreifen. Art und Umfang dieser Maßnahmen sind jedoch völlig unpräzise.

Das KonTraG führte aber zu einer Ausweitung des IKS auf alle Geschäftsbereiche, denen Risiken inhärent sein können.[3] Außerdem soll die Revision mit einem eher problem-orientierten und stärker prospektiv ausgerichteten, Risiko-orientierten Prüfungsansatz vor allem Risiken der zukünftigen Entwicklung transparent machen.[4] Bei Darstellungen zur zukünftigen Lage eines Unternehmens und den damit einhergehenden Risiken handelt es sich aber um prognostizierte Einschätzungen mit meist subjektivem Charakter. Insbesondere wird es u. a. schwierig sein, die den Prognosen zugrunde liegenden Annahmen und Wirkungs-zusammenhänge darzustellen.[5]

Die Regelungen, Vorschriften und Bestimmungen im Bereich der Erarbeitung und Gestaltung eines umfassenden ganzheitlichen Risikomanagements gewähren der Praxis deshalb einen

[1] vgl. Reichling, Peter (2003), S.93
[2] vgl. Coester, Ursula/Hein, Matthias (2005), S.88,89
[3] vgl. Lentfer,Thies (2003), S.14
[4] vgl. Diederichs, Marc (2004), S..40
[5] vgl. Diederichs, Marc (2004), S..55

größtmöglichen Freiraum bei der Umsetzung.[1] Der Gesetzgeber vertraut auf die Selbstorganisation der Unternehmen, die so eine höhere Flexibilität erreichen.[2]

Bei der der Erarbeitung und Gestaltung eines umfassenden ganzheitlichen Risikomanagements lassen sich Konzepte des betriebswirtschaftlichen Risikomanagements auf die gesetzlichen Anforderungen zum Risikomanagement übertragen:[3]

- Phasenkonzepte des Entscheidungs- und Risikomanagementprozesses,
- Methoden aus Planung und Controlling (z. B. Balanced Scorecard, Benchmarking, Planungsrechnungen) oder spezifischen Anwendungsbereichen (z. B. Bonitätsprüfung),
- im Rahmen der betriebswirtschaftlichen Planung entwickelte Konzepte (z. B. schwache Signale) und Systeme (z. B. Frühaufklärungssysteme).

Das betriebswirtschaftliche Risikomanagement hinterfragt jedoch auch Planungsmentalitäten und Erwartungsbildungen, um zu einer besseren Einschätzung der Risiken zu gelangen. Das gesetzliche Risikomanagement berücksichtigt diesen Aspekt nicht, insofern legt der IDW PS 340 die Prüfung des gesetzlichen Risikomanagements als Systemprüfung und nicht als Geschäftsführungsprüfung fest.

2.1.2 Sarbanes-Oxley-Act

Gesetze wie der US-amerikanische Sarbanes-Oxley-Act (SOX) oder Gramm-Leach-Billey-Act (GLIB) dienen der Vertraulichkeit und Verlässlichkeit finanzieller Unternehmensdaten und somit auch dem Anlegerschutz. Die Verbesserung des Anlegerschutzes soll mit detaillierten und zuverlässigeren Publizitätspflichten etabliert werden. Im Rahmen einer „angemessenen Unternehmensführung“ sollen nach SOX die Verlässlichkeit des Jahresabschlusses und die Offenlegung essenzieller Informationen durch die Schaffung interner Organisationsstrukturen sichergestellt werden. Der Aufbau dieser Strukturen muss „eine Dokumentation aller relevanten Prozesse, eine Benennung der damit verbundenen Risiken sowie die Festlegung und Überwachung der Maßnahmen zur Risikobegrenzung“ ermöglichen.[4] Die Verbesserung der Corporate Governance sowie die Abkehr von der Selbstregulierung der Wirtschaftsprüfer stehen im Mittelpunkt des Gesetzes. Neben dem Schutz der Anleger durch genauere und verlässlichere Publizitätspflichten verlangt SOX nach innen

[1] vgl. Diederichs, Marc (2004), S..58
[2] vgl. Wolf, Klaus (2003a), S.24
[3] vgl. Wall, Friederike (2003)
[4] vgl. Coester, Ursula/Hein, Matthias (2005), S.91

„eine Qualitätssicherung der Unternehmensführung und die Transparenz der Unternehmensprozesse“.[1]

Obwohl der SOX nicht direkt für deutsche Unternehmen gilt, ist zu erwarten, dass viele der Anforderungen des SOX in europäisches Recht einfließen und auch in der deutschen Rechtsprechung zukünftig berücksichtigt werden.

SOX verlangt in Section 302 Kontrollen und Verfahren für korrekte Veröffentlichungen der Finanzdaten. Dies erfordert korrekte Erfassung und Verarbeitung aller relevanten Informationen im Unternehmen. Es muss durch entsprechend ausgeprägte Maßnahmen verhindert werden, dass mangelhafte Kontrollen und dadurch bedingte falsche bzw. unvollständige Informationen die Finanzdaten verfälschen. Dieser Ansatz korrespondiert mit KonTraG und den entsprechend angepassten §§ 317 ff. HGB.[2] In SOX Section 404 werden für das Management weiterreichende Konsequenzen festgelegt. Das Management hat die Wirksamkeit des IKS jährlich zu bewerten und muss dies mit Beweismaterial und einer Dokumentation nachweisen können. Im Gegensatz zu anderen Regelwerken ist im SOX die persönliche Haftung der Verantwortlichkeiten eindeutig definiert, sodass Schadensersatzforderungen relativ problemlos durchsetzbar sind.[3] Section 406 fordert vom Vorstand und leitenden Angestellten die Einhaltung eines „code of ethics“, in dem „ehrliches“ Vorgehen und die korrekte Berichterstattung an die Securities and Exchange Commission (SEC) gefordert wird. Section 302 verpflichtet Chief Executive Officer (CEO) und Chief Financial Officer (CFO), eine eidesstattliche Erklärung für periodisch bei der SEC eingereichte Berichte abzugeben.

Anforderungen zur Auslegung von SOX wurden vom Public Company Oversight Board (PCAOB) verbindlich detaillierter festgelegt. Zum Aufbau des IKS wird das COSO-Modell empfohlen. Ein Schwerpunkt dieses Ansatzes ist die Risikobeurteilung. In § 75 des PCAOB Audit Standards No.2 wird die Rolle der Informationssicherheit gewürdigt. Neben den finanztechnischen Ergebnissen der IT rücken nun auch die Prozesse der IT selbst in den Mittelpunkt des Prüfungsgegenstands.[4] Für die Authentifikation, Zugriffskontrolle und das Benutzermanagement empfiehlt das IT Governance Institute die Control Objectives for Information and related Technology (CObIT). Dieser Standard nimmt eine ganzheitliche Sicht auf die IT ein, d. h. berücksichtigt alle Aspekte des IT-Einsatzes von der Planung bis zum Betrieb. Er unterstützt das Management und insbesondere die Interne Revision bei der Wahrnehmung ihrer Verantwortung „bei der Erreichung der Geschäftsziele, die Kontrolle der dabei ver-

[1] Peemöller, Volker H. (2006), S.115
[2] vgl. Schreiber, Ottokar (2006), S.6-7
[3] vgl. Coester, Ursula/Hein, Matthias (2005):, S.92
[4] vgl. Rentschler, Peter (2005a)

wendeten Ressourcen hinsichtlich Effektivität und Effizienz, die Einhaltung rechtlicher Rahmenbedingungen sowie die Handhabung der mit der Geschäftstätigkeit und dem Ressourceneinsatz verbundenen Risiken (z. B. Sicherheitsrisiken)“ im Zusammenhang mit „der IT als Ressource zur Realisierung von Geschäftsprozessen“. Die Revisionssicht auf die IT beinhaltet den Aspekt der „Einheitlichen Grundlage für die Wertung der internen Kontrollen“. Damit werden die Ziele der IT-Governance im Unternehmen (Ausrichtung der IT auf die Geschäftstätigkeit (Nutzenmaximierung), wirtschaftlicher Einsatz von IT-Ressourcen (Daten, Anwendungen, Technologien, Anlagen, Personal) und angemessenes Risikomanagement IT-bezogener Risiken) unterstützt.[1]

Bezüglich der Umsetzung ist das Rahmenwerk technikneutral formuliert, beim Einsatz von IT werden keine Vorgaben gemacht bezüglich spezifischer IT-Kontrollsysteme.[2]

2.1.3 Basel II (EU-Eigenkapitalrichtlinie (Capital Requirements Directive))

Prinzipielles Ziel von Basel II ist es, die Stabilität im Kreditwesen zu erhöhen. Um dies zu erreichen, ist die Unterlegung von Krediten mit Eigenkapital durch Kreditinstitute neu geregelt worden. Die Hinterlegung mit Eigenkapital bei den Kreditinstituten berücksichtigt nun die Risiken des einzelnen Kreditengagements. Die Höhe des zur Absicherung von Krediten einzusetzenden Eigenkapitals hängt nun wesentlich stärker von der Bonität und den Zukunftsaussichten des Kreditnehmers ab. Es werden auch „weiche Faktoren“ wie Strategie, Marktkenntnisse, Managementqualität, Sicherheit der Planung, wie auf Abweichungen reagiert wird, Geschäftsprozesse und vieles mehr überprüft und bewertet, denn alle unternehmerischen Entscheidungen wirken sich über kurz oder lang auf die Zahlen des Jahresabschlusses aus. Die Banken wollen Chancen und Risiken der Unternehmen im Voraus erkennen und bewerten.

Rating-Fragen zum Risikomanagement sind etwa: [3]

- Sind die Ziele für das Risikomanagement definiert?
- Verfügt das Unternehmen über eine (marktorientierte) Unternehmensstrategie?
- Existieren eine Risikostrategie bzw. risikopolitische Grundsätze?
- Ist die Risikostrategie bzw. sind die risikopolitischen Grundsätze aus der Unternehmensstrategie abgeleitet?
- Sind die Systemelemente des Risikomanagements exakt beschrieben?
- Ist ein einheitliches Risikomanagement im Unternehmen umgesetzt?

[1] BITKOM (2005), S.13,14
[2] vgl. Coester, Ursula/Hein, Matthias (2005):, S.92
[3] vgl. Seidel, Uwe M. (2002):,S.118

- Beseht in allen Unternehmensbereichen ein Risikomanagementverständnis/-bewusstsein?
- Können Unternehmensphilosophie und Führungsstil als Risiko-bewusst eingestuft werden?

Die Überprüfung der qualitativen Kriterien stellt einen Frühwarnindikator dar, mit dessen Hilfe Gefahrenpotenziale erkannt werden sollen.[1] So sind die Kosten bzw. Zinsen für einen Kredit je nach Risiko eines Zahlungsausfalls unterschiedlich hoch. Zur Ermittlung und Bewertung von Risiken wird dabei auf sog. Ratings[2] zurückgegriffen. Für den Zinssatz ist nicht mehr nur die Bonität aufgrund des letzten Jahresabschlusses ausschlaggebend, sondern die individuelle Beurteilung des Kreditrisikos nach einem standardisierten System (Rating). Demnach haben Firmen mit einem schlechten Rating höhere, Firmen mit einem guten Rating geringere Zinskosten. Bei der Konzeption dieses Ratingverfahrens fanden alle Faktoren für eine umfassende Überprüfung der Zukunftsfähigkeit des Unternehmens Berücksichtigung. Dies sind neben den finanziellen und geschäftlichen Risiken auch operationelle Risiken. Im Rahmen operationeller Risiken soll die Gefahr möglicher Schäden in Folge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge externer Ereignisse bewertet werden.[3] Bei der Risikogewichtung der Aktiva wird eine neue Berechnungsmethode angewandt, die auch solche operationellen Risiken berücksichtigt. Die Kreditrisikoquantifizierung ist in drei Varianten möglich: Standardmethode, internes Rating und Kreditrisikomodelle. Bei der Standardmethode wird zur Festlegung von Bonitätsgewichtsklassen auf externe Ratings zurückgegriffen. Beim internen Rating wird im Basisansatz aufgrund der Bonitätseinstufung die Ausfallwahrscheinlichkeit des Kreditnehmers geschätzt. Der Advanced-IRB(Internal Ratings-Based)-Ansatz greift im Gegensatz zum Basis-IRB-Ansatz zur Bestimmung der Eigenkapital-Unterlegungspflicht nicht nur auf die Ausfallwahrscheinlichkeit des Kreditnehmers als bankinterner Schätzung zurück.

Mit den neuen Anforderungen an die Eigenkapitalunterlegung werden sich Kredite mit einem hohen Risiko (beim Kreditnehmer) schon deshalb verteuern, weil sie einer erhöhten Eigenkapitalunterlegung bedürfen. Für die Banken besteht ein Anreiz, solche Geschäfte abzuschließen, die möglichst geringe Eigenkapitalanforderungen besitzen, um sie aus dem vorhandenen Eigenkapital unterlegen zu können.[4] Die aufsichtsrechtlich bestimmte Eigenkapitalunterlegung dient zur Begrenzung der Geschäftsaktivitäten einer Bank. Hat das anrechenbare

[1] vgl. Brezski, Eberhard (2004), S.11,12
[2] Reichling, Peter (2003), S.66-83
[3] vgl. Coester, Ursula/Hein, Matthias (2005), S.90
[4] vgl. Reichling, Peter (2003), S.10

Eigenkapital der Bank ein bestimmtes Verhältnis zu den Risikoaktiva erreicht, so ist es den Banken untersagt, weitere risikobehaftete Geschäfte abzuschließen.[1] Andererseits besteht für die Kreditnehmer die Möglichkeit, Einfluss auf die Kreditkonditionen zu nehmen. Dazu gehören eine umfassende Informationspolitik über die zukünftige Unternehmensentwicklung und eine schlüssige Unternehmensplanung.[2]

Das Rating wird daher zu einer Entscheidungsdeterminante für Unternehmen, da sie durch eigene Entscheidungen, Maßnahmen und Aktivitäten ihren Handlungsspielraum (bezüglich der auf Fremdkapital beruhenden finanziellen Möglichkeiten) aktiv gestalten können.[3]

Bisher erfolgten die Bonitätsprüfungen der Kredit gewährenden Banken nur im Nachhinein und nur aufgrund der letzten Jahresabschlüsse. Zusätzliche Unterlagen wurden kaum angefordert. Doch Basel II steht unter dem Motto: Rückblickende Analyse ist gut, eine umfassende Zukunftsplanung ist besser.[4] Für die Unternehmer kommt es nicht nur darauf an, dass sie sich in ihren Produkten und Dienstleistungen auskennen, sie müssen auch erklären können, wie ihr Unternehmen funktioniert, wie sie kalkulieren und wie sie sich auf veränderte Marktlagen einstellen wollen.[5]

Nach Basel II ist die Kreditvergabe an Unternehmen auch von der Qualität des Risikomanagements und von der Einhaltung bestimmter Kriterien bei der Dokumentation der eingesetzten IT-Systeme und -Verfahren abhängig. Ihre Anstrengungen im Risikomanagement können Unternehmen durch einen Risikobericht dokumentieren, der als Grundlage bei den Verhandlungen über die Kreditkonditionen ausschlaggebend sein kann.

Basel II wird aber zunächst keine Auswirkungen auf die Anforderungskriterien für die IT-Security haben: Ein Unternehmen mit schlechter Auftrags- und Liquiditätslage und bester IT-Security wird nur schwer einen Kredit bekommen. Ein Kreditinstitut hat darüber hinaus gar nicht das notwendige technische Wissen/Know-how, um die Funktionalität und Effizienz der IT-Infrastruktur beurteilen zu können. Ein Kredit für ein florierendes Unternehmen mit bester Liquiditäts- und Auftragslage wird daher nicht an den technischen Anforderungen an die IT-Security scheitern. Etwas differenzierter ist die Sache bei Ratings durch einen externen Dienstleister.[6]

Die Europäische Union (EU) ist mit den derzeitigen EU-Eigenkapitalvorschriften dem Baseler Akkord gefolgt. Mit einer Umsetzung der EU-Richtlinien in nationales Recht erfolgt

[1] vgl. Reichling, Peter (2003), S.65
[2] vgl. Kappeller, Wolfgang (2003), S.17-18
[3] vgl. Brezski, Eberhard (2004), S.13-15
[4] vgl. Foerster, Udo (2002)
[5] vgl. Töpfer, Armin (2003), S.27
[6] vgl. Schröder, Georg F.(2006), S.8-10

eine Rechtsverbindlichkeit für die Gesamtheit der in der Europäischen Union tätigen Kreditinstitute und Wertpapierunternehmen. In Deutschland wurden wesentliche Elemente der EU-Eigenkapitalrichtlinie zur Umsetzung des Basel II-Regelwerks mit den Mindestanforderungen an das Risikomanagement (MaRisk) in die deutsche Aufsichtspraxis eingeführt.

Der zweite Aspekt von Basel II sind die Anforderungen an die Sicherheit und Leistungsfähigkeit und damit an die Qualität der IT-Prozesse bei den Banken selber. So bilden die MaRisk auch den Rahmen für den sog. Supervisory Review and Evaluation Process (SREP), der von der nationalen Aufsicht eine institutsspezifische Beurteilung der Risiko- und Kapitalmanagement-Systeme verlangt.

Die Eigenkapitalunterlegung soll auch stärker vom Risikoprofil bei der Bank selber abhängig gemacht werden, um Anreize für die Entwicklung und Implementierung geeigneter Methoden des Risikomanagements zu machen.[1] Die Optimierung des Risikomanagements/Verbesserung des Managements operationeller Risiken soll mit einer risikosensitiven Kapitalunterlegung umgesetzt werden, um so eine Robustheit des gesamten Finanzsystems zu erreichen. Die Aufsicht begrenzt die Risiken, die die Bank eingehen darf. Durch die Limitierung der operationellen Risiken mithilfe der Kapitalunterlegung wird die Qualität des bankeninternen Risikomanagements zudem zu einem Wettbewerbsfaktor:[2]

In stärkerem Maße als bisher haben die Aufsichtsinstanzen die Aufgabe, die verschiedenen bankinternen Verfahren zu prüfen und zu beurteilen. Damit sollen auch die Risikobereiche abgedeckt werden, die bei der Berechnung der Mindesteigenkapitalanforderungen nicht bzw. nicht vollständig berücksichtigt wurden (z. B. Unsicherheiten bei der Berechnung der operationellen Risiken). Z. B. weist auch die Kreditbearbeitung operationelle Risiken auf. So wird bei bonitätsschwachen Kreditnehmern durch erhöhten Bearbeitungs- und Kontrollaufwand von gestiegenen operationellen Risiken auf Seite der Bank ausgegangen.[3]

Durch Basel II werden die Banken, die sich gegenüber den Aufsichtsbehörden für den Einsatz von modernen, risikoadäquaten Verfahren für die Bewertung des Kredit- und Betriebsrisikos qualifizieren, von der Bankenaufsicht für Investitionen in diese Verfahren mit einer signifikanten Reduzierung der gesetzlich vorgeschriebenen Rückstellungen belohnt (d. h., sie können die Eigenkapitalunterlegung flexibel an der konkreten Risikosituation ausrichten). Dazu haben die Banken gegenüber der Bankenaufsicht nachzuweisen, dass

[1] vgl. Reichling, Peter (2003), S.66
[2] vgl. Romeike, Frank (2005), S.257
[3] vgl. Reichling, Peter (2003), S.95,96

- die Betriebsfähigkeit ihrer Systeme für entsprechende Software-Anwendungen und Verfahren sichergestellt ist,
- sie über geeignete Verfahren zur Qualitätssicherung der Daten verfügen,
- die zugrunde liegenden Prozesse die Datenqualität (Vollständigkeit, Konsistenz und Genauigkeit) sicherstellen.

Im weiteren Verlauf wird dieser Aspekt nicht betrachtet. Es geht im Zusammenhang mit der gegebenen Thematik um die Herleitung eines Vorschlags für ein IT-Risikomanagement/IT-Security-Management, mit dem sich ein positiver Einfluss auf das Rating des Unternehmens durch die Banken ergeben soll. So wie die Unternehmen durch eigene Entscheidungen, Maßnahmen und Aktivitäten ihr Rating positiv beeinflussen, und damit ihren Handlungsspielraum (bezüglich der auf Fremdkapital beruhenden finanziellen Möglichkeiten) aktiv gestalten können, so ist Aufgabe des zu entwickelnden IT-Risikomanagements/IT-Security-Managements die Gestaltung der sicheren und zuverlässigen organisatorisch-technischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume.

2.2 Verlautbarungen//Empfehlungen

Der deutsche Gesetzgeber schreibt nicht vor, wie ein Überwachungssystem im Rahmen des Risikomanagements zu gestalten ist. Vermutlich wollte der Gesetzgeber dies der betriebswirtschaftlichen Theorie und der praxisorientierten Rechtsprechung überlassen. Hier kann auf internationale Verlautbarungen wie den COSO-Report, die Grundsätze Risiko-orientierter Unternehmensüberwachung (GoÜ) und den deutschen Corporate Governance Kodex zurückgegriffen werden.

2.2.1 COSO-Report

Mit den Empfehlungen des Committee of Sponsoring Organisations of the Treadway Commission in den USA (COSO Report 1992) und den Empfehlungen des Cadbury Committee in Großbritannien (Cadbury Report 1992) wurde ein Konzept zur Risikosteuerung und -kontrolle vorgestellt. Sie bilden einen Meilenstein im Bereich der Entwicklung und Be-

urteilung von internen Kontrollsystemen und stellen ein integriertes Rahmenwerk für interne Kontrollen vor.[1]

Der COSO-Report nimmt, wie das deutsche KonTraG Aspekte der Unternehmensüberwachung, insbesondere interner Überwachungssysteme (Internal Control) in den Forderungskatalog für die Unternehmensgestaltung und -berichterstattung auf[2] und stellt als Ziel eines Überwachungssystems die Einhaltung der Regelungen zur finanziellen Berichterstattung sowie der für das Unternehmen geltenden Vorschriften heraus.[3]

Unter Internal Control Structure einer Unternehmung wird dabei die Gesamtheit aller Richtlinien und Maßnahmen verstanden, die für die Erreichung der Unternehmensziele erforderliche Sicherheit sorgen sollen. Gemäß den COSO-Empfehlungen basiert "Internal Control" auf fünf miteinander verknüpften Komponenten: Steuerungsumfeld, Risikoabschätzung, Kontrollaktivitäten, Information und Kommunikation sowie Überwachung. Der Risikomanagement-Ansatz des COSO war die erste umfassende und integrierte Methode, die neben allen Geschäftsprozessen und den Unternehmenszielen einen proaktiven Risikoanalyse und Risikosteuerungsprozess berücksichtigte. Proaktiv bedeutet, Zielabweichungen nicht erst nach ihrem Eintritt zu identifizieren, zu analysieren und zu korrigieren. Risk Management soll sich nur auf die Risikoabwälzung durch Versicherungsschutz und die Erfüllung formaler Anforderungen beschränken. Ziel darf nicht sein, die Vergangenheit zu erklären, sondern zukünftige Chancen und Risiken zu antizipieren.[4]

Eine Erweiterung des COSO I-Rahmenwerks stellt Enterprise Risk Management Framework 2004 (ERM) COSO II dar. ERM zielt neben dem Konzept des Internen Kontrollsystems auf das des unternehmensweiten Risikomanagements ab, welches neben der Früherkennung zusätzlich die aktive Steuerung und Bewältigung von Risiken enthält: Nach diesem Konzept setzt sich der Enterprise Risk Management Prozess aus acht interdependenten Elementen zusammen: [5] [6]

- Internal Environment (Basis zur Definition von Risikophilosophie, Risikobereitschaft und Risikokultur durch das Management)
- Objektive Setting (Formulierung von Zielen zur Risikoidentifikation, -bewertung und -steuerung)
- Event Identification (Identifizierung von Ereignissen, die Auswirkungen auf das Unternehmen haben können)

[1] vgl. Allenspach, Marco (2001), S.92
[2] vgl. Wallmüller, Ernest (2004), S.14
[3] vgl. Lentfer,Thies (2003), S.12
[4] vgl. Romeike, Frank (2004), S.65,66
[5] vgl. Peemöller, Volker H. (2005), S.67,68
[6] vgl. Schroff, Joachim (2006), S.10-27

- „Risk Assessment“ (Risikobewertung) (Ermittlung von Möglichkeiten zum Management der Risiken, um eine Gefährdung der Unternehmensziele zu vermeiden)
- Risk Response (Festlegung von Maßnahmen zur Risikosteuerung)
- Control Activities (Aktivitäten, um die vom Management vorgesehenen Risikosteuerungsmaßnahmen zur Unternehmenszielerreichung umzusetzen)
- Information and Communication (Identifizierung, Aufbereitung und Vermittlung der für das Unternehmen relevanten Informationen)
- Monitoring (laufende Überwachung und Beurteilung der Risikomanagementprozesse, um ihre Qualität im Zeitablauf sicherzustellen)

Zur Schaffung und Etablierung ähnlicher Standards vergleichbar COSO II oder auch der australisch-neuseeländischen Norm „Riskmanagement“ wurde in Deutschland der Verein Risk Management Association (RMA) gegründet.[1]

2.2.2 Grundsätze Risiko-orientierter Unternehmensüberwachung

Die Grundsätze Risiko-orientierter Unternehmensüberwachung (GoÜ)[2] der Schmalenbach-Gesellschaft für Betriebswirtschaft stellen dar, welche Absichten das KonTraG verfolgt, und wie es auszulegen ist: Der neu ins Aktiengesetz eingefügte § 91 hebt die allgemeine Lenkungsaufgabe des Vorstands (§ 76 Abs. 1 AktG) hervor und konkretisiert die Sorgfaltspflicht des Vorstands (§ 93 Abs. 1 Satz 1 AktG). Er tut dies, indem er in die Organisationsverantwortung des Vorstands die Einrichtung eines Risikomanagement-Systems legt. Außerdem wird die Bedeutung der Internen Revision und des Controllings für die innerbetriebliche Überwachung betont.

Die GoÜ stellen klar, dass das Risikomanagement nach KonTraG auf das Risiko im engeren Sinne (reine Verlustgefahr) abstellt und sich auf Überwachung, Diagnose und Steuerung aller reinen wie auch spekulativen Unternehmensrisiken (aller das Unternehmen bedrohenden Verlustgefahren), und damit auf alle Komponenten bzw. Teilbereiche des Gesamtunternehmensrisikos i. e. S., bis hin zur risikobezogenen Unternehmenspolitik bezieht.

Es werden Systemelemente eines Überwachungssystems zur „Begrenzung der mit der Unternehmenstätigkeit verbundenen Risiken“ und Aufgaben und Methoden der einzelnen Phasen des Risikomanagement-Prozesses benannt. Außerdem werden die Aufgaben der Dokumentation des Überwachungs- und des Risikomanagement-Systems und zusammen-

[1] vgl. Giefer, Katrin (2006), S.20
[2] vgl. Kromschröder, Bernhard/Lück, Wolfgang (1998)

fassend die Anforderungen an eine Risiko-orientierte Unternehmensüberwachung beschrieben.

2.2.3 Deutscher Corporate Governance Kodex

Resultierend aus dem Prozess der Globalisierung und der Internationalisierung der Kapitalmärkte wurde mit dem deutschen Corporate Governance Kodex eine Bündelung von Prinzipien und Standards erarbeitet. Er soll ein Code of Best Practice darstellen, „der Fragen der internen Arbeitsweise und Organisation der Unternehmensorgane aufnehmen und Richtlinien im Sinne einer verbesserten Corporate Governance vorgeben, jedoch im Vergleich zu einer Regulierung durch zwingendes Recht größere Flexibilität einräumen soll“.[1] Diesem sollen sich die Unternehmen im Rahmen einer freiwilligen Selbstverpflichtung unterwerfen, und er soll laufend neuen nationalen und internationalen Entwicklungen angepasst werden. Die wichtigsten Funktionen des Deutschen Corporate Governance Kodex sind die Herstellung von Transparenz und die Glaubwürdigkeit unternehmerischen Handelns, die durch offene Begründung von Managemententscheidungen erreicht werden soll.[2] Auf Grundlage dieser Vorschläge wurde das Transparenz- und Publizitätsgesetz erlassen, das die deutschen börsennotierten Unternehmen u. a. verpflichtet, einmal jährlich zu erklären, ob sie die Empfehlungen des Kodex einhalten. Dieser neue Corporate Governance Kodex stellt u. a. höhere Anforderungen an die Risikokontrolle im Unternehmen. Risiken müssen proaktiv erkannt und der Risikomanagementprozess Bestandteil der Unternehmensführung sein.[3]

2.3 Haftungsnormen und -probleme

Das KonTraG sieht vor, dass "der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten hat, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden" (§ 91 Abs. 2 AktG).

Gesetzesverletzungen umfassen die Nichtanwendung von richtigerweise anzuwendenden Normen ebenso wie die fehlerhafte Anwendung von Normen. Grund der fehlerhaften Nichtanwendung wie der fehlerhaften Anwendung kann dabei insbesondere auch die fehlerhafte Auslegung einer Norm sein.[4] Die allgemeinen gesetzlichen Formulierungen bedürfen deshalb

[1] Warncke, Markus (2006), S.51
[2] vgl. Warncke, Markus (2006), S.52
[3] vgl. Romeike, Frank (2004(), S.73
[4] vgl. Arnold, Jörg/Frisch, Wolfgang (2005), S.258

sorgfältiger Interpretationen, um im Zweifelsfall nicht als Unternehmen oder Manager haftbar gemacht zu werden.

Das KonTraG sieht eine persönliche Haftung des Vorstands, des Aufsichtsrats und der Geschäftsführer in Bezug auf ihre Pflicht zur Einrichtung eines Risikomanagement- und Überwachungssystems zur Früherkennung Existenz gefährdender Entwicklungen vor. Nach § 93 Abs. 2 AktG sind Vorstandsmitglieder, die ihre Pflichten verletzen, der Gesellschaft zum Ersatz des daraus entstandenen Schadens als Gesamtschuldner verpflichtet. Besondere Verantwortlichkeitsregelungen gemäß Telemediengesetz (TMG) gelten für Unternehmen, die Internet-Dienste (E-Mail, FTP-Server, Internetzugang) anbieten. Dabei geht es um die Verantwortlichkeit für Veröffentlichung rechtswidriger Inhalte im Internet.[1]

In diesem Zusammenhang ist zu beachten, dass das KonTraG Ausstrahlungswirkung auf den Pflichtenrahmen der Geschäftsführer anderer Gesellschaftsformen hat. Ein angemessenes Risikomanagement ist auch Bestandteil der Sorgfaltspflichten, z. B. eines GmbH Geschäftsführers. Der Verwaltungsrat einer Aktiengesellschaft oder Genossenschaft sowie die Geschäftsführer einer Gesellschaft mit beschränkter Haftung tragen die Verantwortung für Schäden, die aus Unterlassung der Ihnen übertragenen Pflichten oder ungenügender Kontrolle bzw. Oberaufsicht der mit der Geschäftsführung betrauten Personen, entstehen: Sie haften gegenüber der Gesellschaft, ihren Eigentümer sowie den Gesellschaftsgläubigern.

Im Falle einer Unternehmenskrise hat der Vorstand basierend auf § 93 Abs. 2 AktG zu beweisen, dass er sich objektiv und subjektiv pflichtgemäß verhalten hat. Konkret heißt dies, dass er nachweisen muss, Maßnahmen zur Risikofrüherkennung und zur Risikoabwehr getroffen zu haben. Es gilt die sog. Beweislastumkehr, d. h., kann das Vorstandsmitglied im Schadensfall nicht beweisen, dass es seine gesamten Pflichten erfüllt hat, wird quasi automatisch eine Pflichtverletzung angenommen.[2]

Die Umsetzung des § 91 AktG (der den Vorstand zur Einrichtung eines Risikomanagements verpflichtet) wird nach dem Rundschreiben 1/2000 der Bundesanstalt für Finanzdienstleistung der Internen Revision zugeordnet: Diese ist für Kontrolle und „zügige Beseitigung der festgestellten Mängel“ verantwortlich.

Die Revision liefert eine wichtige Informationsquelle für den Verwaltungsrat und Sicherheit für den Aktionär und Investor: Mit der Erfassung und Beschreibung von Schwachpunkten sowie der daraus möglicherweise entstehenden Auswirkungen auf das Unternehmen bietet sie dem Verwaltungsrat eine fundierte strategische Entscheidungsgrundlage.

[1] vgl. Knupfer, Jörg (2005), S.46-48
[2] vgl. Bursch, Daniel (2005), S.14

Delegiert die Unternehmensleitung die Prozess-unabhängige Überwachungsfunktion intern z. B. an eine Abteilung innerhalb des Unternehmens, so nennt man diesen Träger der Überwachungsfunktion „Interne Revision“. Die Interne Revision erbringt objektive und unabhängige Prüfungs- („assurance“) und Beratungsdienstleistungen welche der Verbesserung der Geschäftsprozesse dienen.

Zweckmäßigerweise ist die Interne Revision direkt der Unternehmensleitung zu unterstellen, vom laufenden Arbeitsprozess loszulösen, als von den nachgeordneten Stellen unabhängige und organisatorisch selbstständige Stabsstelle zu etablieren. Im Allgemeinen hat die Interne Revision jedoch auch Prozess abhängige Überwachungsaufgaben. Sie ist deshalb auch Teil des Internen Kontrollsystems.

Grundsätzlich kann sich die Unternehmensleitung mit der Einrichtung der Internen Revision von ihren Überwachungspflichten aber nicht entbinden. Sie hat sich laufend davon zu überzeugen, dass die Interne Revision die ihr zugewiesenen Aufgaben korrekt erfüllt.

Die externe Revision hat im Rahmen der Abschlussprüfung zu berichten, ob das vom Vorstand eingerichtete Überwachungssystem und die Interne Revision für ein effektives Risikomanagement geeignet sind. Außerdem muss der Wirtschaftsprüfer sich ein eigenes Bild von den im Lagebericht dargestellten Risiken machen.[1]

Das unternehmensweite Risikomanagement umfasst auch ein IT-Risikomanagement. Die rechtliche Verantwortlichkeit der Vorstände bzw. Aufsichtsräte zur Gewährleistung der IT-Sicherheit ergibt sich daraus, dass sie dem Unternehmen aufgrund ihres Vertrages und gesetzlicher Regelungen verpflichtet sind, Schaden und erkennbare Risiken abzuwenden.[2]

Die Manager verantworten u. a. [3]

- Wiederherstellungskosten bei Datenverlusten so gering wie möglich zu halten
- Wirtschaftliche Schäden bei Ausfall der EDV auf ein minimales Maß zu begrenzen
- Datendiebstahl und Manipulationen „unmöglich“ zu machen
- Wirtschaftsspionage und Know-how-Verlust zu verhindern

Es ist z. B. abzuwägen, welche IT-Ausfallzeiten tolerierbar sind.

Letztlich trägt jeder einzelne Mitarbeiter aber Mitverantwortung für die IT-Sicherheit. So sind Arbeitnehmer ihrem Arbeitgeber aus ihrem Arbeitsvertrag und gesetzlichen Regelungen heraus verpflichtet, bei ihrer Tätigkeit die größtmögliche Sorgfalt walten zu lassen. Im

[1] vgl. Allenspach, Marco (2001), S.97
[2] vgl. Coester, Ursula/Hein, Matthias (2005), S.78
[3] vgl. Grawe, Tonio (2006), S.15

Rahmen der eingeschränkten Arbeitnehmerhaftung sind sie persönlich schadenersatzpflichtig, wenn sie diese Pflichten vorsätzlich oder grob fahrlässig verletzen und aufgrund dessen dem Unternehmen Schaden entsteht. Leitende Mitarbeiter und in Ausnahmefällen auch Projektleiter und maßgebliche Mitarbeiter der EDV-Abteilungen können bei Pflichtverletzungen und kausalem Schadenseintritt sogar grundsätzlich persönlich haftbar gemacht werden.[1]

Damit hängt die Frage zusammen, inwieweit Unternehmen und ihre Vorstände für das Verhalten ihrer Mitarbeiter zur Verantwortung gezogen werden können. Hierzu wurden in der Rechtsprechung und im Schrifttum Grundsätze der Wissens- und Kenntniszurechnung entwickelt. Hiernach kommt bei Kenntnis von rechtswidrigen Handlungen durch Mitarbeiter des Unternehmens auch eine Verantwortlichkeit des (übergeordneten) Unternehmens bzw. der sie vertretenden natürlichen Personen in Betracht.[2]

Nach deutscher arbeitsrechtlicher Rechtsprechung unterliegen Mitarbeiter im Anstellungsverhältnis einer sog. Haftungsprivilegierung, sind bei Vorsatz oder grober Fahrlässigkeit für den durch sie entstandenen Gesamtschaden im Grundsatz voll regresspflichtig. Die ursprünglich auf einzelne Fallgruppen beschränkte Annahme gefahrengeneigter Arbeit wurde nach aktueller arbeitsgerichtlicher Rechtsprechung auf sämtliche Arbeitsverhältnisse ausgeweitet.[3] Bei der Festsetzung der Entschädigungssumme berücksichtigen die Gerichte die Dauer der Betriebszugehörigkeit, das bisherige Verhalten am Arbeitsplatz, die Position im Unternehmen, den vorauszusetzenden Wissensstand und das Gehalt. Arbeitnehmer (auch IT-Leiter) können dieser Regresspflicht dadurch vorbeugen, dass sie die Geschäftsleitung über mögliche Risiken, die zu einem Schaden führen könnten, informieren und Lösungsvorschläge aufzeigen. - In der betriebswirtschaftlichen Praxis empfiehlt sich folgendes Vorgehen: Werden die Vorschläge abgelehnt, so sollten das eigene Vorgehen und die Haltung der Unternehmensleitung beweiskräftig dokumentiert werden. Wird ein IT-Projekt bewilligt, so sollte der IT-Leiter die Geschäftsleitung regelmäßig über die Entwicklung des Projekts informieren und sich gegebenenfalls externe Unterstützung sichern, z. B., indem er qualifizierte Berater hinzuzieht. Vor dem Hintergrund einer unliebsamen rechtlichen Inanspruchnahme ist es für die IT-Verantwortlichen auch ratsam, die gesamte Infrastruktur auf potenzielle Risiken prüfen zu lassen. - Vorstände von AGs oder Geschäftsführer von GmbHs gelten als Organe des Unternehmens, und nicht als Beschäftigte. Sie können ihre Verantwortung auch im Bereich von zentralen Aufgaben der IT nicht delegieren. So haftet die Geschäftsleitung für Fehler und Versäumnisse ihrer IT-Mitarbeiter, wenn sie bei der Erfüllung ihrer Pflichten nicht die „Sorgfalt eines ordentlichen Geschäftsmanns“ walten lässt. Um das Haftungsrisiko zu minimieren,

[1] vgl. Coester, Ursula/Hein, Matthias (2005), S.79
[2] vgl. Knupfer, Jörg (2005), S.48-50
[3] vgl. Schröder, Georg F. (2006), S.13-15

können bei GmbHs die Gesellschafter den Geschäftsführer entlasten und im Geschäftsführungsvertrag eine Haftungsbeschränkung für fahrlässiges Verhalten vereinbaren. Im Gegensatz zu Aktiengesellschaften (bei denen die Entlastung des Vorstands eben nicht zum Verzicht auf Schadensersatzansprüche führt), erlöschen in diesem Fall die bestehenden Schadenersatzansprüche.[1]

Geschäftsbeziehungen zu Kunden und Partnern müssen zunehmend über unterschiedliche Kommunikationskanäle ermöglicht werden. Dabei sind vielfältige Einsatzszenarien möglich, z. B. Integration von Geschäftsprozessen des Außendiensts durch Online-Zugriff auf das Kunden-/Vertriebsauskunftssystem oder Bereitstellung elektronischer Dienstleistungen für Vertriebspartner und deren Geschäftsprozesse. Ein Konzept, das die Einhaltung von Service-Level-Agreements bei Integration der Geschäftsprozesse von Unternehmen mit denen ihrer Kunden und Partner unterstützen soll, ist die Secure Federation.[2] Es handelt sich dabei um ein auf Identitätsföderation basierendes Geschäftsmodell, wobei verschiedene IT-Dienstleistungen wie Single Sign-on/Prozesse im Zusammenhang mit Benutzerkonten über die Unternehmensgrenzen hinweg von Geschäftspartnern gemeinsam genutzt werden.[3]

Die weitaus größte Gefährdung der IT-Sicherheit geht aus organisatorischen Schwächen hervor. Dabei können auch illegale Handlungen der Mitarbeiter (z. B. Raubkopien von Software, illegale Downloads) zur Mitverantwortung der Geschäftsleitung führen.

IT-Security-Maßnahmen dürfen aber nicht so weit gehen, dass sie Rechte von Mitarbeitern des Unternehmens verletzen:[4] Als rechtlich kritisch gilt z. B. das Ausfiltern von Werbe-E-Mail (Spam) an die Mitarbeiter. Die Revision muss darauf achten, dass das Ausfiltern von Spam durch eine Betriebsvereinbarung oder Einzelvereinbarungen abgesichert ist, und somit das Fernmeldegeheimnis der Mitarbeiter nicht verletzt wird. Die Rechtssicherheit der elektronischen Kommunikation mit Kommunikationspartnern wie Kunden oder Lieferanten ist durch entsprechende Signaturmaßnahmen zu gewährleisten.[5]

Da viele Unternehmen nicht über das Know-how und IT-Sicherheitsexperten verfügen, um eine effiziente Sicherheitsinfrastruktur selbst zu implementieren und permanent zu managen, wird die Überwachung der IT-Sicherheit zunehmend an Managed Security Services Anbieter ausgelagert.[6] Die Verantwortung für die Sicherheit der Daten und das Risikomanagement

[1] vgl. Dahmer, Ralf (2006)
[2] vgl. Chanliau, Marc (2004)
[3] vgl. Bascurov, Oleg (2005)
[4] vgl. Schröder, Georg F. (2006)), S.18-54
[5] vgl. Geis, Ivo. (2005)
[6] vgl. Klaftenegger, Peter (2004)

verbleibt aber beim Unternehmen selber. Insofern ist der Outsourcing-Partner in das eigene interne Kontrollsystem einzubinden.[1]

Im Zusammenhang mit der zivilrechtlichen Haftung, z. B. für fehlerhafte Produkte[2], aber auch für Leistungen von z. B. Managed Security Services Anbietern, unterscheidet man eine vertragliche Haftung

- für Folgeschäden nach §§ 459 ff. BGB (Fehlen zugesicherter Eigenschaften, Gewährleistungshaftung bei Mängeln oder schuldhafte positive Vertragsverletzung (Verletzung von Vertragspflichten oder nebenvertraglicher Sorgfaltspflichten)). Dabei liegt die Beweislast bei positiver Vertragsverletzung beim Leistungserbringer, d. h., er muss beweisen, dass er Vertragspflichten oder nebenvertragliche Sorgfaltspflichten nicht vorsätzlich oder fahrlässig verletzt hat,

und eine außervertragliche Haftung einerseits

- aus unerlaubter Handlung (deliktische Haftung) nach § 823 BGB (vorsätzliche oder fahrlässige Verletzung eines Rechtsguts eines anderen). Sämtliche an der Leistungserbringung Beteiligten haften für alle durch einen von ihnen schuldhaft verursachten Fehler entstandenen Schäden. Die Nachweispflicht für das Verschulden und die Kausalität zwischen Fehler und Schaden liegt jedoch in der Regel beim Geschädigten,

und andererseits zum Beispiel

- nach dem Produkthaftungsgesetz und anderen Spezialgesetzen: Ein fehlerhaftes Produkt liegt vor, wenn dieses nicht die nach dem Stand von Wissenschaft und Technik zu erwartende Sicherheit bietet. Der Leistungserbringer haftet für einen auf eine fehlerhafte Leistung zurückzuführenden Schaden, ohne dass ihm Vorsatz oder Fahrlässigkeit nachgewiesen werden muss. Die Beweislast für den Zusammenhang zwischen Fehler und Schaden liegt jedoch beim Geschädigten. Die Haftung für Sachschäden nach dem Produkthaftungsgesetz umfasst lediglich Schäden an Gegenständen des privaten Gebrauchs. Daher stellt die deliktische Haftung nach §§ 823 ff. BGB die wesentliche Haftungsgrundlage für Schäden im gewerblichen Bereich dar.

Managed Security Services Anbieter sind hier also erheblichen zusätzlichen rechtlichen Risiken ausgesetzt.

[1] vgl. Klindtworth, Holger (2003)
[2] vgl. Dahmen, Jörn (2002), S.7-12

3 Operativer Rahmen zur Analyse und Risiko-orientierten Ausgestaltung der IT-Security

Der operative Rahmen zur Analyse und Risiko orientierten Ausgestaltung der IT-Security soll operative Möglichkeiten bezüglich des Umgangs mit IT-Security-Risiken aufzeigen, auf den aufsetzend im weiteren Verlauf ein diesbezüglich möglicher strategischer Handlungsspielraum bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens aufgezeigt wird.

Die Bedingungen, Möglichkeiten und Grenzen des strategischen Handlungsspielraums werden im Allgemeinen durch die unternehmerische Vision bestimmt, wie sie sich im Leitbild und in der Unternehmenskultur ausdrückt. Basis für die Entwicklung der Unternehmenskultur sind Unternehmensphilosophie (Idealziel) und Unternehmenspersönlichkeit (Corporate Identity). Die Unternehmenspersönlichkeit ergänzt die Unternehmensphilosophie, beide dokumentieren die Unternehmenspolitik. Die Unternehmenskultur erfasst historisch gewachsene und gegenwärtige Denkmuster, Verhaltensweisen, Ressourcen sowie Potenziale der Führungspersönlichkeiten und Mitarbeiter.[1] Der strategische Handlungsspielraum resultiert u. a. aus der Beurteilung der gegenwärtigen und sich abzeichnenden Chancen und Risiken der Umwelt und gibt u. a. die strategischen Maßnahmen an, um

- das allen Strategien und Aktionsplänen inhärente Risiko auf ein für die Unternehmung tragbares und ein von der Unternehmensleitung als akzeptabel erachtetes Maß zu reduzieren sowie
- den Wert der Unternehmung insgesamt und auf Dauer zu erhöhen.

Der Prozess der Bestimmung des strategischen Handlungsspielraums muss ein Gleichgewicht einstellen zwischen der Nutzung bestimmter Umweltmöglichkeiten, dem Einsatz der Kernkompetenzen, den Wünschen der unternehmerischen Entscheidungsträger und den objektiven Verpflichtungen der Unternehmung.[2]

Im Rahmen der Risikostrategie wird festgelegt, welche Risikosteuerungsoptionen (Akzeptieren, Begrenzen, Kompensieren, Reduzieren, Überwälzen, Vermeiden) in welchen Risikofeldern gewählt werden sollen.[3]

Bezüglich der IT-Security kann der strategische Handlungsspielraum einen Rahmen für die strategischen Möglichkeiten beschreiben, um die IT-Security-Risiken z. B. auf ein für die Unternehmung tragbares und ein von der Unternehmensleitung als akzeptabel erachtetes Maß

[1] vgl. Gadatsch, Andreas (2006), S.5-7
[2] vgl. Hinterhuber, Hans H. (2004b), S.139-141
[3] vgl. Ibers, Tobias (2005), S.52

zu reduzieren. Letztlich ist das auch der Ansatz des im weiteren Verlauf entwickelten strategischen Controllings der IT-Security, nämlich einen Kontext zu finden, in dem entsprechende Risiken akzeptiert werden können.

Nicht betrachtet werden sollen in diesem Zusammenhang Gefahren, die von den Informationssystemen für verschiedene verfassungsrechtlich geschützte Güter wie informationelle Selbstbestimmung und Fernmeldegeheimnis ausgehen.

3.1 Identifizierung von IT-Risiken und -Bedrohungen der sicherheitskritischen Geschäftsprozesse

3.1.1 Klassische Risikodefinitionen

Der technische Fortschritt trägt einerseits zur permanenten Innovationsfähigkeit, zur Gewinnerzielung und zum langfristigen Überleben von Unternehmen bei. Andererseits birgt er auch die Gefahr von Fehlfunktionen daran gekoppelter technischer Systeme. Dieser Ambivalenz steht ein aus zwei Komponenten zusammengesetzter Risikobegriff gegenüber: Einerseits ist auf die mögliche Unkenntnis von Ursache-Wirkungs-Beziehungen menschlicher oder technischer Aktivitäten abzustellen. Andererseits muss die Zielbezogenheit bzw. die Finalität menschlicher Handlungen berücksichtigt werden. Nur wenn gesetzte Ziele auch verfolgt werden, besteht erst die Möglichkeit ihres (unerwünschten) Nichteintretens.[1]

In den extensiven Risikodefinitionen liegen die Ursachen des Risikos nicht im Entscheidungsprozess und Informationsstand des Akteurs, sondern sind Begleiterscheinungen jeden wirtschaftlichen Tätigwerdens im Unternehmen.[2]

Risiko ist nach DIN, VDE Norm 31000 definiert durch das beim Eintritt eines gefährdenden Ereignisses zu erwartende Schadensausmaß (S) sowie die zu erwartende Häufigkeit/Eintrittswahrscheinlichkeit pro Zeiteinheit (W) dieses Ereignisses, als das Produkt aus Eintrittswahrscheinlichkeit und Schaden (R = W x S). Diese Risikodefinition sieht Risiko als sog. reine Risiken, d. h. als Verlustgefahr. Ein auf dieser Risikodefinition basierendes Risikomanagement wird als Risikomanagement im engeren Sinne oder Risk Management bezeichnet.

[1] vgl. Hölscher, Reinhold (2002), S.257
[2] vgl. Wolf, Klaus (2003a):, S.29

Nach einer allgemeineren Definition wird Risiko als Streuung um einen Erwartungswert definiert. Hierbei werden sowohl positive Abweichungen (Chancen) als auch negative Abweichungen (Gefahren) berücksichtigt. Einem entsprechenden Konzept für ein (in die normale Führungstätigkeit des Managements eines Unternehmens integriertes) Risikomanagement liegt also ein Risikoverständnis zugrunde, welches Risiko als Summe der Möglichkeiten sieht, dass sich Erwartungen des Systems Unternehmung aufgrund von Störprozessen nicht erfüllen.[1] Das im Zusammenhang mit der gegebenen Thematik im Folgenden zu entwickelnde Konzept basiert so gesehen auf einer Erweiterung eines Risk Managements der IT-Security zu einem Risikomanagement, welches die Möglichkeiten analysiert und kontrolliert, dass sich Erwartungen des Systems Unternehmung aufgrund mangelnder IT-Security nicht erfüllen.

Der extensive Risikobegriff leitet sich aus dem entscheidungsbezogenen Risikobegriff ab, wenn Entscheidungen das handlungsbestimmende Element sind. Diese Handlungen wiederum rufen Risiken hervor. Eine Entscheidung wird dabei definiert als Auswahl aus mehreren Handlungsmöglichkeiten, die dem Entscheider zur Realisierung seiner Ziele zur Verfügung stehen. Man spricht von „Entscheidungssituationen unter Risiko“ und „Entscheidungssituationen unter Unsicherheit“: In Entscheidungssituationen unter Risiko liegen subjektive oder objektive Wahrscheinlichkeiten hinsichtlich der zukünftigen Zustände vor (measurable uncertainty), bei Unsicherheit dagegen bestehen keinerlei Wahrscheinlichkeitsvorstellungen (unmeasurable uncertainty).

Des Weiteren kann in verteilungsorientierte und ereignisorientierte Risiken unterschieden werden. Verteilungsorientierte Risiken ergeben sich aufgrund von Schwankungen bestimmter (Markt) Parameter (z. B. Absatzmenge) und spiegeln eine Vielzahl nicht trennbarer Einzelstörungen wider. Gemäß dem Zentralen Grenzwertsatz aus der Statistik konvergiert die Summe solcher Einzelstörungen gegen eine Normalverteilung. Für ereignisorientierte Risiken ist bei der Aggregation von Einzelrisiken keine Verteilungsannahme möglich.[2]

Risiken entstehen durch die unvollständige Prognostizierbarkeit der Auswirkungen unternehmerischer Entscheidungen und externer Faktoren zukünftiger Entwicklungen.[3] Risiko bedeutet dann die Gefahr, dass Ereignisse (externe Faktoren) oder Entscheidungen und Handlungen (interne Faktoren) das Unternehmen daran hindern (informatorische, ursachen-

[1] vgl. Dahmen, Jörn (2002), S.35
[2] vgl. Reichling, Peter (2003), S.229
[3] Diederichs, Marc (2004),S.8

bezogene Komponente) definierte Ziele zu erreichen bzw. Strategien erfolgreich zu realisieren (wertende, wirkungsbezogene Komponente).[1] Die ursachenbezogene Komponente bezieht sich auf die Möglichkeit des Eintritts eines bestimmten Ereignisses, die wirkungsbezogene Komponente auf die Möglichkeit der (negativen) Zielverfehlung. Dies führt zur betriebswirtschaftlichen Sicht von Risiko als Ausmaß, in dem das Erreichen geschäftlicher Ziele oder Strategien durch Ereignisse oder Handlungen/Unterlassungen von innerhalb oder außerhalb des Unternehmens gefährdet ist. So stellt ein Ereignis für ein Unternehmen ein Risiko dar, wenn sein Eintreten sowohl unsicher ist, als auch Auswirkungen auf das Erreichen der Unternehmensziele hat.[2]

Risiko kann nur dann auftreten, wenn eine Zielsetzung bzw. Zielverfolgung mit der Unkenntnis/Ungewissheit gekoppelt ist, ob das angestrebte Ziel auch tatsächlich erreicht wird/werden kann.[3] Ein Merkmal von Risiko ist dann sein Entstehen aus der Unsicherheit bezüglich Entscheidungsprämissen.[4]

Ein die IT-Sicherheit betreffendes bzw. gefährdendes Ereignis ist immer unsicher bzw. in der Regel nicht prognostizierbar. Ob es ein Risiko für das Unternehmen darstellt, hängt davon ab, ob sein Eintreten Auswirkungen auf das Erreichen der Unternehmensziele hat.

Realisiert sich das Risiko, so ist es die positive oder negative Abweichung vom erwarteten Ausgang. Als Risikomaß wird hierbei üblicherweise die Varianz bzw. die Standardabeichung vom erwarteten Wert benutzt.

Die informationsorientierte Risikosicht deutet Risiko als eine „spezifisch geartete Informationsstruktur, welche den Entscheidungen zugrunde liegt“. Das Risiko wird bestimmt durch Ungewissheit, geprägt von Unbestimmtheit und Unvollständigkeit.[5]. Risiko umfasst dann nicht nur die einer Entscheidung zugrunde liegende Unsicherheit bezüglich des Eintritts einer bestimmten Umwelt-Konstellation. Es leitet sich auch aus dem unvollständigen, das Problemlösungsverhalten bestimmenden Informations-Input und aus der Qualität der Prämissenfestlegung ab.

Die Risikobewertung eines Ereignisses hat eine deutliche psychologische Beeinflussbarkeitskomponente: Ein Ereignis wird als Risiko betrachtet, wenn sein Eintreten unsicher ist und sein Nichteintreten dem Eintreten vorgezogen wird. Das Vorliegen eines Risikos ist in doppelter Hinsicht subjektiv: Ob sein Eintreten als unsicher betrachtet wird, hängt vom

[1] Diederichs, Marc (2004), S.10
[2] vgl. Finke, Robert (2005), S.18
[3] vgl. Hölscher, Reinhold (2002), S.258
[4] vgl. Martin, Thomas A. (2002), S.71
[5] vgl. Wolf, Klaus (2003a), S.30

Wissen des Beurteilenden ab, und ob der Beurteilende das Risiko akzeptiert oder ablehnt, ist ebenfalls subjektiv.[1] Das Wissen eines Wirtschaftssubjekts ist dabei definiert als Gesamtheit seiner Vorstellungsinhalte über Regelmäßigkeiten seiner Umwelt und über Interaktionen mit dieser Umwelt, die es durch Informationsaufnahme und -verarbeitung erworben hat.[2] Wissen wird von Individuen konstruiert und kann deren Erwartungen über Ursache-Wirkungszusammenhänge repräsentierend definiert werden. Diese intuitive Form der Risikowahrnehmung basiert auf einer Vermittlung von Informationen über die Gefahrenquelle, den psychischen Verarbeitungsmustern von Unsicherheit und früheren Erfahrungen mit Gefahren.[3] Die subjektive Risikowahrnehmung und -bewertung weist somit Beeinflussbarkeitsmöglichkeiten auf:

Bei subjektiven Risiken handelt es sich um individuelle Risikomerkmale wie Leichtsinn, Sorgsamkeit, Zuverlässigkeit … .Im sozialen Kontext sind Risiken und deren individuelle Wahrnehmung oft objektiv nicht erschließbar, sondern als Effekte sozialer Konstruktion automatisch umstritten.[4] Ursache und Ausmaß von Risiken messen sich an der Fähigkeit des Akteurs, Umweltentwicklungen vorherzusehen. Die Wirkung des Risikos ist die Zielgefährdung, mit dieser findet letztlich das Opportunitätskostenprinzip Eingang in die Risikobetrachtung.[5]

Analog sind Werte bzw. Werthaltungen im Unternehmen im sozialen Kontext der Gesellschaft zu sehen, in dem das Unternehmen eingebunden ist. So wird automatisch ein Bezug hergestellt zwischen dem, an was ein Unternehmen glaubt und dem, was in der Gesellschaft an Werthaltungen vorherrscht.[6]

Risiken entspringen prinzipiell einem Informationsdefizit.[7] In letzter Konsequenz wird Risiko immer bestimmt durch von Unbestimmtheit und Unvollständigkeit geprägter Ungewissheit. In diesem Sinne ist die informationsorientierte Risikosicht die allgemeinste Risikosicht. Rationale Entscheidungen sind von einem gewissen Informationsstand der Akteure abhängig. Und wenn Entscheidungen das handlungsbestimmende Element sind und Handlungen wiederum Risiken hervorrufen, ist der Bogen zur extensiven Risikodefinition hergestellt. Konsequenterweise wird im weiteren Verlauf Risiko auf abstraktester Ebene als von Unbestimmtheit und Unvollständigkeit geprägter Ungewissheit begründet angesehen.

[1] vgl. Finke, Robert (2005), S.16
[2] vgl. Gössinger, Ralf (2005), S.85
[3] Hölscher, Reinhold (2002), S.78
[4] vgl. Japp, Klaus P. (2000), S.14
[5] vgl. Wolf, Klaus (2003a), S.30
[6] vgl. Seidenschwarz, Werner/Huber, Christian (2002), S.133
[7] Keuper, Frank [2005], S.269

Im Bereich der IT-Sicherheit wird Risiko üblicherweise als Zusammentreffen einer Schwachstelle mit einer Bedrohung definiert. Das Management der Risiken basiert dann auf einer Schwachstellenanalyse und einer Bedrohungsanalyse. Dieser Ansatz erscheint für ein operatives Risikomanagement sinnvoll. Für das strategische Risikomanagement definiert man Risiko aufsetzend auf der betriebswirtschaftlichen Sichtweise besser als mögliche Nichterfüllung von Erwartungen und (entsprechend der entscheidungstheoretischen Sicht) als Informationsdefizit (abgeleitet aus dem Grad der Bestimmtheit und dem Wissensgrad, d. h. der Ungewissheit (objektive Unmöglichkeit des Wissens)) über das Erreichen angestrebter Ziele.[1] Die Bewertung der IT-Security auf Basis des IT-Security-Managements (als Ausprägung des strategischen Risikomanagements im Bereich der IT-Security) ermittelt dann den Grad der Bestimmtheit und der Ungewissheit über das Erreichen angestrebter Ziele, auf strategischer Ebene die Absicherung bzw. Ermöglichung neuer Geschäftsprozesse/Geschäftsmodelle (soweit durch die IT-Security beeinflussbar). Die „operative Bewertung“ der IT-Security bestimmt den Erreichungs-/Aufrechterhaltungsgrad des Soll-IT-Security-Niveaus. In diesem Fall werden IT-Security-Risiken im operativen IT-Security-Management (als Ausprägung des operativen Risikomanagements im Bereich der IT-Security) auf Basis der Schwachstellenanalyse und der Bedrohungsanalyse gemanagt, um aus den Ergebnissen einer Risikoanalyse (mit der Definition von Risiko als Zusammentreffen einer Schwachstelle mit einer Bedrohung) die zu ergreifenden IT-Sicherheitsmaßnahmen festzulegen.

3.1.2 Ansätze zur Typisierung/Generalisierung von Risiken der IT-Sicherheit

Grundsätzlich lassen sich für alle Unternehmen Risiken in die Hauptkategorien Risiken des leistungswirtschaftlichen Bereichs (Beschaffungs-, Produktions-, Absatz- und Technologierisiken), Risiken des finanzwirtschaftlichen Bereichs (Liquiditätsrisiken, Marktpreisrisiken, politische Risiken, Ausfallrisiken, Kapitalstrukturrisiken) und Risiken der Corporate Governance (Management aller Risiken, die mit dem Ziel einer guten, verantwortungsvollen und auf langfristige Wertschöpfung ausgerichtete Unternehmensführung und Kontrolle verbunden sind) einteilen. Des Weiteren können alle Risiken durch interne oder externe Ereignisse und Störungen verursacht werden. Die Abgrenzung zwischen den einzelnen Risikokategorien ist aufgrund der Vielschichtigkeit und Komplexität aber häufig schwierig.[2]

[1] vgl. Wallmüller, Ernest (2004), S.9
[2] vgl. Romeike, Frank (2004), S.168-173

Im Hinblick auf die Steuerung strategischer Erfolgsfaktoren werden Risiken nach der Herkunft der ursächlichen Handlungen oder Ereignisse in exogene und endogene Risiken unterteilt. Endogene Risiken resultieren aus einer unternehmerischen Handlung oder Entscheidung innerhalb des Unternehmens. Sie sind in starkem Ausmaß an strategische Erfolgsfaktoren gebunden und Ursache und Wirkung im Rahmen von Planungen zumeist gut absehbar. Die Ursachen exogener Risiken liegen außerhalb der unternehmerischen Entscheidungsgewalt, d. h. im Umfeld des Unternehmens. Diese Risiken wirken zwar auch auf die strategischen Erfolgsfaktoren, können diesen aber nicht direkt zugeordnet werden.[1] Im Zusammenhang mit der gegebenen Thematik, insbesondere dem strategischen Controlling geht es um exogene Risiken. Konzepte zum Umgang mit diesen Risiken ergeben sich aus Überlegungen zum Anpassungsprozess an das Umfeld des Unternehmens.

Risiken können des Weiteren in Verhaltens- und Zustandsrisiken unterteilt werden. Mögliche Gefahren aufgrund unerwarteter mangelhafter interner Abläufe (z. B. mangelnde Sorgfalt von Mitarbeitern oder Fehlfunktionen von Systemen) oder unerwarteter externer Beeinträchtigungen der internen Abläufe (z. B. Hackerangriffe oder Naturkatastrophen) werden als „Operationelle Risiken“ bezeichnet.[2] Im Rahmen von Basel II werden operationelle Risiken definiert als die „Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen oder Systemen oder von externen Ereignissen eintreten“.

Die Verbesserung des Managements operationeller Risiken ist das eigentliche Ziel des Risikomanagements.[3] Operationelle Risiken können in die Risikobereiche: Äußere Faktoren, Systeme, Prozesse, Personen, Zufall eingeordnet[4] sowie in operative (das Richtige falsch machen[5]) und strategische Risiken (das Falsche machen[6]) eingeteilt werden.

Dabei resultiert die Möglichkeit von Zufällen aus der Komplexität des Geschäftssystems, insbesondere der komplizierten technischen Infrastruktur. Dadurch kann eine Vielzahl gefährlicher Wechselwirkungen auftreten. Das Gegenteil dieser Komplexität ist die lose Kopplung. Dadurch kann die Fähigkeit von Geschäftsvorgängen, Organisationen und technischen Systemen, bei unvorhergesehenen Ereignissen das Geschäft fortzuführen und vor Schaden zu bewahren, unterstützt werden.[7]

[1] vgl. Reichmann, Thomas/Form, Stephan (2000), S.4,5
[2] vgl. Merbecks, Andreas (2004), S.87
[3] vgl. Romeike, Frank (2005, S.255
[4] vgl. Wieczorek, Martin (2003), S.8-13
[5] vgl. PwC (2000):, S.9
[6] vgl. PwC (2000):, S.9
[7] vgl. Wieczorek, Martin (2003), S.14-15

Operative Risiken umfassen externe Risiken, organisatorische Risiken, technologische-/prozessbezogene Risiken und personalbezogene Risiken. Technologische Risiken beinhalten Risiken der Kommunikation sowie der Hard- und Software.[1]

Man unterscheidet zwischen Sicherheitsvorfällen (Security Incidents) und Angriffen (Attacks). Ein Sicherheitsvorfall ist definiert als das Ausnutzen von Sicherheitslücken oder das bewusste Umgehen getroffener Sicherheitsmaßnahmen mit dem Ziel, Informationen zu verändern, zu zerstören oder zu stehlen oder die Verfügbarkeit eines Dienstes zu unterbrechen. Ein Angriff ist ein einzelner Versuch, unautorisierten Zugang zu einem System zu erhalten. Ein Sicherheitsvorfall besteht aus einer Anzahl von methodischen, z. B. in einem zeitlichen Zusammenhang stehenden Angriffen. Die meisten Angreifer benutzen ausgeklügelte Agentenprogramme, mit denen das Netzwerk systematisch nach Sicherheitslücken durchsucht wird.[2] Man unterscheidet drei große Kategorien von Sicherheitsvorfällen: Malicious Code (Viren, Würmer, Trojaner), Hacking (Ausnutzen von Sicherheitslücken in Hard- und Software durch Personen) und Denial of Service (DOS) (direkter Angriff auf die Verfügbarkeit eines Dienstes).[3]

Risikofaktoren der IuK-Technologie werden z. B. unterteilt in: [4]

- Vernetzung, Internet-Nutzung

  Die Möglichkeiten der Vernetzung führen über menschliches Versagen (Fehlbedienung, mangelhafte Konfiguration/Administration) oder dem Ausfall von Netzen/Netzteilen (z. B. aufgrund mangelhafter Stromversorgung, Kapazitätsauslastung von Speichermedien oder gezielten Angriffen) zur Beeinträchtigung der Verfügbarkeit und korrekten Funktionalität von zentralen Diensten. Weitere Risikopotenziale der Vernetzung sind z. B.: Abhören von Leitungen, unbefugter Zugriff auf Komponenten im Netz von außerhalb, Vortäuschen einer falschen Identität oder das Einschleusen von Malicious Code (Viren, Würmer, Trojaner). Dies sind Potenziale zum Angriff auf die Sicherheitsziele Verfügbarkeit, Vertraulichkeit, Integrität und sogar Verbindlichkeit.

- Outsourcing

  Outsourcing bietet zusätzliche Angriffsflächen, z. B. durch Know-how Abfluss (wenn externe Kenntnis zu Zugang/Zugriff und Strukturen der IT-Systeme erhalten), fehlendes eigenes Know-how und Abhängigkeitsverhältnisse (wenn Sicherheitslücken zunächst

[1] vgl. Wallmüller, Ernest (2004), S.15
[2] vgl. Kyas, Ottmar (2000), S.25
[3] vgl. Horster, Patrick (2002b), S.305,306
[4] vgl. Sonntag, Matthias (2005, S.56-58

nicht erkennbar sind und Sicherheitsvorfälle teilweise nur mithilfe externer Fachleute analysiert und behoben werden können).

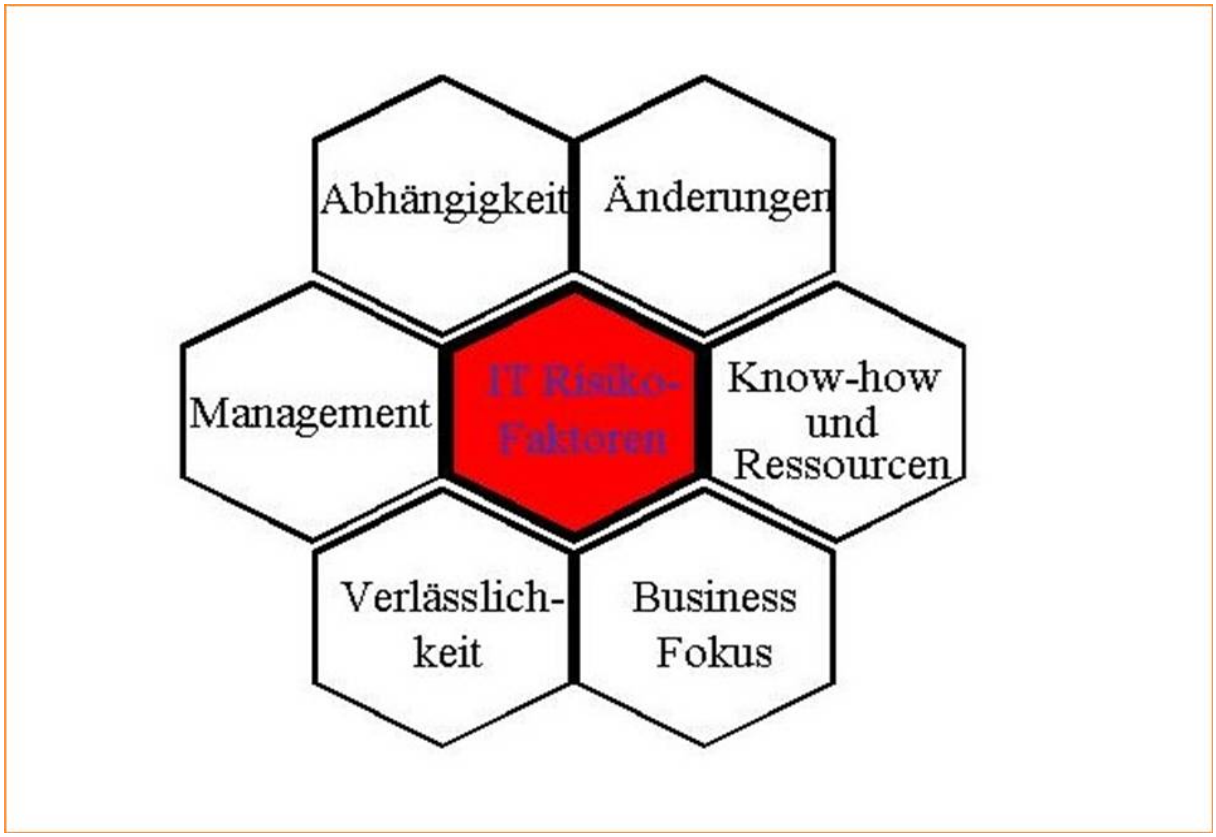
Verhaltensrisiken können durch das Problem des Bewertens und Bildens von Information begründet sein: Es entsteht durch Filtern, Auswerten, Erzeugen und Verteilen/Nicht-Verteilen von Informationen in der Zeitdimension.[1] Zustandsrisiken/IT-Risiken werden unterteilt in IT-Infrastrukturrisiken, IT-Anwendungsrisiken und IT-Geschäftsprozessrisiken: IT-Infrastrukturrisiken beziehen sich auf die Angemessenheit der IT-Infrastruktur für die Informationsverarbeitung. In der IT-Grundschutzmethode wird die Infrastruktur, die für einen bestimmten Geschäftsprozess notwendig ist, als IT-Verbund bezeichnet.[2]

IT-Anwendungsrisiken ergeben sich aus Unzulänglichkeiten der IT-Anwendungssysteme. IT-Geschäftsprozessrisiken beruhen darauf, dass IT-Kontrollen zwar hinsichtlich der Teilprozesse, nicht aber hinsichtlich des Gesamtprozesses wirksam werden.

Im Rahmen des Managements von operativen Risiken bietet sich zur Strukturierung der vielfältigen IT-Risiken ein IT-Risk-Framework an. Dabei wird zwischen sechs Risikobereichen unterschieden:

Der Bereich Management umfasst Risiken im Zusammenhang mit der IT-Organisation und IT-Steuerung. Diese Risiken basieren auf unklaren Organisationsstrukturen und einer ungenügend nachvollziehbaren Steuerung. Der Bereich Abhängigkeit umfasst Risiken, die sich gegen die Verfügbarkeit von Systemen (Katastrophenrisiko) richten und sich aus der Abhängigkeit von Anderen ergeben. Der Bereich Änderungen beinhaltet Risiken, die sich aus unzureichenden Prozessen im Bereich Systementwicklung, Einführung und Wartung ergeben. Know-how und Ressourcen ist der Bereich von Risiken, basierend auf der mangelnden Fähigkeit eines Unternehmens, flexibel in einem von schnellem technologischem Wandel geprägten Umfeld reagieren zu können. Business Fokus richtet sich auf Risiken im Zusammenhang mit der Ausrichtung der IT auf die Unterstützung der Geschäftsprozesse. Verlässlichkeit umfasst Risiken im Zusammenhang mit den klassischen IT-Bedrohungen der Zuverlässigkeit (Verfügbarkeit, Vertraulichkeit und Integrität) der durch die eingesetzte Informations- und Kommunikationstechnologie unterstützten Prozesse.

[1] vgl. Bieta, Volker (2004), S.8
[2] vgl. Humpert, Frederik (2005), S.7



(Quelle: Gaulke Markus (2003))

Abb. 5 Bereiche für IT-Risiken im IT-Risk-Framework

Strategische Risiken sind solche Risiken, die die Erfolgspotenziale des Unternehmens gefährden.[1] Sie beinhalten die Gefahr, dass der Rahmen für das unternehmerische Handeln nicht so ausgerichtet ist, dass z. B. die Verschwendung von Ressourcen aufgrund von nicht mehr gültigen Prämissen und damit einer ungültigen Strategie vermieden wird.

Risiken der IT-Sicherheit im engeren Sinn werden den technologischen Risiken der operativen Risiken zugerechnet. Risiken der IT-Sicherheit im weiteren Sinn sind in allen Bereichen operationeller Risiken vorstellbar. Risiken der IT-Sicherheit im engeren wie auch im weiteren Sinn können insbesondere sowohl Zustands- als auch Verhaltensrisiken sein.

3.1.3 Sicherheitsanalysen zur Abschätzung von Risiken

Die für die erforderliche IT-Sicherheit zu ergreifenden IT-Sicherheitsmaßnahmen werden klassischerweise auf Basis der Ergebnisse einer Risikoanalyse bestimmt. Diese untersucht IT-

[1] vgl. Martin, Thomas A. (2002), S.75

Systeme auf Schwachstellen und auf Bedrohungen hin, die zu Gefährdungen für die IT-Sicherheit führen könnten. Diese Risikoanalyse setzt zunächst eine Schutzbedarfsanalyse voraus, welche die verwendeten IT-Systeme und Datenbestände nach ihrer Bedeutung für das Unternehmen klassifiziert. Mit Sicherheitsanalysen wird dabei der Schutzbedarf der Geschäftsprozesse und damit der der von ihnen verwendeten IT-Systeme und Datenbestände untersucht.[1]

Die erweiterte Sicherheitsanalyse gemäß Grundschutzhandbuch überprüft vor allem technisch, ob die getroffenen Standard-Sicherheitsmaßnahmen gängigen Angriffsszenarien standhalten. Mögliche Instrumente der erweiterten Sicherheitsanalyse sind spezielle Risikoanalysen, die Differenz-Sicherheitsanalyse und Penetrationstests. Für eine Risikoanalyse in diesem Sinn lässt sich zum Erkennen von Schwachstellen das Verfahren der Angriffsbäume nutzen. Ausgehend vom Ziel eines Angriffs analysiert dieses Verfahren, welche Möglichkeiten genutzt werden könnten, um in ein System einzudringen. Die Machbarkeit der einzelnen Schritte dorthin wird bewertet und logisch verkettet. Nach Analyse der aus dem Angriffsbaum abzulesenden potenziellen Schwachstellen und Analyse der denkbaren Gefährdungen sollen dann Maßnahmen getroffen werden, um die Schwachstellen zu schließen oder zu minimieren, für die Gefährdungen existieren. Bei der sog. Differenz-Sicherheitsanalyse werden die Maßnahmen der IT-Sicherheit auf Höherwertigkeit analysiert, d. h., inwieweit die Maßnahmen von den Standard-Grundschutzmaßnahmen abweichen. Anschließend wird verglichen, ob diese höherwertigen Maßnahmen den Musterlösungen entsprechen, die sich in der Praxis für hochschutzbedürftige IT-Bereiche etabliert haben, und beurteilt, ob diese geeignet sind. Kryptografische Verfahren beispielsweise erhöhen die Vertraulichkeit und Integrität von Daten, sind aber in Bezug auf die Verfügbarkeit meist ungeeignet. Ziel eines Penetrationstests ist immer, mit mehr oder weniger großem Vorwissen Zugriff auf gespeicherte Daten zu erlangen und die Vorgehensweise zu dokumentieren. So sollen Schwachstellen aufgespürt und Anhaltspunkte gegeben werden, wie die Infrastruktur besser gesichert werden kann.[2]

Sicherheits-Erfordernisse können aus dieser rein technischen Perspektive, aber auch aus einer Business-Perspektive betrachtet werden. Erstere entspricht der Risikoanalyse von IT-Security-Risiken im operativen IT-Security-Management (als Ausprägung des operativen Risikomanagements im Bereich der IT-Security) auf Basis der Schwachstellenanalyse und der Bedrohungsanalyse. In der Bedrohungsanalyse werden potenzielle Bedrohungen erfasst, die sich aus dem technologischen, politischen oder wirtschaftlichen Umfeld des Unternehmens, aus

[1] vgl. Rieger, Holger (2005b), S.69
[2] vgl. Humpert, Frederik (2005), 50-55

dem Standort, seiner aktuellen Situation, seiner Marktposition, seinem Image ergeben. Für eine solche Risikoanalyse ist zunächst ein Überblick über mögliche Gefahrenpotenziale notwendig, um relevante, aber nicht offensichtliche und nicht vorhersehbare Risiken zu identifizieren. So sind auch Risiken zu identifizieren, die auf den ersten Blick nicht als Bedrohung erkennbar sind. Operationelle Risiken sind kaum zu identifizieren und zu quantifizieren. Schäden etwa aufgrund menschlicher Fehler oder Computerviren können alle Bereiche des Unternehmens betreffen.[1] Operationelle (IT-)Risiken sind mit jeder wirtschaftlichen Aktivität verbunden, schwer erfassbar und in hohem Maße unternehmensspezifisch ausgerichtet. Eine gezielte Handhabung muss in Form eines operationellen (IT-)Risikomanagements ("Operational (IT-)Risk Management") stattfinden. Ein sinnvolles Management der operationellen Risiken stützt sich dabei auf das Management der Qualität der Geschäftsprozesse sowie die Kenntnisse der Mitarbeiter von Prozessen und Prozessverknüpfungen innerhalb des Unternehmens.

Als geeignete Methode zur Schätzung des Verlustpotenzials eines Risikofaktors wird die Worst-Case- bzw. Middle-Case-Analyse genannt. Im Worst-Case wird der unter den ungünstigsten Bedingungen eintretende prozentuale Verlust bezogen auf eine Risikoeinheit (z. B. das Eigenkapital der Unternehmung) ermittelt. Im Middle-Case soll der prozentuale Verlust geschätzt werden, der im minderschweren (zweit schlimmsten) Fall eintritt. Hierbei ist der Middle-Case so anzusetzen, dass er neben dem geringeren Verlustpotenzial in der Regel mit einer größeren Möglichkeit des Risikoeintritts einhergeht. Dieser Ansatz berücksichtigt explizit die im Rahmen von KonTraG zu betrachtenden Konsequenzen einer besonders ungünstigen Entwicklung für das Unternehmen.[2] Der Erfolg des (operativen) Risikomanagements hängt aber nicht davon ab, jedes Risiko exakt zu berechnen. Im Rahmen der Analyse werden wichtige Erkenntnisse zur strategischen Bedeutung bestimmter Risiken gewonnen.[3] Dementsprechend wird die ordinale Risikobewertung bevorzugt, die auch im IT-Sicherheitshandbuch des BSI Anwendung findet. Dabei wird das zu untersuchende System in Objekte zerlegt, denen Risiken in den Kategorien Tragbarkeit/Untragbarkeit und sehr wahrscheinlich bis hin zu sehr unwahrscheinlich zugeordnet werden.

In der Business-Perspektive der Sicherheitserfordernisse soll die strategische Risikoanalyse dem Management ermöglichen, sich auf eine Strategie zum Umgang mit Risiken festzulegen. Die Herausforderung für die Unternehmung besteht dabei in der Bewältigung des Unerwarteten: Sie muss die Fähigkeit aufbauen, das Nichtvorhersehbare erfolgreich und effizient

[1] vgl. Merbecks, Andreas (2004), S.88
[2] vgl. Reichling, Peter (2003), S.228
[3] vgl. Merbecks, Andreas (2004), S.103,104

zu meistern. Auch angesichts zunehmender Beschleunigung der Veränderung kommt dabei der unternehmerischen Flexibilität, der Wahrung der Handlungsbefähigung und einer i. d. S. verstandenen strategischen Führung wesentliche Bedeutung zu.[1]

Im Zusammenhang mit der gegebenen Thematik geht es um den Umgang mit operationellen Risiken, d. h. um mögliche Gefahren ausgehend von unerwarteten mangelhaften internen Abläufen oder unerwarteten externen Beeinträchtigungen der internen Abläufe. Solche Risiken werden eingeteilt in operative und strategische Risiken.

Aus der Unternehmenstätigkeit resultierende Risiken lassen sich mit Hilfe von Elementen der strategischen Unternehmensanalyse erfassen. Dabei werden die Leistungserstellung des Unternehmens (interne Risiken) und das Unternehmensumfeld (externe Risiken) getrennt analysiert. Die mit der Leistungserstellung verbundenen Risiken, Risiken im Unternehmen lassen sich beispielsweise als personell, sachlich-technisch sowie organisatorisch-strukturell charakterisieren. Notwendig ist zu Beginn eine Unterteilung des Unternehmens in Risikobereiche, die sich an die vorhandene Aufbau- oder Ablauforganisationsstruktur anlehnt. Basis für die Analyse von internen Risiken kann dabei grundsätzlich die Sichtweise der funktionalen oder der prozessualen Darstellung des Unternehmens und seiner Risiken sein. Bei der Analyse von Risiken aus dem Umfeld geht es im Allgemeinen um ökonomische, politisch/rechtliche, soziale, technologische Umweltrisiken und Risiken auf Beschaffungs- und Absatzmärkten. Aufgabe des Risiko-Controllings ist es dabei, aus den allgemein gehaltenen Daten über die Entwicklung im weiten Unternehmensumfeld risikorelevante Daten herauszufiltern und aufzubereiten.[2]

3.1.3.1 Angebots-seitige Risiken: Leistungsrisiken der primären Wertschöpfungskette und der Unterstützungsfunktionen

Der Bereich der unternehmerischen Leistungserstellung weist erhebliches Risikopotenzial auf z. B. aufgrund eines nur unzureichend qualifizierten Personalstammes, insbesondere bezüglich Computerspezialisten. Aber auch Risiken, die die Qualität und Ergiebigkeit der Leistung beeinträchtigen können, sind hier wichtig. Dies sind neben personellen Produktionseinflüssen aufgrund fehlerhafter Arbeitsorganisation und Arbeitsweise sowie Mängeln der Arbeitskräfte hinsichtlich Fähigkeiten, Fertigkeiten und Sorgfalt auch materielle und technische Produktionseinflüsse. Bei diesen liegen die Ursachen in fehlerhaftem Material sowie

[1] vgl. Hinterhuber, Hans H. (2004a), S.V
[2] vgl. Burger, Anton/Buchhart, Anton (2002), S.36-41

technischen Risiken, die mit der Produktion und den dafür eingesetzten Ressourcen in Zusammenhang stehen, z. B. Risiken technischer Anlagen, die zu einem Ausfall der Produktion oder zu einer ungeplanten Erhöhung der Produktionskosten führen können. Aber auch z. B. Einkaufs- und Beschaffungsrisiken in Form einer Preis- oder Lieferabhängigkeit oder mangelnder Qualität des benötigten Materials werden in diesem Zusammenhang genannt.[1]

Operative Risiken sind vor allem diese Angebots-seitigen Risiken, die zu einem teilweisen oder vollständigen Ausfall der Leistungserstellung/Produktion oder zumindest zu ungeplanten Erhöhungen der Leistungserstellungskosten führen können. Sie werden auch als Betriebsrisiken bezeichnet[2] und gehören zu den Leistungsrisiken der primären Wertschöpfungskette und der Unterstützungsfunktionen (z. B. Kalkulationsfehler oder Ausfall der EDV), d. h. Risiken, die mit der Leistungserstellung (Wertschöpfung) und den dafür eingesetzten Ressourcen in Zusammenhang stehen, also z. B. Feuerschäden, Maschinenausfall oder Arbeitsunfälle.[3]

Operative IT-Risiken können weitgehend mithilfe IT-gestützter Risikomonitoring-Systeme (zur Überwachung von Unternehmensdaten unter Risikogesichtspunkten) abgedeckt werden, zum Beispiel:

- Fehler im Prozess (Fehler in den eigentlichen operativen Systemen oder Einzelfehler, die durch die vorhandenen Kontrollen nicht aufgedeckt werden),
- Fehler im Reporting (Untersuchung von Differenzen durch Analyse der Rohdaten und Vergleich mit verdichteten Daten aus Auswertungen der Systeme),
- Manipulationen von Systemen (bewusste Verwendung des EDV-Systems mit dem Ziel der Schädigung des Unternehmens).

Dabei muss zunächst die Datenqualität sichergestellt werden. Dies betrifft die Validität (Gültigkeit), Integrität, Vollständigkeit und Relevanz. Es sind fehlerhafte und unvollständige Datensätze zu identifizieren. Sobald die notwendige Grundqualität hergestellt ist, können Prozess orientierte Gesichtspunkte in den Vordergrund treten.[4]

3.1.3.2 Nachfrage-seitige Marktrisiken: Strategierisiken

Der Markt bildet den eigentlichen Ausgangspunkt bei der Analyse der unternehmerischen Risiken. Je mehr ein Unternehmen und seine generierten Umsätze von den Marktgegeben-

[1] vgl. Reichling, Peter (2003), S.221
[2] vgl. Ibers, Tobias (2005), S.42
[3] vgl. Gleißner, Werner/Meier, Günter (2000)
[4] vgl. Klindtworth, Holger (2005)

heiten abhängt, umso größer ist sein marktbezogenes Risiko. Ein typisches Beispiel stellt die Telekommunikationsbranche dar. Aufgrund schnelllebiger Produkte und z. B. aufgrund von Produktinnovationen sind die Risiken hier erheblich. Es sei nur an den harten Wettbewerbsdruck bei den Verhandlungen um die UMTS-Lizenzen erinnert.[1]

Der Rahmen für das unternehmerische Handeln ist so auszurichten, dass z. B. die Verschwendung von Ressourcen aufgrund von nicht mehr gültigen Prämissen und damit einer ungültigen Strategie vermieden wird. Unternehmerische Entscheidungen müssen dabei häufig unter hoher Unsicherheit gefällt werden. Aus diesem Grund gewinnen flexible Strategien an Bedeutung, welche Handlungsspielräume eröffnen und welche dem Fall der möglichen Veränderung von Entscheidungsprämissen Rechnung tragen.[2] :

Der Strategiefindungsprozess verläuft in der Praxis selten analytisch-rational und adaptiv (an die Unternehmensumfeldanpassung orientiert), sondern ist vielmehr oft von Intuition geprägt.[3] Bei der Formulierung von Strategien wird gewöhnlich eine Vielzahl von Prämissen gesetzt, die auch miteinander verknüpft sein können. Eine Reduktion der Komplexität des Unternehmensumfelds wird durch Selektion und Verdichtung der großen Menge von Umweltinformationen mittels der Setzung von Prämissen möglich.[4] Zu Prämissen der Strategie werden die als Hypothesen über zukünftige Sachverhalte zu interpretierende mehr oder weniger begründbare oder beweisbare Annahmen, wenn von ihrem zukünftigen erwarteten Eintreten die unternehmenszielerreichende Strategierealisation abhängt.[5] Dabei ist eine Fokussierung auf die wichtigsten Prämissen notwendig.[6] Die praktische Durchführung der Selektion und die verwendeten Filterkriterien können aber nie irrtumsfrei sein. In Bezug zu einer Unternehmensumwelt mit hoher Komplexität spricht man von den Selektionsrisiken der Planung.

Selektion bedeutet immer, dass Ausblendungen stattfinden. Diese Ausblendungen können Ursachen enthalten, die in der zukünftigen Entwicklung zu unvorhergesehenen Störungen führen[7] und auf zukünftige Strategie-Umsetzungsgefahren hindeuten.

Für das strategische Risikomanagement ist es außerdem wichtig, Szenarien mit plausiblen Abläufen von Aktionen und Reaktionen abzubilden und durchzuspielen. Ziel der Szenariotechnik ist es, die zukünftige Entwicklung des Untersuchungsgegenstandes unter Zugrunde-

[1] vgl. Reichling, Peter (2003), S.219
[2] vgl. Edelmüller, Martina (2003) , S.5
[3] vgl. Eschenbach, Rolf (2003), S.12
[4] vgl. Piser, Marc (2004), S.38
[5] vgl. Piser, Marc (2004), S.43
[6] vgl. Piser, Marc (2004), S.44
[7] vgl. Piser, Marc (2004), S.38

legung alternativer Umfeldbedingungen transparent zu machen. Dabei wird die Ungewissheit über die Richtigkeit unternehmerischer Entscheidungen bewusst akzeptiert.[1]

Obige Überlegungen werden im weiteren Verlauf auf das strategische IT-Security-Management übertragen. Zunächst wird aber zwecks Risikoanalyse im operativen IT-Security-Management untersucht, welcher Zusammenhang zwischen Risiken und der Wichtigkeit und Kritikalität der IT-Systeme und –Prozesse bzw. damit be- und verarbeiteter Informationen angenommen werden kann. So wird transparent, mit welchen Ansätzen die der Risikoanalyse vorausgehende Schutzbedarfsanalyse die verwendeten IT-Systeme und Datenbestände nach ihrer Bedeutung für das Unternehmen klassifizieren kann.

3.1.4 Risikobetrachtungen orientiert an der Kritikalität der IT-Systeme, -Prozesse sowie be- und verarbeiteter Informationen

Maßnahmen der IT-Sicherheit/IT-Security müssen das Ziel haben, die IT-gestützten Geschäftsprozesse des Unternehmens abzusichern, d. h. vor Störungen zu schützen. Weniger von Bedeutung ist die Absicherung von IT-Systemen, die für die Geschäftsprozesse kaum relevant sind. Der Grad der notwendigen Informationssicherheit muss der Wichtigkeit der zu schützenden Informationen und der Priorität entsprechender Anwendungen angemessen sein.

Inwieweit dabei eine Erfassung der Bedeutung von Informationen möglich ist, hängt auch vom Wissen des Beurteilenden selber ab.[2]

Anhaltspunkte, welche Anwendungen als höher priorisiert zu betrachten sind, können etwa sein, wenn Anwendungen[3]

- für zeitkritische oder vertrauliche Geschäftsprozesse genutzt werden
- unter spezieller Produktionsüberwachung stehen
- eine vergleichsweise große Zahl von Anwendern haben

Die notwendige Sicherheit aufgrund der Wichtigkeit der zu schützenden Objekte steigt mindestens linear an, d. h., die Sicherheitsanforderungen werden entsprechend der den zu schützenden Objekten beigemessenen Wichtigkeit ansteigen.

Bei der IT-Sicherheit von Informationssystemen geht es darum, Auswirkungen möglicher Ausfälle der Systeme in Form von Unterbrechungen in der Versorgung mit (auf den entsprechenden Informationssystemen basierenden bzw. durch diese zur Verfügung gestellten)

[1] vgl. Reichmann, Thomas (1993), S. 250
[2] vgl. Gössinger, Ralf (2005), S.86
[3] vgl. Hirch, Axel/Rahmel, Jürgen (2005):, S.8

Leistungen bzw. Services zu vermeiden. Kern der Problematik der IT-Sicherheit von Informationssystemen ist weniger, wenn z. B. die dahinter stehenden kritischen Infrastrukturen angegriffen oder sensible Geschäftsinformationen ausgespäht werden. Übergeordnetes Ziel ist die Gewährleistung der Versorgungssicherheit.

So fokussieren z. B. die Anforderungen für Technische Schutzmaßnahmen nach § 87 Telekommunikationsgesetz auf die Gewährleistung der Verfügbarkeit von Telekommunikationsanlagen, die dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten dienen. Die Anforderungen betreffen Personal, Organisation sowie die eingesetzte Technik. Sie sind so gestaltet, dass durch die zu ihrer Erfüllung ergriffenen Schutzmaßnahmen eine "dem Stand der Technik und internationalen Maßstäben" entsprechende "angemessene Standardsicherheit" für die in der Vorschrift genannten Schutzziele erreicht wird.

Hierauf müssen alle präventiven Tätigkeiten und sog. virtuellen Schutzmaßnahmen abzielen. Damit verbundene Überlegungen sind im Bereich der Risikovorsorge (Vermeidung von Versorgungsausfällen) anzusiedeln.[1]

Bemerkenswert an dem Anforderungskatalog für technische Schutzmaßnahmen nach § 87 Telekommunikationsgesetz (TKG) ist, dass er die Kriterien zur Beurteilung des Verlusts der Verfügbarkeit einer technischen Einrichtung vorgibt: Ob der Verlust der Verfügbarkeit zu einer erheblichen Beeinträchtigung führt, soll anhand der möglichen Schadensauswirkung für die Allgemeinheit beurteilt werden, und zwar anhand der Ausfalldauer, die Anzahl der betroffenen Nutzer bei Ausfällen von Einrichtungen von öffentlichen Telekommunikationsnetzen, und der Bedeutung der betroffenen Telekommunikationsdienste.

Das Risiko möglicher Ausfälle der Systeme in Form von Unterbrechungen in der Versorgung mit Leistungen bzw. Services wird sicher am stärksten dadurch beeinflusst, wenn nicht der Wichtigkeit der zu schützenden Informationen und der Wichtigkeit der Geschäftsprozesse angemessene Maßnahmen/Schutzvorrichtungen der IT-Sicherheit/IT-Security implementiert werden. Des Weiteren werden Risiken determiniert durch die Stärke der Schutzvorrichtungen (Risiko I) sowie (dadurch, dass im Sinne einer Kettenreaktion andere Bedrohungen Schäden verursachen können, und/oder die entsprechenden Objekte als Ziel für potenzielle Angreifer interessanter werden) die Kritikalität bzw. Attraktivität der zu schützenden Objekte (in der Einschätzung der potenziellen Angreifer) (Risiko II).

Die Betrachtung von Risiken erfordert die Analyse der Zusammenhänge ihres Entstehens. Auswirkungen von Risikoereignissen stellen oft die Ursache für andere Risikoereignisse dar.

[1] vgl. Sonntag, Matthias (2005), S.15-18

Risikoereignisse und -ursachen bilden so in der Regel mehrgliedrige Wirkungsketten. Einzelne, als unwesentlich wahrgenommene Risikoereignisse können Ketten weiterer Risikoereignisse mit tief greifenden Auswirkungen auslösen. Für die Risikoanalyse ist es deshalb wichtig, die Stellen in den Geschäftsprozessen zu finden, die kritisch für die Fortführung der Geschäftstätigkeit sind[1] und mit entsprechenden Schutzmechanismen abgesichert werden können.

Schutzmechanismen werden als „stark" bezeichnet, wenn man bezüglich möglicher Angriffe keine guten Erkennungs- und Reaktionsgegenmaßnahmen benötigt. „Schwache" Schutzmechanismen erfordern dagegen bessere Erkennungs- und Reaktionsgegenmaßnahmen. Schwache Schutzmechanismen können oft durch gute Erkennungs- und Reaktionsmechanismen kompensiert werden. Dabei sind Erkennungsmechanismen ohne entsprechende Reaktionsmechanismen grundsätzlich nutzlos. Z. B. braucht man ein Einbruchmeldesystem erst gar nicht zu installieren, wenn der Angreifer weiß, dass niemand auf den Alarm reagiert.[2]

Risiken können durch noch so starke Schutzvorrichtungen aber nie völlig ausgeschaltet werden (Risiko I).

Auf Ebene der Risikopolitik ist dies die Aussage, dass der Grenznutzen risikopolitischer Maßnahmen mit zunehmendem Grad an Sicherheit abnimmt.[3] Äquivalent damit ist die Aussage, dass die Sicherheit (vor möglichen Ausfällen der Systeme in Form von Unterbrechungen in der Versorgung mit Leistungen bzw. Services) mit der Stärke der Schutzvorrichtungen nur unterproportional ansteigt.

Die Kritikalität der zu schützenden Objekte impliziert (wie oben bei der Wichtigkeit) mit der Kritikalität mindestens linear ansteigende Sicherheitsanforderungen. Nimmt man nun an, dass die bei gegebener Kritikalität sich ergebenden Sicherheitsanforderungen mit den notwendig starken Schutzvorkehrungen abgedeckt sind, und damit die der Stärke der Schutzvorrichtungen entsprechende Sicherheit gegeben ist (also Sicherheitsanforderungen = Sicherheit), so folgt, dass die notwendige Stärke der Schutzvorrichtungen mit der Kritikalität der zu schützenden Objekte überproportional ansteigt:

Mit dem obigen Verlauf von Risiko I in Abhängigkeit der Stärke der Schutzvorrichtungen folgt der Zusammenhang zwischen Risiken determiniert durch die Stärke der Schutzvorrichtungen und der Kritikalität der zu schützenden Objekte. Bei größerer Kritikalität werden potenziell stärkere Schutzvorkehrungen, größere Risiken sind nicht akzeptabel.

[1] vgl. Romeike, Frank (2004), S.155156
[2] vgl. Schneier, Bruce (2000), S.270-272
[3] vgl. Ibers, Tobias (2005), S.51

Die zweite Implikation der Kritikalität der zu schützenden Objekte sind mit der Kritikalität überproportional ansteigende Risiken (dadurch, dass im Sinne einer Kettenreaktion andere Bedrohungen Schäden verursachen können, und/oder die entsprechenden Objekte als Ziel für potenzielle Angreifer interessanter werden). Wird dies mit dem obigen Zusammenhang überlagert,

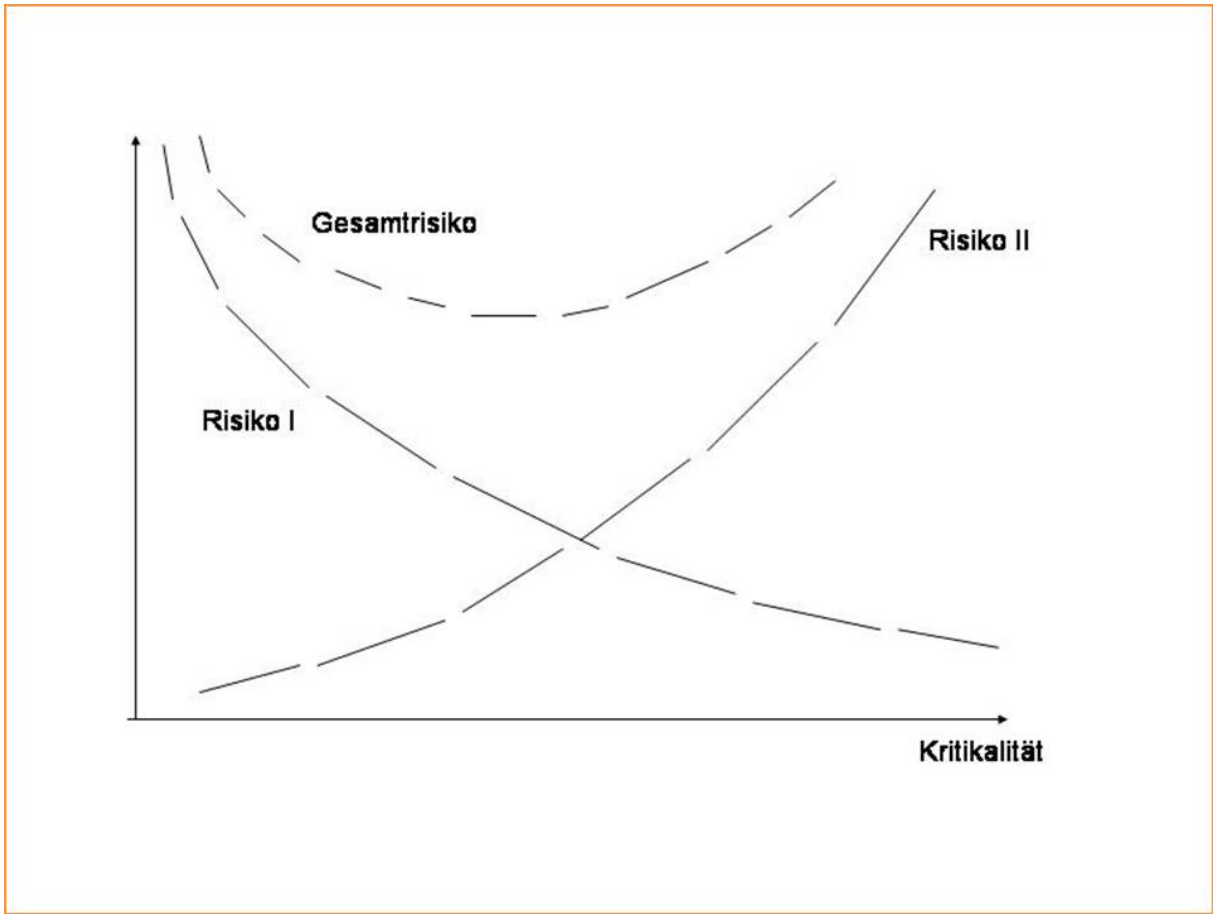


Abb. 6 *Gesamtrisiko in Abhängigkeit der Kritikalität der zu schützenden Objekte*

so ergibt sich theoretisch ein Minimum für das Gesamtrisiko in Abhängigkeit der Kritikalität. Dieses Gesamtrisiko wird einerseits durch stärkere Schutzmechanismen bei steigender Kritikalität verringert, und andererseits steigt es bei höherer Kritikalität dadurch, dass im Sinne einer Kettenreaktion andere Bedrohungen Schäden verursachen können, und/oder die entsprechenden Objekte als Ziel für potenzielle Angreifer interessanter werden, wieder an.

Ein ähnlicher Verlauf ergibt sich bei Überlagerung der Kostenkurven für Sicherheitsmaßnahmen mit denen für potenzielle Schäden.[1] Durch ein ausgewogenes Verhältnis von Präventivkosten und Schadenskosten können die Risikokosten (als Summe aus Präventivkosten und Schadenskosten) minimiert werden. Durch den verstärkten Einsatz präventiver

[1] vgl. Romeike, Frank (2004), S.254

Schadenverhütungsmaßnahmen kann der Grad an Sicherheit erhöht, und damit eine Reduzierung der Schadenskosten erreicht werden. Ein wirtschaftlich optimaler Grad an Sicherheit liegt vor, wenn bei einer weiteren Erhöhung der Präventivkosten die dadurch erzielte Senkung der Schadenkosten zu keiner weiteren Reduzierung der Risikokosten mehr führt.[1] Dies soll jedoch nicht weiter untersucht werden, da potenzielle Schäden für Risiken der IT-Sicherheit aufgrund der Dynamik der technologischen Entwicklung und immer ausgefeilterer Methoden potenzieller Angreifer kaum sinnvoll betrachtet werden können.

Für Überlegungen zu einer angestrebten Minimierung des Gesamtrisikos bei gegebener Kritikalität wäre es interessant, ob der Verlauf des Gesamtrisikos beeinflussbar ist, sodass bei gegebener Kritikalität der zu schützenden Objekte das Gesamtrisiko minimiert wird.

Risiko I ist dadurch bedingt, dass bei kleiner Kritikalität tendenziell weniger starke Schutzvorrichtungen implementiert werden. Der Verlauf des Gesamtrisikos ist mit dem Ziel, dass bei größerer Kritikalität der zu schützenden Objekte das Gesamtrisiko minimiert wird, dann durch Abflachung des Verlaufs von Risiko II beeinflussbar:

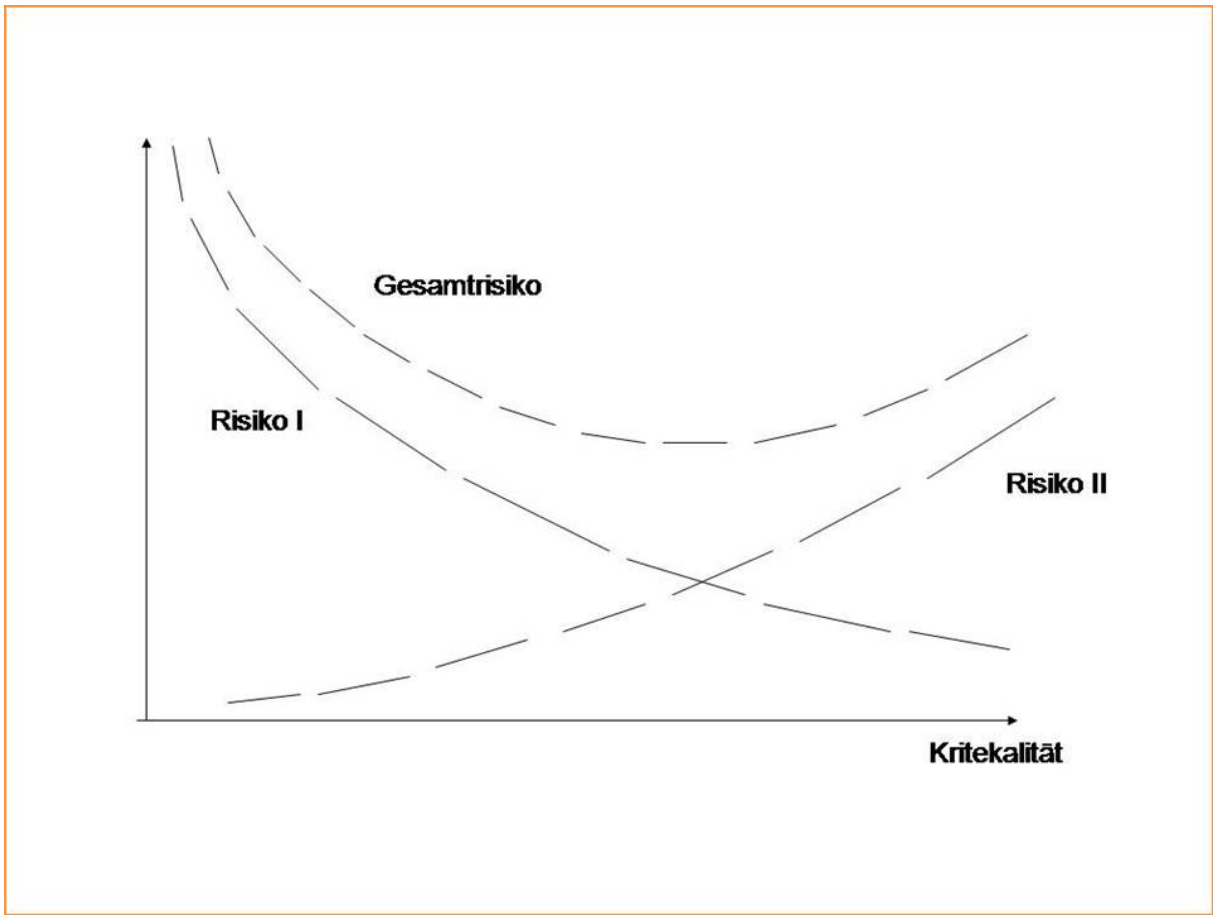


Abb. 7 Minimierung des Gesamtrisikos

[1] vgl. Dahmen, Jörn (2002), S.18

Risiko II wird dadurch determiniert, dass im Sinne einer Kettenreaktion andere Bedrohungen Schäden verursachen können, und/oder die entsprechenden Objekte als Ziele für potenzielle Angreifer interessanter werden. Das Risiko möglicher Ausfälle der Systeme in Form von Unterbrechungen in der Versorgung mit (auf den entsprechenden Informationssystemen basierenden bzw. durch diese zur Verfügung gestellten) Leistungen bzw. Services, kann dadurch minimiert werden, dass Abhängigkeiten zwischen verschiedenen Bedrohungen, Kausalketten reduziert werden.

Die zweite Möglichkeit („Mitakteure“ dürfen nicht auf Strategieänderungen anderer reagieren, was insbesondere bei völliger Unkenntnis anderer über die eigenen Ziele zutrifft) entspricht dem Ansatz bei der Bewertung potenzieller IT-Sicherheitsvorfälle mithilfe der ordinalen Risikobewertung: Der potenzielle Eintritt entsprechender Einbruchsszenarien wird dort nicht nur von den eingesetzten Computer-/Betriebs-/Netzwerksystemen, der bestehenden Infrastruktur und Sicherheitsvorkehrungen, sondern auch von weichen Faktoren wie Attraktivität des Unternehmens als Angriffsziel für Angreifer und Integrität/Sicherheitsbewusstsein der Mitarbeiter abhängig gemacht.[1] Neben einem entsprechenden Motiv und hinreichender „krimineller Energie“ gilt hinreichende Sachkenntnis über das Unternehmen und de Arbeitsprozesse als Tatvoraussetzung für kriminelle Handlungen.[2]

Aus diesen Überlegungen ergibt sich als Aufgabe für das IT-Risikomanagement als wichtigem Bestandteil des operativen IT-Security-Managements:

- der Wichtigkeit der zu schützenden Informationen und der Priorität entsprechender Anwendungen angemessene Sicherheitsmaßnahmen zu evaluieren,
- Abhängigkeiten zwischen verschiedenen Bedrohungen, Kausalketten sowie die Attraktivität des Unternehmens als potenzielles Angriffsziel für Angreifer zu reduzieren. Die Komplexität dieser Abhängigkeiten kann durch die sog. lose Kopplung reduziert werden. Diese lose Kopplung wird bezüglich der Integration der im Unternehmen eingesetzten IT-Lösungen und der unternehmensübergreifenden Datenintegration mittels einer Service-orientierten Architektur (SOA) unterstützt, wo die Anwendungslandschaft aus lose gekoppelten Anwendungsbausteinen mit klar modellierten Schnittstellen besteht, die über wohl definierte Services miteinander kommunizieren. Das Entstehen einer Bedrohung bzw. eines Risikos wird mit Hilfe

[1] vgl. Kyas, Ottmar (2000), S.29
[2] vgl. Bosse, Richard/Scholz,Wolfgang (2007), S.8

von Ursache-Wirkungsketten aufgezeigt, an dessen Ende ein Ereignis steht, das unmittelbar die Prozesse im Unternehmen schädigen oder stören kann.

Insgesamt soll als wichtigstes Ziel die Fähigkeit von Geschäftsvorgängen, Organisationen und technischen Systemen unterstützt werden, bei unvorhergesehenen Ereignissen das Geschäft fortzuführen und vor Schaden zu bewahren.

Das Steuern und Überwachen der Risiken bedingt die Einbeziehung sämtlicher wechselseitig wirkender Ursache-Wirkungs-Beziehungen der Einzelrisiken [1] Ursache-Wirkungs-Beziehungen, die wichtige Hinweise für die Risikosteuerung geben, können analysiert werden, indem man die positionierten Risiken einer Szenario- und Sensitivitätsanalyse unterzieht.

Wichtig ist auch das Management des Risikos, dass nicht die vom IT-Risikomanagement evaluierten (der Wichtigkeit der zu schützenden Informationen und der Wichtigkeit der Geschäftsprozesse angemessenen) Maßnahmen/Schutzvorrichtungen der IT-Sicherheit/IT-Security implementiert werden. Zunächst wird jedoch untersucht, was für das IT-Risikomanagement Voraussetzung ist, um (der Wichtigkeit der zu schützenden Informationen und der Priorität entsprechender Anwendungen) angemessene Sicherheitsmaßnahmen strukturiert zu evaluieren: Schutzkonzepte für die IT-Komponenten und IT-sicherheitsstrategische Konzepte, in der die IT-Komponenten eingeordnet werden können.

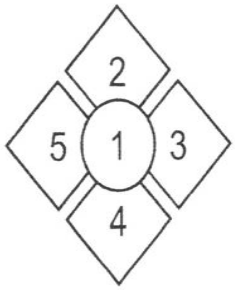
3.2 Formulierung IT-Sicherheitsstrategie bezogener Schutzkonzepte auf Typusebene (IT-Ressourcen) bzw. Objektebene (IT-Objekte)

Anhand einer Schutzbedarfsanalyse werden die aus der Sicherheitspolitik des Unternehmens abgeleiteten Sicherheitsziele der Geschäftsprozesse ermittelt. [2] Die Ressourcen der Informationsverarbeitung Personal, Hardware, Software, Daten begründen dabei Gefährdungen der unterstützten Geschäftsprozesse.[3] Anhand der Schutzbedarfsanalyse erfolgt die Erhebung der Sicherheitsziele der verschiedenen Informationssysteme.[4]

Die IT-Objekte, die innerhalb der IT auf strategischer, planaerischer und operativer Ebene gesteuert und gestaltet werden, können z. B. in: 1. IT-Management-Prozess, 2. IT-Organisation, 3. Information, 4. Informations- und Kommunikationssysteme einschließlich

[1] vgl. Kirchner, Michael (2002), S.18
[2] vgl. Müller, Klaus-Rainer (2003), S.19
[3] vgl. Krcmar, Helmut/Junginger, Markus (2003), S.251
[4] vgl. Müller, Klaus-Rainer (2003), S.47

der erforderlichen Infrastruktur für diese Systeme und 5. IT-Wertbeitrag für das Unternehmen eingeteilt werden. Gleichzeitig sind dies IT-Objektbereiche, denen konkretere IT-Objekte zugeordnet werden können:[1]



- IT-Management Prozess (inkl. IT-Governance)
- IT-Organisation (vgl. COBIT IT Resources)
- Information (vgl. COBIT Information Criteria)
- Informations- und Kommunikationssysteme inkl. die erforderliche Infrastruktur für diese Systeme (vgl. COBIT IT Resources)
- IT-Wertbeitrag für das Unternehmen (IT-Value Management)

(Quelle: Dietrich, Lothar (2004), S.27)

Abb. 8 Fünffelder-Modell IT-Objektbereiche

Zwecks Sicherstellung der erforderlichen Qualität, Sicherheit und Ordnungsmäßigkeit des Informatikeinsatzes kann für jeden IT-Objektbereich ein umfassendes und revisionsfähiges Informations-Management-System konzipiert werden.

Die Erarbeitung diesbezüglicher Schutzkonzepte klassifiziert die verwendeten IT-Systeme und Datenbestände nach ihrer Bedeutung für das Unternehmen. Sie läuft klassischerweise in den Phasen Sicherheitsanalyse (Ermittlung der Schutzbedürftigkeit der Geschäftsprozesse und damit der Schutzbedürftigkeit der von ihnen verwendeten IT-Systeme und Datenbestände) und Risikoanalyse (zur Bestimmung der für die erforderliche IT-Sicherheit zu ergreifenden IT-Sicherheitsmaßnahmen), welche eine Schwachstellenanalyse und Bedrohungsanalyse enthält, ab.

Die aus der Sicherheitsanalyse resultierende Schutzbedarfsfeststellung ist Grundlage für die Bewertung der identifizierten Risiken. Diese Bewertung fließt in die Priorisierung der umzusetzenden Maßnahmen/Maßnahmenplanung ein. Diese Maßnahmenplanung ermittelt die zur Vermeidung oder Verminderung eines nicht-akzeptablen Risikos geeigneten Maßnahmen. Hieraus ergibt sich (über alle betrachteten Schutzobjekte hinweg) der Risikobehandlungsplan, der Grundlage für die Umsetzungsphase ist.

[1] vgl. Dietrich, Lothar (2004), S.27

Am Anfang der Planungen zur Umsetzung des Grundschutzprozesses wird die gesamte Informations- und Kommunikationstechnologie erhoben und strukturiert: [1] Dabei wird die gesamte technische Umgebung des Unternehmens betrachtet. Zur Abbildung dieser Strukturerhebung werden sog. IT-Verbünde (organisatorisch klar abgrenzbare Mengen aller zur Ausführung einer Geschäftsaufgabe oder eines Geschäftsprozesses notwendigen IT-Objekte) gebildet, die die IT-Umgebung des gesamten Unternehmens bilden (z. B. kaufmännische Verwaltung, Administration, Produktionsbetrieb, IT-Betrieb). Kriterium zur Bildung der IT-Verbünde ist, dass diese substanziell zum Funktionieren der Organisation beitragen müssen. Als Modell der IT-Verbünde werden in der sog. IT-Strukturanalyse die Netzwerke mit ihren Komponenten, die IT-Systeme und Anwendungen erhoben und gruppiert. Die IT-Strukturanalyse soll alle in das Schutzkonzept einzubeziehenden IT-Objekte erfassen. Dies ist Grundlage für die Feststellung des Schutzbedarfs, wobei immer zunächst der Schutzbedarf einer Anwendung anhand der von ihr verarbeiteten Daten objektiv ohne Blick auf mögliche Schadensfolgen bestimmt wird.

Dabei soll die Einordnung der Systeme in Schutzbedarfskategorien anhand „messbarer" Kriterien erfolgen und nachvollziehbar sein. Bei der Bildung operationalisierbarer Maßstäbe für diese Kategorien sind Schadensszenarien (z. B. Verstöße gegen Gesetz, Vorschriften oder Verträge, Beeinträchtigungen des informationellen Selbstbestimmungsrechts, Beeinträchtigungen der persönlichen Unversehrtheit, Beeinträchtigungen der Aufgabenerfüllung, negative Außenwirkung, finanzielle Auswirkungen) zu bewerten, wobei ein Schadensfall mehrere Schadensszenarien betreffen kann.

Die Festlegung des Schutzbedarfs ist für jeden der Aspekte der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) durchzuführen. Die Schutzbedarfe der Anwendungen werden dann auf die IT-Objekte übertragen. Dabei werden nach den Anwendungen die zugehörigen Systeme und dann die Infrastrukturkomponenten betrachtet. Bei der Übertragung des Schutzbedarfs der IT-Anwendungen auf die IT-Systeme sind das Maximumprinzip, die Abhängigkeiten, der Kumulationseffekt und der Verteilungseffekt zu berücksichtigen. Das Maximumprinzip besagt, dass der höchste Schutzbedarf aller Anwendungen für ein IT-System maßgeblich ist. Mit Abhängigkeiten ist gemeint, dass eine Anwendung X mit großer Bedeutung auf die Ergebnisse einer Anwendung Y mit niedriger Bedeutung angewiesen ist. In diesem Fall muss auch die Bedeutung der Anwendung Y angeglichen werden. Beim Kumulationseffekt ist darauf zu achten, ob mehrere kleine Schutzbedarfe einen größeren zur Folge haben können. Der Verteilungseffekt bezieht sich auf Systeme, deren Schutzbedarf niedrig ist, obwohl eine Anwendung mit hohem Schutzbedarf darauf ausgeführt wird, sodass bei einem Ausfall des

[1] vgl. Humpert, Frederik (2005), S.36-47

Systems nicht die ganze Anwendung betroffen ist. Der Verteilungseffekt kann nur dann angewandt werden, wenn es um die Verfügbarkeit von Systemen geht. Vertraulichkeit und Integrität verteilen sich nicht, da die Daten bezüglich dieser Grundaufgaben die gleichen Anforderungen an jedes System stellen. Nach Abschluss der Strukturanalyse und der Schutzbedarfsfeststellung werden die einzelnen Komponenten des IT-Verbundes im Schichtenmodell den einzelnen Bausteinen des Grundschutzhandbuchs zugeordnet. Dieses Modell soll alle relevanten und notwendigen Punkte für die Beschreibung des eigenen IT-Umfelds enthalten. Die Schichten im Grundschutzmodell sind „Übergeordnete Aspekte“, „Infrastruktur“, „IT-Systeme“, „Netze“ und „Anwendungen“.

Durch diese Modellierung wird die Komplexität des IT-Verbundes reduziert. Die Aufteilung in einzelne Bausteine und kleine Teile ermöglicht leicht Aktualisierungen. Dies kommt dem entgegen, dass Sicherheit ständiger Kontrolle und Revision bedarf. Durch eindeutig definierte Modell- und Objekttypen sowie die Festlegung möglicher Beziehungstypen wird ähnlich wie in ARIS die Grundlage für eine methodisch fundierte Vorgehensweise gelegt, welche in wesentlichen Teilen durch automatische Prüfungen überwacht werden kann. Durch Modellierung in Sichten wird dabei eine deutliche Reduzierung der Komplexität bei der Modellerstellung und –pflege erreicht. Grundlage für eine möglichst redundanzfreie und ganzheitliche Modellierung bildet die Sichtenintegration, in der Modellelemente der unteren Sichten in der obersten Sicht integriert und alle Modellelemente in einer gemeinsamen Datenbasis integriert werden.

In den Bausteinen des Grundschutzhandbuchs werden nach der allgemeinen Beschreibung des betrachteten IT-Objekts typische Gefährdungslagen (wie sie unter den Voraussetzungen des Grundschutzhandbuchs auf diese Systeme zutreffen) dargestellt. Die Gefährdungslage bezieht sich auf den Gefährdungskatalog des Grundschutzhandbuchs, die alle typischen Gefährdungen eines IT-Objekts auflisten: Höhere Gewalt, organisatorische Mängel, menschliches Fehlverhalten, technisches Versagen, vorsätzliche Handlungen.

Oft wird es als zu aufwendig erachtet, die gesamte Informations- und Kommunikationstechnologie zu erheben und zu strukturieren. Die Schutzbedarfsfeststellung kann dann auf einer Erhebung der relevanten (im Sinne von Wichtigkeit/Kritikalität für das Unternehmen bedeutenden) Schutzobjekte bzw. der als besonders sensitiv/risikobehaftet erachteten Anwendungen sowie einer unternehmensspezifischen Schutzbedarfsskala basieren. Schutzobjekttypen sind z. B. Informationen, Anwendungen, IT-Systeme, Räume, Leitungen und Verbindungen. Von den (für die wichtigsten Geschäftsprozesse) benötigten Anwendungen

ausgehend, werden die von diesen verarbeiteten Informationstypen ermittelt auf Ebene z. B. der Herkunft oder des Verwendungszwecks.

Jede der drei Grundanforderungen der IT-Sicherheit wird in der Praxis (abhängig z. B. von den jeweiligen Informationstypen) einen unterschiedlich großen Schutzbedarf erfordern, der im Rahmen einer Schutzbedarfsanalyse definiert und dokumentiert werden muss. Für jedes Schutzobjekt ist daher für jede der Komponenten „Verfügbarkeit", „Integrität" und „Vertraulichkeit" eine Abschätzung potenzieller Folgen eines möglichen Sicherheitsvorfalls vorzunehmen und auf einer Schutzbedarfsskala in die Klassen „niedrig/mittel", „hoch" und „sehr hoch" einzuordnen. Bewertungskriterien dafür können etwa aus den Bereichen „Verstöße gegen Gesetze", „Behinderung von Geschäftsprozessen" oder „finanzielle Auswirkungen" kommen.[1]

Objektiviertes Kriterium zur Beurteilung der Wichtigkeit/Kritikalität der für das Unternehmen relevanten Schutzobjekte bzw. der als besonders sensitiv/risikobehaftet erachteten Anwendungen ist im Zusammenhang mit dem strategischen Ansatz der Grad des Einflusses für das Erreichen der Zieldimensionen des IT-Security-Prozesses. Diese Einflussfaktoren sind auch die notwendige Verlässlichkeit und Beherrschbarkeit entsprechender Systeme und Anwendungen, sofern von diesen die korrekte Umsetzung der IT-Security-Strategie abhängt. Die Wichtigkeit/Kritikalität der Schutzobjekte bezieht sich (in dem im Folgenden zu entwickelnden Modell der Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in den Kontext Handlungsbefähigung trotz Unsicherheit) auf die Zielgegenstände des strategischen IT-Security-Managements. Dies sind die mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens.

Der oft sehr kurze Lebenszyklus moderner, hoch komplexer IT-Produkte und Gesamtlösungen bedingt aber zumeist, dass eine derartige Erarbeitung des individuellen Sicherheits- bzw. Schutzkonzepts nicht rechtzeitig abgeschlossen werden kann bzw. zu aufwendig ist. Um den erforderlichen Gesamtaufwand zu minimieren, wird auf eine umfassende Sicherheitsanalyse verzichtet und direkt eine Bewertung (Evaluation) der Sicherheit eines IT-/IV-Systems zur Einordnung in eine vorgegebene oder gewünschte Schutzklasse vorgenommen. Grundlage der Evaluierung sind dabei die Anforderungen an das zu bewertende Produkt.

Eine solche Einordnung kann mithilfe der CC (Common Criteria)/ISO/IEC 15408 erfolgen. Herstellern von IT-Systemen, IT-Produkten und IT-Komponenten wird ein Beurteilungsraster

[1] vgl. Hirch, Axel/Rahmel, Jürgen (2005):, S.7-10

geliefert, mit dem sie die Entwicklung bzw. Weiterentwicklung und Pflege ihrer Produkte so gestalten können, dass diese über definierte Sicherheitseigenschaften verfügen und dass das Vorhandensein solcher Eigenschaften für Dritte nachvollziehbar wird. Dazu werden funktionale und qualitative Anforderungen an die Untersuchungsgegenstände definiert. Die funktionalen Anforderungen betreffen dabei das Vorhandensein und die Ausprägung bestimmter technischer Funktionen, mit deren Hilfe sichere Systeme aufgebaut werden können. Die qualitativen Aspekte beziehen sich auf die Korrektheit der realisierten Funktionen und andererseits auf die Wirksamkeit vorgesehener Schutzmaßnahmen.

Es ist ein individueller Aufbau der Sicherheitsbeschreibung in Form einer Zusammenstellung verfeinerbarer und veränderbarer Anforderungsblöcke möglich, sodass Entwickler wie Nutzer speziell für den Evaluationsgegenstand angepasste Sicherheitsanforderungen vorgeben können. Aus den Annahmen zur Einsatzumgebung, den Bedrohungen und der organisatorischen Sicherheitspolitik werden in einem iterativen Prozess der Sicherheitsbedarf und daraus die Sicherheitsziele definiert. Zu den Sicherheitszielen werden dann als Sicherheitsanforderungen aus dem in den Common Criteria Kapitel 2 und 3 vorgegebenen Katalog die Functional Requirements und Assurance Requirements abgeleitet.

Die Anforderungen an die Funktionalität sowie an die Qualität werden jedoch in sog. Schutzprofilen (Protection Profiles) zusammengefasst. Diese werden mit einem ausführlichen Beschreibungsteil ergänzt, in dem u. a. ein vorhandenes Sicherheitskonzept beschrieben wird, und die Bedrohungen den Anforderungen gegenübergestellt werden. Der Nutzer spezifiziert durch diese Protection Profiles seine Sicherheitsanforderungen an ein Produkt. Der Entwickler erklärt und beschreibt die produktspezifische Umsetzung der Anforderungen in den sog. IT-Sicherheitszielen (Security Targets).

Ein Protection Profile (PP) ist ein möglichst wiederverwendbares Anforderungsprofil für eine Gruppe von Produkten und/oder Anwendungen, unabhängig von der späteren Umsetzung und Einsatzumgebung. Es beschreibt die Anforderungen an die Funktionalität und Qualität bezogen auf ein Sicherheitsproblem für ein späteres Produkt oder System. Ein ausführlicher Beschreibungsteil erläutert das Sicherheitskonzept und stellt die Bedrohungen den Anforderungen gegenüber. Solche Schutzprofile helfen dem Anwender, seinen Sicherheitsbedarf zu bewerten. Zu Beginn der Evaluierung werden die Sicherheitsanforderungen des Profils in spezielle Sicherheitsvorgaben (Security Targets) überführt. Dazu kommen vor allem Beschreibungen der Einsatzumgebung.[1]

[1] vgl. PC-Welt (2004), S.55

Die Security Targets (ST) sind gedacht für den Hersteller zur produktspezifischen Umsetzung der Sicherheitsanforderungen, für den Prüfer/Zertifizierer als Bewertungsgrundlage und Evaluationsgegenstand, für den Nutzer als Rückschluss zu seinen Anforderungen.

Der ISO Guide für die Erstellung von Protection Profiles (PP) und Security Targets (ST) (PD ISO/IEC TR 15446:2004 Information Technology Security techniques Guide for the Production of Protection Profiles and Security Targets) gibt Hinweise für die Entwicklung der PP und ST. Der Guide ist aber kein offizielles Dokument zur Registrierung, Prüfung und Zertifizierung von PP, ST und Produkten. Der Guide gibt nützliche Hinweise und Erklärungen, hauptsächlich für den Ersteller von PP und ST.

Die Erstellung von Schutzprofilen und IT-Sicherheitszielen nach den Common Criteria wird durch ein frei verfügbares Werkzeug, die CC-Toolbox, unterstützt. Dieses Werkzeug stellt die Common Criteria in retrievalfähiger Form bereit, ermöglicht definierte Konsistenz- und Vollständigkeitsprüfungen und unterstützt die Erzeugung von Evaluationsdokumenten durch Generierung von prototypischen Berichten.[1]

3.3 Einordnung der IT-Ressourcen und IT-Objekte in IT-sicherheitsstrategische Konzepte

Die Komponenten der IT-Strategie beziehen sich auf die physischen Objekte Hardware, Software, Netze und Personal und logische Objekte wie Informationssysteme, Datenbanken, Kommunikationsbeziehungen sowie Konzepte wie Vorgehensmodelle, Systementwicklungsmethoden, Richtlinien für den Werkzeugeinsatz.[2]

Mit IT-sicherheitsstrategischen Konzepten seien z. B. Vorgehensmodelle, Systementwicklungsmethoden, Richtlinien für den Werkzeugeinsatz gemeint, die über die Sicherheitsschutzziele definierte Konzepte darstellen. Diese dienen dem operativen und strategischen IT-Sicherheitsmanagement als Orientierungshilfen zur Ausgestaltung und Bewertung der IT-Sicherheit. Die Einordnung der IT-Ressourcen und IT-Objekte in diese Konzepte kann über die funktionale Sicht auf die IT-Systeme erfolgen, welche die entsprechenden IT-Ressourcen benutzen, bzw. mit den entsprechenden IT-Objekten modelliert werden können.

[1] vgl. Initiative D21 e.V. (2002),, S.26
[2] vgl. Hasenkamp, Ulrich (2003), S.206,208

Produktfunktionen werden in die Kategorien Zugang (Schnelligkeit, Auffindbarkeit…), Nutzung (Bedienbarkeit, Übersichtlichkeit…), Inhalt (Aktualität, Vielfalt, Serviceangebot…) und Kommunikation (z. B. Antwortgeschwindigkeiten) unterteilt.[1]

Bezüglich der Kommunikation wird z. B. eine umfassende Ende-zu-Ende Sicherheit bei gleichzeitiger Verringerung der Verwundbarkeit und Steigerung der Effizienz von IT-Security-Strukturen verlangt. Zentralisierte Sicherheitslösungen, die zentralisierte Komponenten wie Gültigkeitsprüfung von Zertifikaten oder Sets zur Schlüsselwiederherstellung nutzen, erfüllen für viele Unternehmen nicht mehr die Bedürfnisse heutiger Organisationsprozesse.

So kann man sich bei der Ausgestaltung der IT-Sicherheit z. B. am Ziel der Gewährleistung der Datensicherheit orientieren: Der IDW-Prüfungsstandard 330 definiert Datensicherheit im Sinne der GoBS über die Sicherheitsschutzziele Verfügbarkeit und Integrität. Im Grundschutzhandbuch des BSI kommt als Schutzziel die Vertraulichkeit von Informationen (im Sinne von Daten) hinzu, die für die externe Revision aber weniger relevant ist.

DIN 44300 Teil 1 definiert Datensicherheit als „Sachlage, bei der Daten unmittelbar oder mittelbar so weit wie möglich vor Beeinträchtigung und Missbrauch bewahrt sind, und zwar unter Berücksichtigung verarbeitungsfremder Risiken wie auch im Verlauf auftrags- und ordnungsgemäßer Erbringung einer Datenverarbeitungsleistung“.

Datensicherung und Datenwiederherstellung sind auf die Gewährleistung der physischen Unversehrtheit und der Integrität der auf beliebigen Speichermedien gespeicherten Daten bzw. Software ausgerichtet. Die physische Unversehrtheit ist zerstört, wenn Datenträger bzw. die auf ihnen gespeicherten Daten einschließlich Software nicht mehr gelesen bzw. fehlerfrei verarbeitet werden können. Die Integrität der auf Speichermedien gespeicherten Daten ist gestört oder zerstört, wenn die Daten zwar lesbar, aber nicht aktuell, richtig oder vollständig sind, gelöscht bzw. überschrieben wurden bzw., sofern es sich um Software handelt, diese nicht die erwartete Funktionalität besitzt, es sich beispielsweise um eine falsche Version handelt.

Die Verfahren der Datensicherung und Datenwiederherstellung müssen auf die Spezifik der Datenträger und der Risiken, denen die auf ihnen gespeicherten Daten ausgesetzt sind, ausgerichtet sein. Das Maßnahmenbündel für den Bereich "Datensicherungskonzept" wird unterteilt in Maßnahmen zur Notfallvorsorge und zur Organisation der Datensicherung.

[1] vgl. Stoi, Roman (2002), S.163

Als Beispiel für eine operative Bewertung der IT-Sicherheit sei das Konzept der EAL-Stufen der Common Criteria (ISO 15408) genannt. Diese wird als Common Evaluation Methodology bezeichnet. EAL-Stufen definieren eine Stufe der Vertrauenswürdigkeit (Evaluation Assurance Level) in eine Sicherheitsleistung:

Eine Common Criteria -Evaluierung soll die Wirksamkeit der vom Hersteller behaupteten Sicherheitsfunktionalität bestätigen. Die EAL-Stufen beschreiben dazu präzise Anforderungen an eine IT-Sicherheitsprüfung. Da die Wirksamkeit der Sicherheitsleistung insbesondere durch das Ausnutzen vorhandener Schwachstellen bedroht ist, ist bei allen Evaluierungsaspekten die Analyse der Schwachstellen ein zentrales Prüfziel. Mit wachsenden EAL-Stufen müssen zunehmend komplexer ausnutzbare Schwachstellen abgedeckt werden. Eine höhere EAL-Nummer bedeutet höhere Anforderungen an den zu prüfenden Umfang, an die Prüftiefe und an die Prüfmethoden. Daher macht das Vorgehen Sinn, mit niedrigeren EAL-Stufen den Evaluierungsprozess zu starten. Darauf aufbauend kommt für die nächsthöheren EAL-Stufen zusätzlicher Prüfaufwand hinzu. Eine niedrigere EAL-Stufe kann vom Prüfumfang her also als Untermenge des Prüfaufwandes der höheren Stufen betrachtet werden.[1] [2]

Im Zusammenhang mit der gegebenen Thematik steht der Umgang mit strategischen Risiken der IT-Sicherheit im Mittelpunkt der Überlegungen zu IT-sicherheitsstrategischen Konzepten zur strategischen Ausgestaltung und strategischen Bewertung der IT-Sicherheit.

[1] vgl. BSI (2003)
[2] vgl. Collenberg, Thomas/Wolz Matthias (2005), S.79

4 Grenzen der Risikoprognose und Ansätze zur Einbeziehung nicht-antizipierbarer Risiken auf Ebene der operativen Bestandteile der ganzheitlichen IT-Security-Strategie bei der Ausgestaltung der IT-Security

Prognose wird definiert als „Vorhersage einer künftigen Entwicklung aufgrund kritischer Beurteilung des Gegenwärtigen“.[1] Prognose muss von Früherkennung abgegrenzt werden: Bei der Früherkennung steht der operative Kontrollaspekt im Vordergrund. Sich abzeichnende Entwicklungen sollen möglichst umgehend entsprechende Maßnahmen einleiten. Die Prognose bezieht sich dagegen auf den strategischen Planungsaspekt: auf der Basis von Prognosen sollen Planungen für Maßnahmenalternativen ermöglicht werden.[2] Erschwert wird dies dadurch, dass es wegen positiver Informationskosten nicht immer optimal ist, möglichst exakte Informationen zu beschaffen und zu verarbeiten. Der Nutzen der Informationen muss gegen ihre Kosten abgewogen werden, u. U. muss die Planung mit ungenauen Informationen arbeiten.[3]

Die Voraussagbarkeit zukünftiger Ereignisse hängt dabei vom Wissen und den Kenntnissen des Voraussagenden ab: den Kenntnissen von Zusammenhängen, den sogenannten Ursache-Wirkungs-Beziehungen und von relevanten Informationen bezüglich des Vorliegens der Voraussetzungen zum Ablauf dieser Ursache-Wirkungs-Ketten. Mit den erforderlichen Kenntnissen erscheinen Ereignisse, die ohne diese Kenntnisse als zufällig erscheinen, möglicherweise deterministisch. Als deterministisch bezeichnet man ein Ereignis, das mit Sicherheit eintreten wird, als zufällig ein Ereignis, das lediglich eintreten kann.[4]

Wirtschaftlicher und technischer Fortschritt bezüglich Geschäftsprozessen hat immer die Bedingung zu erfüllen, dass die entsprechenden Aktivitäten, Arbeiten oder Tätigkeiten zur Erstellung eines Produkts oder einer Dienstleistung nachvollziehbar, nach gewissen Regeln, pünktlich und berechenbar mit möglichst geringem Einsatz von Produktionsfaktoren durchgeführt werden sollen.[5] Im Alltag und im Wirtschaftsleben gibt es jedoch Konstellationen oder Interaktionen, die für uns nicht durchschaubar sind. Daraus gehen nichtlineare, chaotische Effekte hervor.[6] Diese begründen Unsicherheit, Ungewissheit und Risiken.

[1] vgl. Stahlknecht, Peter (2003), S.16
[2] vgl. Ibers, Tobias (2005, S.85
[3] vgl. Bischof, Jürgen (2002), S.56,57
[4] vgl. Finke, Robert (2005), S.15,16
[5] vgl. Rosenkranz, Friedrich (2006), S.1
[6] vgl. Allenspach, Marco (2001), S.45

Sicherheit und Fortschritt wird durch Risiken belastet. Die Herausforderung besteht darin, den Zusammenhang zwischen unkalkulierbarer Zukunft und Risiko transparent zu machen.

Die Vorhersage zukünftiger (Schadens-)Entwicklungen wird durch Bildung möglichst großer Grundgesamtheiten möglich, die zumindest in der näheren Zukunft nur geringfügige Risiko-Abweichungen erwarten lassen.[1]:

Der Ursprung des Risikomanagements ist das Versicherungsmanagement, d. h. Risikoabwälzung durch Versicherung. Versicherungen versuchen den intransparenten Zusammenhang von unkalkulierbarer Zukunft und Risiko erwartbar zu machen (Normalisierungsfunktion).[2] Dies gelingt ihnen auf der Grundlage großer Grundgesamtheiten. Die erwartete zukünftige Schadensentwicklung lässt sich so im Prinzip auf vergangene Erfahrungen stützen, das versicherungseigene Risiko wird kalkulierbar.

Wenn jedoch Grundgesamtheiten in sensiblen Anwendungsfeldern wie komplexen Hochtechnologien durch Modellierung und Synthetisierung vieler kleiner Fehlerquellen fingiert werden müssen, ist die Bestimmung von Eintrittswahrscheinlichkeiten und Schadensverläufen nach dem Wahrscheinlichkeitskalkül auf dieser Basis sehr fragwürdig: Solche komplexen Technologien (wie z. B. die Atomkraft) sind mit nicht auszuschließenden immensen Schadensfunktionen verbunden und führen zu einer Auflösung des Zusammenhangs zwischen Versicherung und Risiko. Zentrales Merkmal dieser Risiken ist die Ungewissheit im Hinblick auf die Art möglicher Schäden und die Verursachung dieser Schäden dergestalt, dass (katastrophale) Auswirkungen solcher Schadensverläufe auf ihre eigenen Ausgangsbedingungen möglich sind.[3] Z. B. kann auch das IT-Risiko „Hoch- und Grundwassergefährdung“ im Katastrophenfall Systeme, Daten und anderweitige Schutzvorrichtungen zerstören. Letzteres kann im Sinne einer Kausalkette dazu führen, dass andere IT-Bedrohungen Schäden verursachen. Solche Systeme sind schlecht oder gar nicht kalkulierbar. Man kann mit ihnen für den Schadensfall keine verlässlichen Erfahrungen bilden.

Die stochastische Natur solcher Schadensereignisse macht eine Voraussage über ihr Eintreten unmöglich. Im Bereich der Wahrnehmung von seltenen Zufallsereignissen spielt die Wahrscheinlichkeit keine große Rolle: Die Zufälligkeit ist der eigentliche Risikofaktor.[4]

Durch die Einbeziehung von Risikominderungsmaßnahmen wurde das US-amerikanische Versicherungsmanagement zum Risk Management weiterentwickelt. Der Aufgabenbereich

[1] vgl. Japp, Klaus P. (2000), S.7
[2] vgl. Japp, Klaus P. (2000), S.9
[3] vgl. Japp, Klaus P. (2000), S.10
[4] vgl. Hölscher, Reinhold (2002), S.79

des nun als Risk Manager bezeichneten Verantwortlichen innerhalb eines Unternehmens wurde um die Koordination der Risikominderungsmaßnahmen erweitert.[1]

Moderne Risikofinanzierungsprodukte (Captives, Finite Risk Lösungen, Multi-line-multi-year Programme, Multi-Trigger-Produkte, Risk Securisation,…) überwinden den Dualismus zwischen „versicherbaren“ und „nicht versicherbaren“ Risiken, indem z. B. Finanzierungs- und Versicherungselemente miteinander kombiniert werden oder mehrere Sparten (etwa Feuer, Betriebsunterbrechungs- und Haftpflichtversicherung) in einem Produkt zusammengefasst werden. Ausgangspunkt ist das gesamte Risikoportefeuille des Unternehmens oder einer Gruppe von Unternehmen. Voraussetzung für ein solches Produkt ist stets ein proaktives Risikomanagement beim Versicherungsnehmer.[2]

Für das Risikomanagement, das Zusammenhänge strukturieren, interpretieren und vorbereitet sein muss, um in unvorhersehbaren Umfeldern bestmögliche Antworten geben zu können, ergibt sich ein „unlösbarer Zirkelschluss“: Erschwert wird dieses Risikomanagement, wenn Rückkopplungseffekte zu berücksichtigen sind, wenn ein Problem wahrgenommen wurde, sich das Verhalten des Systems verändert, was auf die Systemeigenschaften zurückwirkt.[3]

Ein vergleichbares Problem besteht beim Live-Response Ansatz bei Computer-forensischen Ermittlungen. Mit einer Computer-forensischen Ermittlung will eine durch einen Angriff geschädigte Organisation erkennen, welche Angriffsmethode oder welche Schwachstelle des angegriffenen Systems zum Systemeinbruch oder dem Verstoß gegen interne Regeln geführt hat, um eine Wiederholung zu verhindern und die Schwachstelle zu beseitigen. Die Analyse eines noch aktiven, nicht ausgeschalteten Systems erlaubt die Sammlung der meisten relevanten (weil flüchtigen) Daten und wird Live-Response genannt. Eines der Hauptprobleme der Live-Response ist, dass die Reihenfolge der Sicherung nicht zweifelsfrei festgelegt werden kann, da jede Tätigkeit am System dasselbe verändern kann.[4]

Themenauswahl, Modellansatz, Messmethoden enthalten a-priori Annahmen über genau die Risiken, die es zu messen gilt. Man kann nicht davon ausgehen, die Risiken zu kennen, die es zu messen gilt.[5] Dabei stellen Risiken nur in die Zukunft extrapolierte Möglichkeiten dar. In solchen Situationen kann man sich nicht mehr auf Erfahrungsmuster der Vergangenheit verlassen.

[1] vgl. Dahmen, Jörn (2002), S.19
[2] vgl. Romeike, Frank (2004), S.256-269
[3] vgl. Allenspach, Marco (2001), S.46
[4] vgl. Geschonnek, Alexander (2006)
[5] vgl. Allenspach, Marco (2001), S.52

Es kommt nicht nur darauf an, die Dinge im Risikomanagement besser zu gestalten, sondern durch eine neue Logik besser anzugehen. Eine solche „neue Logik“ kann die Szenariotechnik liefern. Szenarien sind flexibel vernetzte (Denk-)Rahmen, die bisher unbekannte Optionen erschließen können.[1] Szenariodenken verfolgt das Ziel, die Ungewissheit durch das Erkennen möglichst weniger konsistenter Alternativen zu strukturieren.[2] Als qualitative, explorative Prognosemethode hat sie zum Ziel, potenzielle Entwicklungsalternativen aufzuzeigen und deren Zustandekommen zu verdeutlichen. Unerwartete (negative) Ereignisse sollen so frühzeitig identifiziert und durch geeignete Handlungsstrategien beeinflusst werden.[3] Die Szenariotechnik versucht aber nicht wie die Prognose unsichere Daten „sicher zu rechnen“, sondern nimmt die Ungewissheit zunächst hin, um in einem weiteren Schritt ihre Struktur verstehen zu lernen und sie schließlich in die Strategieüberlegungen zu integrieren.[4]

Umfelder werden unvorhersehbar, wenn die Akteure mehr Optionen haben als in vorhandenen Modellen einbeziehbar. Strategie ist dann das Lösungskonzept, das den Handlungsspielraum liefert. Eine Einschätzung von Verhaltensrisiken (Risiken, die nicht auf Zuständen von Systemen oder Komponenten beruhen), kann durch Identifizierung der Strategien der „Mitspieler“ (potenzielle Angreifer, Spione, Saboteure) geschehen.[5] D. h., anstatt das Risiko direkt zu antizipieren, trifft man eine Voraussage der Strategie des Gegners und beurteilt, welche Risiken für die betroffene Organisation bei dieser Strategie auftreten können.

In der finanzwissenschaftlichen Theorie gibt es zahlreiche vor allem mathematisch-statistische Ansätze, Risiken zu erkennen und mit entsprechenden Kenntnissen zu begegnen. In der unternehmerischen Praxis von Nicht-Finanzdienstleistern sind die betriebsinternen Risikostrukturen durch eine grundlegend andere Kapitalbindungsstruktur jedoch viel komplexer.[6] Eintrittswahrscheinlichkeiten und Schadensfunktionen implizieren auch Rationalitäts- und Objektivitätsmaßstäbe, die oft nicht gegeben sind, weil sie Gegenstand der sozialen Risikokommunikation sind. Das Wahrscheinlichkeitskalkül kann so verschiedene Perspektiven (maßgeblich der vom Schaden Betroffenen, aber auch von Technik-Experten) ermöglichen. Eintrittswahrscheinlichkeiten und erwartete Schadensfunktionen sind je nach Perspektive auch anders einschätzbar. Der Subjektivität der Risikobewertung liegt dann in

[1] vgl. Bieta, Volker/Siebe, Wilfried (1998), S.52
[2] vgl. Bieta, Volker/Siebe, Wilfried (1998), S.52
[3] vgl. Wolf, Klaus (2003b), S.182
[4] vgl. Reichmann, Thomas (1993), S. 251
[5] vgl. Bieta, Volker (2004), S.XII
[6] vgl. Ibers, Tobias (2005), S.22

Präferenzen begründet, die der sozialen Interaktion ausgesetzt sind und somit endogen variieren.[1]

Objektiv gleichartige Situationen werden von verschiedenen Wirtschaftssubjekten unter Umständen unterschiedlich riskant wahrgenommen. Es spielen nicht nur unterschiedliche Erwartungen über zukünftige Entwicklungen, sondern auch unterschiedliche Zielsetzungen eine Rolle. Erst dies generiert einen Klassifizierungsmaßstab für eine Einstufung in die Kategorien erwünscht bzw. Ziel führend und unerwünscht bzw. nicht Ziel führend.[2]

Risiken und Gefahren sowie damit verbundene Unsicherheiten haben nicht nur eine objektive und eine subjektive, sondern auch eine soziale Seite. Mit unterschiedlichen Möglichkeiten zur Beherrschbarkeit sind unterschiedliche Handlungskompetenzen wie auch unterschiedliche Gefühle und Sicherheiten verbunden. Sicherheit ergibt sich nicht nur aus dem Vorhandensein von diesbezüglichen Institutionen wie Versicherungen oder rechtlichen Vorschriften, sondern ist zusätzlich in Beziehungen verschiedener Art eingebettet. Wenn staatlich garantierte Sicherheitssysteme ihre Funktionen reduzieren, so sind Angst und Betroffenheit dort am größten, wo zusätzliche kompensatorische Sicherheitsbedingungen fehlen.

Derartige Überlegungen veranlassen, Außengaranten der Sicherheit von Innengaranten zu unterscheiden. Diese stehen in einem komplexen Wechselverhältnis zueinander. Außengaranten sind die staatlich garantierten Sicherheitssysteme (rechtliche Vorschriften) oder Institutionen wie Versicherungen; sichernde Innengaranten sind Kompetenz, Umsicht und persönliche Ressourcen. Zu den Formen der Sicherheit zählen auch die individuell erworbenen Kompetenzen im Sinne von Orientierung und der sozialen Kompetenz, die es ermöglicht, jeweils spezifische kompensatorische Kompetenzen im Umgang mit Unsicherheit zu entwickeln.

Unsicherheit ergibt sich aus dem Verlust der Außen- und Innengaranten. Zur Herstellung von Sicherheit gehört auch jeweils spezifische kompensatorische Kompetenz im Umgang mit Unsicherheit zu entwickeln, Strategien, Aktionsräume und Optionen sichtbar zu machen, die im konkreten Alltag beschritten werden können. Diese Handlungsbefähigung wird im Angelsächsischen mit Begriffen wie "enabling" oder "empowering" umschrieben. Kompetenz im Umgang mit Unsicherheit kann als Befähigung zur Herstellung von Handlungsfähigkeit verstanden werden.[3]

[1] vgl. Japp, Klaus P. (2000), S.10-11
[2] vgl. Hölscher, Reinhold (2002), S.257
[3] vgl. O. Nigisch (1998)

Im sozialen Kontext werden Risiken in Heuristiken der Verfügbarkeit, der Freiwilligkeit und der Katastrophendimension bewertet und dann akzeptiert oder auch nicht. Diese Heuristiken stellen darauf ab, die individuelle Handlungsfähigkeit zu erhalten. Z. B. meinen viele Menschen, dass Fliegen gefährlicher sei als Autofahren, da sie glauben, gute Autofahrer zu sein – das Verhalten eines Flugzeugs können sie dagegen nicht beeinflussen. Das Kriterium „gefährlich“ wird in den Kontext der Handlungsbefähigung projiziert.[1] Im Rahmen der Erhebung und Quantifizierung der Folgen von Sicherheitsverletzungen bei der Informationssystem-Schutzbedarfsanalyse erfolgt z. B. auch eine Unterteilung u. a. in Folgen für die Handlungsfähigkeit.[2]

Spätestens in der virtuellen Welt des Internets sind IT-Risiken überwiegend nicht quantifizierbar, sondern in erster Linie qualitativer Natur. Viele IT-Risiken beruhen auf Verhaltensrisiken und sind auch nicht vorhersehbar. Daher führt eine alleinige IT-Risikoanalyse durch Berechnung von potenziellen Schadenshöhen der Risiken nicht zum Ziel, da die Mehrzahl der Risiken nicht berücksichtigt werden kann.

Bei dem Versuch, alle für das Unternehmen bedeutsamen Risiken zu quantifizieren, stößt das Management also auch auf nicht messbare Risiken für deren Bewertung allgemein akzeptierte Risikomodelle fehlen. Es ist jedoch mitunter möglich, schwer messbare Risiken qualitativ zu umreißen. Damit werden zumindest die Bedeutung dieser Risiken und der entstehende Handlungsbedarf klarer.[3] Die Ergebnisse einer IT-Risikoanalyse sollen so zur positiven Veränderung der Risikosituation beitragen.

Bei nicht antizipierbaren Risiken kann die Aufgabe, sich auf die aus der „Umgebung“ entspringenden Risiken einzustellen, sodass negative Auswirkungen auf den Grad der (subjektiven) Zielerreichung möglichst vermieden werden, dadurch gelöst werden, dass zunächst ein Kontext gesucht wird, in dem Risiken akzeptiert werden.

Ein systematisches Prinzip der Kontextselektion ist die funktionale Differenzierung. Die Zeitdimension spezialisiert sich auf die Unterscheidung von Vergangenheit und Zukunft, die Sachdimension auf die von System und Umwelt und die Sozialdimension auf die von Konsens und Dissens. Kontexte benötigen eine Differenz, in die Bedeutung hineinprojiziert werden kann, um überhaupt unterscheidbar zu sein, und zugleich über eine Identität in der zeitlichen, technisch-sachlichen oder sozialen Einheit der Differenz verfügen zu können.

[1] vgl. Japp, Klaus P. (2000), S.12-13
[2] vgl. Müller, Klaus-Rainer (2003) , S.49
[3] vgl. Merbecks, Andreas (2004), S.107

Die Kontextbildung betrifft die Aufspaltung in Horizonte sinnhafter Möglichkeiten. Solche sind z. B. in zeitlicher Hinsicht Reversibilität, in technischer Hinsicht Verlässlichkeit, in sachlicher Hinsicht Beherrschbarkeit und in sozialer Hinsicht Möglichkeit zur Verständigung. Diese Sinnhorizonte sind die Basiskontexte der Risikokommunikation.

Der technisch-organisatorische Kontext für die IT-Sicherheit von Systemen wird so in die „Sinnhorizonte“ Verlässlichkeit (Sicht des Systems) und Beherrschbarkeit (Sicht der Anwender/Benutzer) aufgespalten. Der technisch-organisatorische Kontext für die IT-Sicherheit von Systemen, aus Sicht des IT-Systems der Kontext Verlässlichkeit (beurteilt nach den Kriterien Verfügbarkeit, Integrität und Vertraulichkeit) und aus Sicht der Betroffenen (Anwender/Benutzer) der Kontext Beherrschbarkeit des Systems (beurteilt nach den Kriterien Nachprüfbarkeit und Rechtssicherheit) umfasst also die Sichten auf die Sicherheit des Systems.

Die Prognose von Risiken der IT-Sicherheit, beruhend auf Erfahrungswerten der Vergangenheit, ist in der Regel nicht möglich. Ob Risiken im Sinne der Erhaltung der Handlungsbefähigung akzeptiert werden können, ist auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen nicht beurteilbar. Besser beurteilbar sind Strategien. Der Kontext, in dem Risiken akzeptiert werden können, sollte daher auf der Strategieebene liegen. Der technisch-organisatorische Kontext für die IT-Sicherheit von Systemen ist dann in den Kontext, in dem Risiken akzeptiert werden können, zu transformieren. Auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen stehende Kriterien werden so in diesen Kontext projiziert.

Wenn es um die Bewertung und Akzeptanz von den der Planung zugrunde liegenden Risiken geht, werden Heuristiken z. B. der Verfügbarkeit, der Freiwilligkeit und der Katastrophendimension herangezogen.

Die Unterscheidung von Sicherheit und Risiko stützt sich dabei auf die Unterscheidung von Subjekt und Objekt: Es gibt riskante Bewertungen der Subjekte, aber auch wissenschaftlich zugängliche Sachverhalte, die von den Experten als sicher qualifiziert werden.

Für das Beispiel Technik lässt sich leicht zeigen, dass Sicherheit gar nicht vorkommt. Sie wird nur laufend angestrebt, als Realzustand ist sie nicht erreichbar. Ein Unternehmensnetz oder auch nur einzelne Computer können nie völlig „sicher“ betrieben werden. Durch Innentäter oder spätestens sobald man Informationen von außerhalb des Firmennetzes benötigt, besteht eine Bedrohung durch z. B. Viren, Würmer oder Trojaner. Geraten beispielsweise vertrauliche Dokumente in die falschen Hände, kann dies fatale Folgen haben. Ein Ad-

ministrator muss sicherstellen, dass nur berechtigte Benutzer Zugriff auf das Netzwerk und die darin gespeicherten Daten haben. Selbst ein völlig isolierter Computer wäre immer noch durch Hardware-Defekte, Software-Fehler und durch seine Bediener bedroht. Auch die physikalische Sicherheit von Netzwerken und Daten ist durch z. B. Hardware-Defekte oder Stromausfälle gefährdet.[1]

Sicherheit ist ein Reflexionsbegriff in dem Sinne, dass sich in ihr ihr Gegenteil (Unsicherheit als bewusst wahrgenommener Mangel an Sicherheit) reflektiert. Risiko bezieht sich auf Unsicherheit, nämlich bezüglich des Erreichens angestrebter Ziele. Die Standardunterscheidung zwischen Sicherheit und Risiko ist somit keine Differenz, in die Bedeutung hineinprojiziert werden kann, damit der gesuchte Kontext (von anderen Kontexten) unterscheidbar ist, und über eine Identität in der zeitlichen, technisch-sachlichen oder sozialen Einheit der Differenz verfügt. Man kann deshalb anstelle der Standardunterscheidung zwischen Sicherheit und Risiko mit der Unterscheidung von Gefahr (tatsächlicher Mangel an Sicherheit) und Risiko arbeiten. Getrennt werden die beiden Seiten durch die Zurechnungsrichtung, nach innen oder nach außen, auf System oder Umwelt insgesamt, Selbst- oder Fremdzurechnung, wobei Risiko die Seite der Selbstzurechnung und Gefahr die der Fremdzurechnung eines Schadens darstellt.

Gefahr und Risiko unterscheiden sich demnach durch den Grad der wahrgenommenen Steuerungsfähigkeit durch Personen oder Organisationen. Alles, was von außen als Bedrohung wahrgenommen werden kann, kann als Gefahr bezeichnet werden. Dagegen sind Risiken nach dieser Auffassung solche Bedrohungen, die vom Betrachter selbst oder durch von ihm beeinflussbare Organisationen gesteuert werden können.[2]

Auch Gewissheit (oder Sicherheit von Wissen[3]) (über zukünftige Entwicklungen) ist im Allgemeinen nie erreichbar. Auch hier kann man in Risiko und Gefahr differenzieren: Meint man mit Gefahr „externe Ungewissheit“, so resultiert sie aus der Unternehmensumwelt, die auf das Unternehmen einwirkt. Hierbei spielt neben den Kapital-, Beschaffungs- und Absatzmärkten auch die technologische, rechtlich-politische und sozio-kulturelle Umwelt eine Rolle. Eine große Dynamik geht insbesondere von den Auswirkungen der Informationstechnologie auf die Unternehmen aus. Risiko als „interne Ungewissheit“ wird durch unternehmensinterne Einflussgrößen bestimmt.

[1] vgl. PC-Welt (2004), S.3
[2] vgl. Hölscher, Reinhold (2002), S.76
[3] Ibers, Tobias (2005), S.31

In einer an Komplexität und „externer Ungewissheit“ zunehmenden Umwelt nimmt die Bedeutung der Schaffung von strategischen Handlungsspielräumen zu, um sich den aus der Unternehmensumwelt auf das Unternehmen einwirkenden Gefahren, wenn diese gewisser werden, mit einer entsprechenden Alternative aus dem strategischen Handlungsspielraum anpassen zu können. Strategische Handlungsspielräume führen zu Optionen, die die Entscheidungsträger ausüben können, aber nicht müssen. Gehen solche Handlungsspielräume z. B. nicht in die Bewertung ein, bleibt ein großer Teil des Werts strategischer Projekte unberücksichtigt.[1]

Diese Handlungsspielräume bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens/die durch die Umwelt vorgegebenen Strategiealternativen beeinflussen den Unternehmenserfolg. Das unternehmerische Risikomanagement-System (wie auch das im Folgenden zu entwickelnde IT-Security-Management) hat sicherzustellen, dass den unternehmerischen Erfolg gefährdende Risiken frühzeitig erkannt sowie adäquat gesteuert werden. Risiken resultieren aus der Ungewissheit, dass aufgrund von Störungen geplante Ziele verfehlt werden könnten. Diese Ziele beziehen sich auf die zu unterstützenden und zu optimierenden Geschäftsprozesse und die zu ermöglichenden Geschäftsmodelle des Unternehmens. Das Management hat die organisatorische Abwicklung der Geschäftsprozesse mit Blick auf die unternehmerische Zielsetzung zu gestalten.

Der gesuchte (auf der Strategieebene liegende) Kontext, in dem Risiken akzeptiert werden können, ist also der Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens. Dieser Kontext hat zwei Seiten. Die auf das System bezogene Seite dieses Kontexts sind die eigenen Handlungsmöglichkeiten (Flexibilität). Die auf die Umwelt bezogene Seite dieses Kontexts sind die möglichen Randbedingungen des Umfelds. Diese Differenz wird bei der Auflösung der Ungewissheit zur Sicherstellung von Potenzialen bzw. Strategien zur Ausnutzung operativer Flexibilität und zur Steigerung von Managementflexibilität herangezogen. Der technisch-organisatorische Kontext für die IT-Sicherheit von Systemen wird in die auf das System bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume, also eigene Handlungsmöglichkeiten (Flexibilität) transformiert.

[1] vgl. Freihube, Klaus (2001)

Eine sinnhafte Dimension der Flexibilität stellen Realoptionen dar. Das zunehmende Änderungstempo der Rahmenbedingungen unternehmerischen Handelns und daraus resultierender Ungewissheit bezüglich der Zielerreichung verlangen neue Wege strategischen Denkens und neue Analysewerkzeuge. Realoptionen können den Kern eines solchen strategischen Frameworks und ein zunehmend wichtiges Sicherheitsanalyse-Werkzeug bilden. Durch das Hinzufügen einer wichtigen Dimension analytischer Flexibilität erlauben Realoptionen eine Verbindung von strategischer Intuition und analytischer Korrektheit: Auch bei der Bewertung von Unternehmen z. B. existiert eine Lücke zwischen der Marktkapitalisierung und Ergebnissen traditioneller Bewertungsmodelle wie dem discounted cash flow (DCF), die mit einem solchen Analysewerkzeug geschlossen werden kann.

Das strategisch-operative IT-Security-Management muss Gefahren/externe Ungewissheit und Risiken/interne Ungewissheit für den IT-Security-Prozess (wobei sich Ungewissheit auf Zielvorgabe und -erreichung bezieht) identifizieren, bewerten und steuern. Zielvorgabe und -erreichung wiederum bezieht sich auf die Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse. In diesem Kontext soll das strategisch-operative IT-Security-Management strategisch-operative Handlungsspielräume unterstützen/absichern. Um sich in einer an Komplexität und „externer Ungewissheit“ zunehmenden Umwelt an die aus der Unternehmensumwelt auf das Unternehmen einwirkenden Gefahren, wenn diese gewisser werden, mit einer entsprechenden Alternative aus einem strategisch-operativen Handlungsspielraum anpassen zu können, muss das strategisch-operative IT-Security-Management die Möglichkeiten in diesem strategisch-operativen Handlungsspielraum unterstützen/absichern. Dieser strategisch-operative Handlungsspielraum bezieht sich auf den Gegenstand des strategischen IT-Managements, die mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens. Diese IT-Projekte wiederum werden mittels der physischen Objekte Hardware, Software, Netze und Personal und logischen Objekte wie Informationssysteme, Datenbanken, Kommunikationsbeziehungen sowie Konzepte wie Vorgehensmodelle, Systementwicklungsmethoden und Richtlinien für den Werkzeugeinsatz umgesetzt.. Auf diese physischen und logischen Objekte beziehen sich auch die operativen Bestandteile einer ganzheitlichen IT-Security-Strategie, welche auf den Ebenen der Gründe für die Unbestimmtheit der Zielvorgabe und Zielerreichung des IT-Security-Prozesses identifiziert wurden.

4.1 Auflösung der Ungewissheit zur Sicherstellung von Potenzialen bzw. Strategien zur Ausnutzung operativer Flexibilität und zur Steigerung von Managementflexibilität

Was die Planung von Unternehmensprozessen, auch des IT-Security-Prozesses erschwert, und theoretischer Überlegungen für entsprechende Konzepte bedarf, ist die Unvorhersehbarkeit der zukünftigen Entwicklung. Die zukünftige Entwicklung der Umwelt, zukünftige Anforderungen an die IT-Security aufgrund neuer gesetzlicher Erfordernisse, externer und interner Ordnungsmäßigkeitsbedürfnisse sowie immer neu auftauchender IT-Bedrohungen, kann nur geschätzt werden.

Umweltzustände werden unterteilt in Sicherheitssituationen, Risikosituationen und Ungewissheitssituationen. Eine Sicherheitssituation liegt vor, wenn der wahre (zukünftige) Umweltzustand bekannt ist. Dies wird angenommen, wenn jeder Aktion ein eindeutiges Ergebnis zugeordnet werden kann. Bei Risiko- und Ungewissheitssituationen ist das Ergebnis einer Aktion nicht eindeutig bestimmt. Bei einer Risikosituation existieren zumindest subjektive Wahrscheinlichkeiten für die einzelnen Umweltzustände. Diese Situation ist die, welche in der klassischen Entscheidungslehre betrachtet wird.[1]

Alle Prognosen und Annahmen über zukünftige Entwicklungen sind mit Unsicherheit behaftet.[2] Häufig werden Wahrscheinlichkeiten für bestimmte Umweltzustände angegeben. Man kann dann die Entscheidungstheorie für die Planung von Aktivitäten heranziehen. Vor allem bezüglich der IT-Sicherheit ist es aber im Allgemeinen nicht sinnvoll, mit Wahrscheinlichkeiten zu arbeiten.

Ein Ziel des (sich mit Ungewissheitssituationen befassenden) Risikomanagements ist es, die Anteile an Ungewissheit zu mindern, indem sie messbar und handhabbar gemacht werden.[3] IT-Security kann so gesehen werden, dass sie gegenüber der IT-Sicherheit auch strategische Aspekte aufweist. Ein Ansatz zur Auflösung der Ungewissheit bezüglich Umfeldentwicklungen kann darauf abzielen, Strategieoptionen zu untersuchen: Die Ungewissheit bezüglich Umfeldentwicklungen kann in zwei Richtungen getrennt voneinander untersucht werden: eigene Handlungsmöglichkeiten und mögliche Randbedingungen des Umfelds.[4] Dies soll den Ausgangspunkt für das im weiteren Verlauf entwickelte Modell zum strategisch-operativen

[1] vgl. Freihube, Klaus (2001), S.16,17
[2] vgl. Wikimedia Foundation (2005)
[3] Ibers, Tobias (2005), S.32
[4] vgl. Fink, Alexander (2001), S.157

Risiko-Controlling in Form eines dem klassischen Risikomanagementprozess übergeordneten Bausteins bilden.

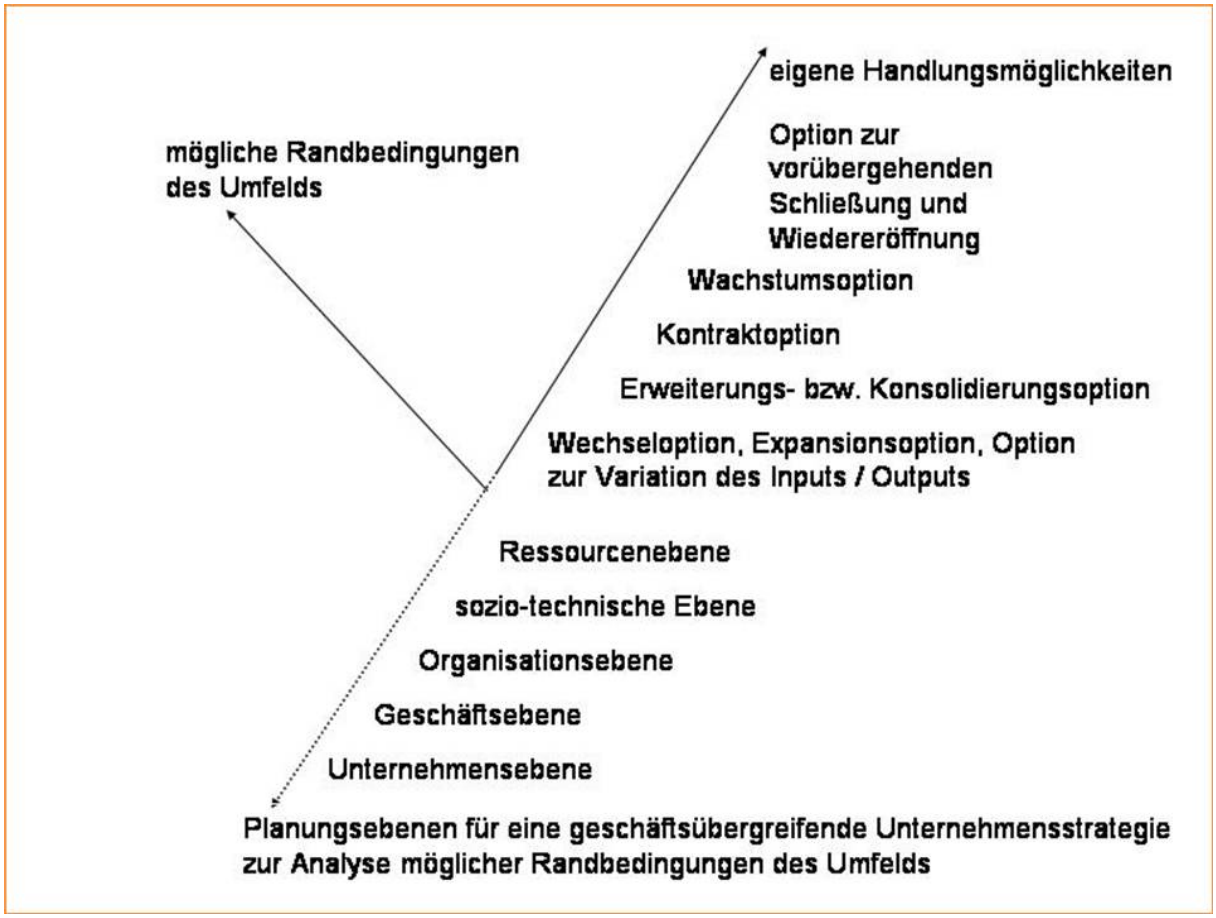


Abb. 9 Auflösung der Ungewissheit bezüglich Umfeldentwicklungen

Die Richtungen eigene Handlungsmöglichkeiten und mögliche Randbedingungen des Umfelds sind die Differenz des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume (bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens). Eigene Handlungsmöglichkeiten ist die auf das System bezogene Seite, und mögliche Randbedingungen des Umfelds ist die auf die Umwelt bezogene Seite dieses Kontexts.

Darüber hinaus trägt dies der Unterscheidung von Einflussgrößen in lenkbare und nicht lenkbare Größen Rechnung: Mögliche Randbedingungen des Umfelds stellen in der Regel nicht lenkbare Größen in Zusammenhang mit ursachenbezogenen Risikokomponenten dar. Nicht lenkbare Größen liegen außerhalb unseres unmittelbaren Einflussbereichs, müssen aber trotzdem überwacht werden, da sie die Entwicklung wesentlich beeinflussen können. Lenkbare Größen (eigene Handlungsmöglichkeiten) ermöglichen direkte Eingriffe (in das System) und sind deshalb direkte Ansatzpunkte für Strategien und Maßnahmen. Indikatoren signalisieren

dagegen nur den Grad der möglichen Zielerreichung und dienen der Früherkennung/Frühwarnung.[1]

Mit der Untersuchung der Ungewissheit bezüglich Umfeldentwicklungen in zwei Richtungen getrennt voneinander wird also der Kontext der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume (bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens) zerlegt. Diese Zerlegung soll letztlich die proaktive Berücksichtigung von Umwelt- (und Wettbewerbs-) bedingten Unsicherheiten (im Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume) ermöglichen. Dazu wird eine Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in die auf das System bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse gebildet.

Die möglichen Randbedingungen des Umfelds und die eigenen Handlungsmöglichkeiten (bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens) werden auf den Planungsebenen für eine geschäftsübergreifende Unternehmensstrategie untersucht.

Bei der Analyse möglicher Randbedingungen des Umfelds kann die Szenarioanalyse weiterhelfen. Als Instrument des strategischen Controllings strukturiert die Szenarioanalyse die Ungewissheit (Szenarienmanagement als strukturierendes Organisationsprinzip[2]) nicht durch Korrelation einer nicht überschaubaren Zahl von Einflussgrößen, sondern entwickelt anhand einiger signifikanter Variablen in sich schlüssige Alternativen.

Während Frühwarninformationen die voraussichtlichen Wirkungen von bereits existenten, jedoch nur verdeckt erkennbaren Ereignissen bzw. Entwicklungen aufzeigen, geht es bei der Erarbeitung von Szenarien um potenzielle zukünftige Situationen und das nachvollziehbare Aufzeigen des möglichen Entwicklungsverlaufs dorthin.[3] Szenarien (mehrere alternative Zukunftsbilder) bilden die Basis für vorbeugendes Nachdenken, das die Voraussetzung für vorbeugendes Handeln schafft.[4]

Am Anfang der Szenario-Entwicklung steht die Definition eines Szenario-Feldes, das den Bereich beschreibt, dessen Zukunft in Form von Szenarien beschrieben werden soll.[5] Um das Szenario-Feld umfassend beschreiben zu können, werden im Rahmen der Szenario-Feld-

[1] vgl. Gomez, Peter (2002), S.119
[2] Bieta, Volker/Siebe, Wilfried (1998), S.71
[3] vgl. Hahn, Dietger (2006), S.14
[4] vgl. Fink, Alexander (2001), S.7
[5] vgl. Fink, Alexander (2001), S.75

Analyse die relevanten Schlüsselfaktoren ausgesucht, für die jeweils mehrere denkbare Zukunftsentwicklungen aufgezeigt werden können.[1] Dabei hat es sich als sinnvoll erwiesen, das Szenario-Feld zunächst durch Systemebenen (grundsätzliche Einflusssphären) und Einflussbereiche zu beschreiben.[2] Um die Entwicklungsmöglichkeiten des Szenario-Feldes darzustellen, werden die einzelnen Einflussbereiche durch mehrere geeignete Einflussfaktoren beschrieben. Externe Quellen zur Ermittlung von Einflussfaktoren sind z. B. Checklisten oder eigene Literaturrecherchen. Die prägnante Beschreibung der Einflussfaktoren soll eine gemeinsame Grundlage für spätere Bewertungen und Zukunftsüberlegungen schaffen.[3]

Im Mittelpunkt steht das Denken in Wirkungsketten und Wirkungsnetzen[4], in Gesamtzusammenhängen und wechselseitigen Abhängigkeiten.[5]. Für eine Vernetzung im Denken und in der Wissensspeicherung ist es notwendig, sich dem Wandel und vorgegebenen Strukturen anzupassen, diese umzusetzen, und Trends vorab zu erkennen.[6] Das vernetzte Denken in Alternativen wird als Szenario-Software bezeichnet.[7] Die Szenariotechniken, die Methoden der Problem-, Umfeld- und Störereignisanalyse werden als Szenario-Hardware bezeichnet. [8] Verbunden werden Szenario-Hardware und Szenario-Software mit dem Szenariomanagement zur „vernetzten Perspektive des Umfeldwandels“.[9]

Im (operativen) Bereich der IT-Sicherheit ist diese Szenario-Hardware im Wesentlichen durch den „operativen Rahmen zur Analyse und Risiko orientierten Ausgestaltung der IT-Security“ (Kapitel 3) beschrieben. Die in Kapitel 5 betrachteten Aspekte betreffen im IT-Risikomanagement ebenfalls zunächst die Szenario-Hardware. Mit der Integration eines Anpassungsprozesses an die Umgebung in das zu entwickelnde Modell zum strategisch-operativen Risiko-Controlling kommen Aspekte der Szenario-Software hinzu.

Bei der Untersuchung der Ungewissheit bezüglich Umfeldentwicklungen in Richtung eigener Handlungsmöglichkeiten sind Entscheidungsfreiheiten/Flexibilitätspotenziale zu analysieren, um wandelnden Konstellationen im Umfeld entsprechen zu können. Dieses kann als funktionaler Aspekt der Aufgaben eines Controllingsystems gesehen werden, welches als ergebniszielorientiertes Koordinationssubsystem der Führung zur Koordination von Planung, Kontrolle und Informationsversorgung dient. Diese Aufgaben umfassen alle Aktivitäten zur

[1] vgl. Fink, Alexander (2001), S.74
[2] vgl. Fink, Alexander (2001), S.76
[3] vgl. Fink, Alexander (2001), S.78
[4] Gadatsch, Andreas (2006), S.7-12
[5] vgl. Reichmann, Thomas (1993), S. 262
[6] vgl. Kremin-Buch, Beate/Unger, Fritz/Walz, Hartmut (2004), S.11
[7] vgl. Bieta, Volker/Siebe, Wilfried (1998), S.52
[8] vgl. Bieta, Volker/Siebe, Wilfried (1998), S.52
[9] vgl. Bieta, Volker/Siebe, Wilfried (1998), S.53

Sicherung der Koordinations-, Reaktions- und Adaptionsfähigkeit der Führung.[1] Fehlende Flexibilität kann dazu führen, dass veränderte Anforderungen nicht oder nicht nachvollziehbar umgesetzt werden, was die Revisionsfähigkeit gefährdet.

Zur Abbildung und „Beurteilung strategischer und operativer Handlungsmöglichkeiten“[2] werden im Folgenden Realoptionen angesetzt. Diese lassen sich einerseits als „Managementansatz zur proaktiven Berücksichtigung von umwelt- und wettbewerbsbedingten Unsicherheiten“ und andererseits als „Instrument zur Bewertung von Handlungsflexibilität“ einordnen.[3] Als Investitionsbeurteilungsverfahren bietet sich der Realoptionsansatz zur Berücksichtigung von Handlungsflexibilität bei phasenweisen Investitionsprozessen an. Erwünschter Effekt dabei ist die Sensibilisierung des Managements für die Bedeutung immaterieller Vermögenswerte/intellektuellem Kapitals.[4]

Der Realoptionsansatz ermöglicht „die Verfeinerung der Analyse von Unsicherheiten, Flexibilität und deren Interaktion voranzutreiben“.[5] Die Bewertung von Optionen ist ein wichtiges Instrument zur Steuerung von Risiken.[6] Darüber hinaus kann der Realoptionsansatz zur Identifikation wichtiger Projekteigenschaften beitragen.

Reale unternehmerische Entscheidungssituationen sind durch eine permanente Variation der Umweltbedingungen und damit die Notwendigkeit zur permanenten Handlungsfähigkeit gekennzeichnet. Realoptionsbasierte Modelle lassen die Beobachtung der Umwelt und gleichzeitig die Ausübung von Handlungsfreiheiten zu[7], dienen der Darstellung von Handlungsmöglichkeiten (bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens).

Um Realoptionen (als wichtiges Instrument der strategischen Planung[8]) bei der Planung einzubeziehen, sind diese auf den Planungsebenen für eine geschäftsübergreifende Unternehmensstrategie (Ressourcenebene, sozio-technische Ebene, Organisationsebene, Geschäftsebene und Unternehmensebene) zu betrachten. Diese Realoptionen, z. B. Wechseloption, Expansionsoption, Option zur Variation des Inputs/Outputs, Erweiterungs- bzw. Konsolidierungsoption, Kontraktoption, Wachstumsoption, Option zur vorübergehenden Schließung und Wiedereröffnung sind auf den Gegenstand des strategischen IT-Managements zu beziehen, auf das Management der mittels geeigneter IT-Projekte zu implementierenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens.

---

[1] vgl. Stoi, Roman (2002), S.155
[2] Romeike, Frank (2005), S.33
[3] Hommel, Ulrich (2001), S.14
[4] vgl. Stoi Roman (2003), S.178
[5] Hommel, Ulrich. (2001), S.24
[6] vgl. Finke, Robert (2005), S.25
[7] vgl. Niemann, Rainer (2001), S.44
[8] Hommel, Ulrich. (2001):, S.213

4.2 Kritikalitäts- und Kontext-orientierter Ansatz

Um auf die Ebene der IT-Sicherheit/IT-Security zu gelangen, dazu kann man an der zweiten Richtung ansetzen, in der die Ungewissheit bezüglich Umfeldentwicklungen untersucht wurde: mögliche Randbedingungen des Umfelds.

Bei dieser Analyse wird versucht, z. B. mit Hilfe von Prognose- und Frühaufklärungstechniken Rahmenbedingungen für das Management hinsichtlich möglicher Zukunftsentwicklungen eingrenzbar zu machen, um eine Basis für den strategischen Managementprozess und die Strukturgestaltung des Unternehmens zu bekommen. Die Rahmenbedingungen für das Management werden als unmittelbarer Kontext des Unternehmens bezeichnet. Er wirkt als Auslöser und zeigt Handlungsbedarf auf. Unterschieden werden eine externe und eine interne Sicht auf den Kontext eines Unternehmens. In Bezug auf die externe Sicht steht primär die Analyse der Konkurrenz, der strategischen Gruppen, der Branchenstruktur und -dynamik sowie der globalen Umwelt im Vordergrund. Die interne Sicht analysiert vorrangig gegenwarts- und vergangenheitsbezogene Faktoren wie Leistungsprogramm, Technik, Größe, Rechtsform und Eigentumsverhältnisse, Organisationsstruktur, Koordinationsformen, Organisationskultur, Führungskonzept und -stil.[1]

Der Anspruch, dass eine Entscheidung (oder Aktivitäten) in einer gegebenen Situation ein Zielbündel zweckrational und wertoptimierend erreichen soll, ist nur unter Einbeziehung situationsspezifischer Begleitumstände und Kontexte (als wesentliche Merkmale der Risikowahrnehmung) zu erfüllen. Diese Wahrnehmungsmuster sind bewährte Konzepte, „die in vielen Fällen wie eine universelle Reaktion von Menschen auf die Wahrnehmung von Gefahren das eigene Verhalten steuern“.[2] Die auf die Umwelt bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse (mögliche Randbedingungen des Umfelds) wird mit den Rahmenbedingungen für das Management identifiziert. Diese Rahmenbedingungen für das Management beziehen sich (im Zusammenhang mit der Anpassung an das organisatorische und das technische Umfeld des Unternehmens) wiederum auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen. Dieser ist aus Sicht des IT-Systems der Kontext Verlässlichkeit (beurteilt nach den Kriterien Verfügbarkeit, Integrität und Vertraulichkeit), und aus Sicht der Betroffenen (Anwender/Benutzer) der Kontext Beherrschbarkeit des Systems (mit den Aspekten Komplexitätsreduktion und

[1] vgl. Seidenschwarz, Werner (2003): S.30,31
[2] Hölscher, Reinhold (2002), S.85

Kontrollierbarkeit, beurteilt z. B. nach den Kriterien Nachprüfbarkeit und Rechtssicherheit). Der technisch-organisatorische Kontext für die IT-Sicherheit von Systemen umfasst die Sichten auf die Beurteilung der Sicherheit des Systems, wobei die IT-Infrastruktur die zentrale Rolle spielt. Die IT-Infrastruktur wiederum ist das zentrale Element eines IT-Security-Frameworks, welches die Ebene der IT-Sicherheit/IT-Security mit der Strategieebene verbindet.

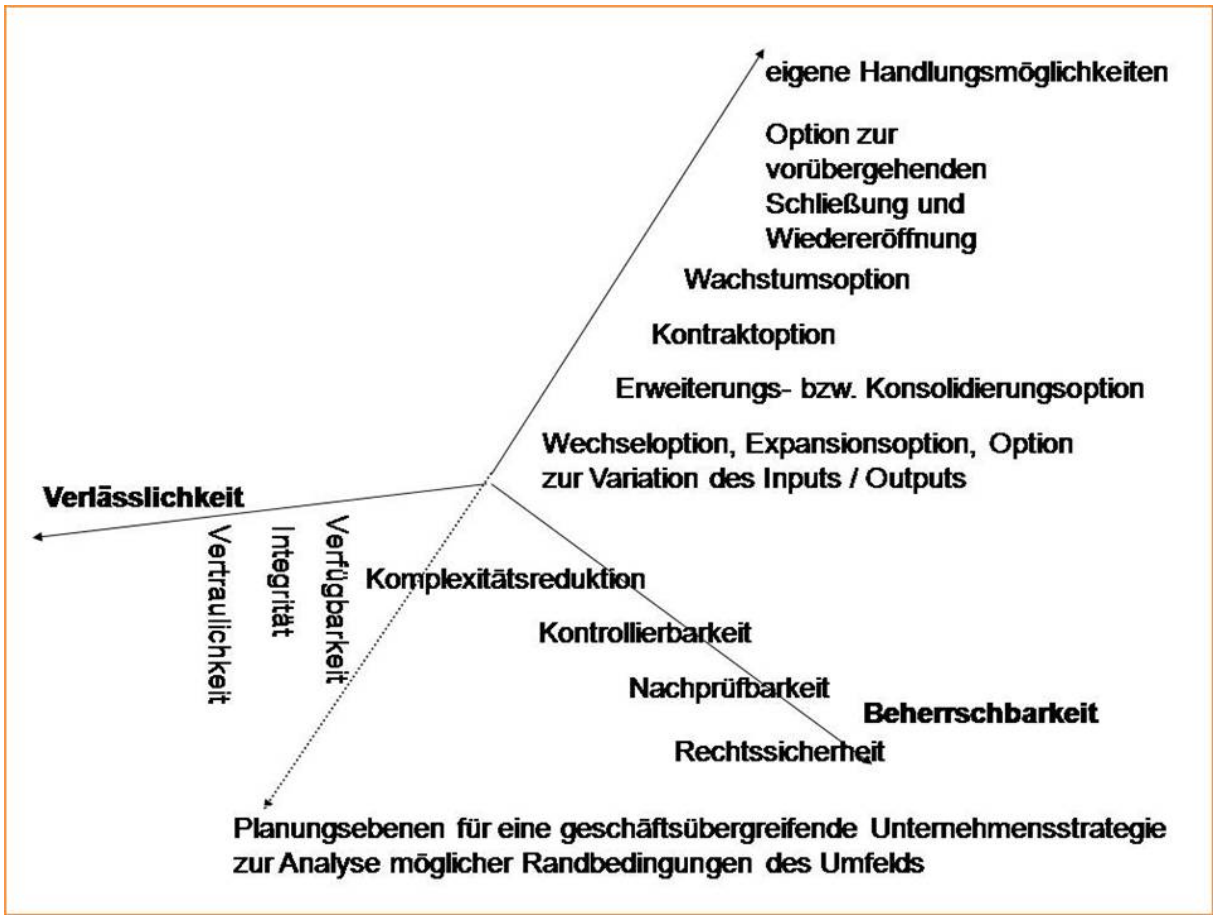


Abb. 10 Ersetzung der Richtung „mögliche Randbedingungen des Umfelds“

Man unterscheidet auch Lenkungsbereiche und Umfeldbereiche. Erstere sind direkt beeinflussbar (z. B. interne Organisation, Prozess, EDV, Personal), während Umfeldbereiche (z. B. der rechtliche, politische, soziale und externe technologische Kontext) sich einem unmittelbaren Einfluss durch das Unternehmen entziehen.[1] So ist die Sicht der Benutzer/Anwender auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen (Beherrschbarkeit) der Lenkungsbereich dieses Kontexts, während die Sicht des Systems auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen den Umfeldbereich dieses Kontexts darstellt. An diesen Umfeldbereich muss das Unternehmen sich anpassen.

[1] vgl. Wolf, Klaus (2003b), S.185

Im sozialen Umfeld wird das Kriterium „gefährlich“ in den Kontext der Handlungsbefähigung trotz Unsicherheit projiziert. Die beiden Seiten der Unterscheidung von Risiko und Gefahr werden dort durch die Zurechnungsrichtung getrennt, nach innen oder nach außen, auf System oder Umwelt insgesamt, wobei Risiko die Seite des Systems und Gefahr die der Umwelt darstellt. Auf IT-Risiken aus der Umwelt trifft daher die Bezeichnung Gefahr zu.

Der technisch-organisatorische Kontext für die IT-Sicherheit von Systemen kann einerseits aus dem Blickwinkel „gefährlicher“ Risiken betrachtet werden. Das ist die Sicht der Betroffenen (Anwender/Benutzer), die die Risiken des Systems im Kontext der Beherrschbarkeit beurteilen. Betrachtet man die IT-Infrastruktur (als zentralen Bestandteil des Systems, auf den die Sichten des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen gerichtet sind) von innen her, vonseiten des Systems, so ist dies die Sicht auf die Verlässlichkeit des IT-Systems.

Handlungsspielräume (bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens) in Abhängigkeit von möglichen Risiken der IT-Security stehen im Mittelpunkt des im Folgenden zu entwickelnden Modells zum strategisch-operativen Controlling der IT-Security. Risiken der IT-Security sind nicht antizipierbar. Die Dynamik der technologischen Entwicklung mit immer neuen Möglichkeiten potenzieller Angreifer macht neue Schwachstellen und Bedrohungen unvorhersehbar. Präventive Gegenmaßnahmen sind dann kaum möglich. Eine auf ihrer Erfassung beruhende Risikobewertung ist dann ebenfalls nicht möglich. Eine indirekte Bewertung wird aber über die Analyse der Handlungsspielräume in Abhängigkeit von potenziellen Risiken der IT-Security möglich. Die in einer Kausalkette einen möglichen Schaden auslösenden potenziellen Risiken sind immer in einer möglichen Nichterfüllung von Sicherheitsanforderungen begründet. Wenn man potenzielle Risiken der IT-Security nicht kennt, kann man also Handlungsspielräume (bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens) in Abhängigkeit von Sicherheitsanforderungen analysieren. Dies ist dann die eigentliche Aufgabe des strategisch-operativen Controllings der IT-Security, welches auf Risikoüberwachung, Risikocontrolling und Risikosteuerung basiert, welche Handlungsspielräume zunächst in Abhängigkeit von potenziellen Risiken der IT-Security analysieren und optimieren sollen.

Die auf die auf das System bezogene Kontextseite der Gestaltung der organisatorischen Abwicklung der Geschäftsprozess bezogenen Ziele (bezüglich der Unterstützung strategisch-operativer Handlungsspielräume bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens) sollen in entsprechende Anforderungen auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen projiziert werden. Diese Vor-

gehensweise stellt die Alternative zur Antizipation von Risiken (Voraussehen negativer Ereignisse und ihrer Folgen) auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen dar. Aus den identifizierten Anforderungen werden dann Maßnahmen abgeleitet, die, anstatt den ex-ante nicht identifizierbaren Risiken entgegenzuwirken, die Anforderungen abdecken.

Heute vorkommende Risiken lassen sich auch qualitativ kaum abschließend erfassen. Es wird dann auf eine (quantitative oder qualitative) Risikoanalyse verzichtet, stattdessen werden bestimmte sinnvolle Sicherheitsmaßnahmen vorgeschrieben.[1]

Wenn die auf die strategische Zielsetzung einwirkenden und deren Erreichung gefährdenden Risiken nicht vorhersehbar/abschätzbar sind, kann man die Anforderungen analysieren, die zur Umsetzung der strategischen Zielsetzung notwendig sind. Diese Anforderungen beziehen sich auf die Objekte, für die man eigentlich eine Risikoanalyse durchführen müsste. Statt einer Risikoanalyse führt man eine Anforderungsanalyse durch. Vor allem die Früherkennung von Risiken der IT-Security scheint kaum möglich. Man sollte dann präventiv alle Anforderungen abdecken, die entsprechend der Kritikalität der betreffenden IT-Objekte relevant sind.

Im Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens, welcher der Ausgangskontext des im weiteren Verlauf entwickelten strategisch-operativen Controllings der IT-Security ist, sollten die auf eine mögliche Nichterfüllung dieser Anforderungen einwirkenden Risiken akzeptiert werden können.

Bezieht man Zielvorgabe und Zielerreichung des IT-Security-Prozesses auf die im strategischen Controlling der IT-Security betrachtete Unterstützung/Absicherung strategisch-operativer Handlungsspielräume (bei der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse), so sind die Gründe für die Unbestimmtheit der Zielvorgabe und Zielerreichung des IT-Security-Prozesses die ungenauen gegenwärtigen und ungewissen zukünftigen Anforderungen an die IT-Sicherheit/IT-Security.

Die mangelnde Prognostizierbarkeit zukünftiger Umfeldentwicklungen versucht das strategische Controlling - den Prozess des strategischen Managements bei der Strategieentwicklung und bei der Strategieumsetzung unterstützend – mit Prämissenkontrolle, strategischer Durchführungskontrolle und strategischer Überwachung zu kompensieren. Im

[1] vgl. Möller, Thorsten (2007), S.37

weiteren Verlauf wird aus diesem Ansatz ein strategisch-operatives Risiko-Controlling/Controlling der IT-Security entwickelt. Hierbei soll das strategisch-operative Risiko-Controlling/Controlling der IT-Security den Prozess des strategischen Managements bei der Strategieentwicklung und bei der Strategieumsetzung insofern unterstützen, dass es die (als Voraussetzung zur Erreichung der Unternehmensziele/strategisch-operativen Zielsetzungen des Unternehmens angenommene) Handlungsbefähigung/Flexibilität/strategisch-operative Beweglichkeit (bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander), so weit diese durch die IT-Sicherheit von Systemen beeinflusst wird, überwacht und steuert. Dieses strategisch-operative Risiko-Controlling/Controlling der IT-Security wird mithilfe der Komponenten (strategische und operative) Prämissenkontrolle, (strategische und operative) Durchführungskontrolle und (strategische und operative) Überwachung eines entsprechenden Performance-Managements als dem klassischen Risikomanagement-/IT-Security-Management-Prozess übergeordneter Baustein konzipiert. In ein entsprechendes strategisch-operatives Risiko-Controlling wird des Weiteren über das strategische und operative Performance-Management ein Anpassungsprozess an die Umgebung bezüglich der IT-Security integriert. Dieser passt den Prozess zur Formulierung und Umsetzung der strategisch-operativen Zielsetzungen des Unternehmens, bezüglich der IT-Security ständig an das Unternehmensumfeld an. Der Bezug zur IT-Sicherheit von Systemen wird über deren Bedeutung für die als Voraussetzung zum Erreichen der strategisch-operativen Zielsetzungen des Unternehmens gesehene strategisch-operative Beweglichkeit/Handlungsbefähigung (bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander) hergestellt.

5 Methoden für ein Gefährdungspotenzial-orientiertes Management der IT-Security zum Erreichen und Aufrechterhalten eines angemessenen, wirtschaftlich vertretbaren IT-Security-Niveaus

Management bedeutet im Allgemeinen Planung, Ausgestaltung, Steuerung und Kontrolle der Zielerreichung: Management bzw. Unternehmensführung entfaltet u. a. eine Gestaltungsfunktion: Schaffung eines institutionellen Rahmens als Basis einer kontinuierlichen Überlebens- und Handlungsfähigkeit. Die Unternehmensziele bilden dabei den Ausgangspunkt sämtlicher Gestaltungsmaßnahmen.[1] Unternehmerische Prozesse sind so zu managen, dass festgelegte bzw. vorgegebene Anforderungen an die Produkte/Dienstleistungen erreicht werden. Außerdem soll auf intern oder extern bedingte Änderungen der Prozesse oder der Anforderungen an die Produkte/Dienstleistungen in „angemessener" Zeit reagiert werden können.[2] Im Rahmen der Koordination und Unternehmenssteuerung sind eine Ressourcenplanung für anstehende Risikomanagementaufgaben durchzuführen sowie die Steuerungsinstrumente zu beurteilen.[3]

Das IT-Management soll „eine Infrastruktur bereitstellen, mit der sich eine für alle Ebenen des Unternehmens geeignete Informationsstruktur realisieren lässt".[4] Der Erfolg des IT-Managements muss dabei an seinem Beitrag zur Umsetzung der Unternehmensstrategie gemessen werden.[5]

Strategisches Management kann definiert werden als bewusstes Aufbauen und Sichern von Erfolgspotenzialen.[6] Das Management der Unternehmensstrategie muss also u. a. auf dem Suchen neuer Geschäftsmöglichkeiten basieren, um „Erfolgspotenziale aufzubauen und die Unternehmensexistenz zu sichern".[7] Dieses bezieht neben umfassender Berücksichtigung technologischer, ökonomischer, politischer und sozio-psychologischer Umweltbedingungen auch unternehmensinterne Größen (Systeme und Strukturen) und deren Gestaltungsmöglichkeiten mit ein.[8] Das Management von Strategien beschäftigt sich mit der Entwicklung, Gestaltung, Steuerung, Operationalisierung, Umsetzung und Etablierung wertsteigender Strategien in einer Organisation.[9] Ein Teilbereich ist dabei z. B. das Management der Qualität

[1] vgl. Wolf, Klaus (2003b), S.18
[2] vgl. Löbel, Jürgen (2005):, S.32
[3] vgl. Ibers, Tobias (2005), S.52
[4] Hasenkamp, Ulrich (2003), S.206
[5] vgl. Kearney, A..T. (2005)
[6] vgl. Eschenbach, Rolf (2003), S.10
[7] Seidenschwarz, Werner/Huber, Christian (2002), S.135
[8] vgl. Hanke, Thomas (2006), S.12
[9] vgl. Seidenschwarz, Werner/Huber, Christian (2002), S.134

der Strategieprozesse: Im Rahmen der Strategieentwicklung sind „Qualitäts- und Anwendungsstandards in Bezug auf Vorgehensweise und Instrumente“ zu gestalten.[1]

Erfolgreiches Strategiemanagement muss in der Lage sein, das „Spannungsfeld zwischen Gegenwarts- und Zukunftsorientierung zu gestalten“.[2] Die strategische Führung der Unternehmung verlangt dazu, ausgehend von der Erforschung der auf die Umweltdynamik wirkenden Kräfte u. a. eine Konzentration strategischer Analysen auf kritische Bereiche, ein Denken in Alternativen und Wenn/Dann- Konstellationen.[3]

Wird die IT-Security-Strategie als geschäftsübergreifende Unternehmensstrategie gesehen, so ist es demnach das Ziel des strategischen IT-Security-Managements, neue Geschäftsmöglichkeiten und entsprechende Geschäftsmodelle mit zugehörigen Erfolgspotenzialen zu ermöglichen bzw. abzusichern, das bewusste Aufbauen und Sichern von Erfolgspotenzialen zu unterstützen. Dies kann konkret durch die Unterstützung des Managements der IT-Projekte (was Gegenstand des strategischen IT-Managements ist) im Sinne der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume geschehen.

Managementprozesse müssen kontinuierlich auf Veränderungsbedarf geprüft werden, um so Strategien für die zukünftige Geschäftstätigkeit zu definieren und umzusetzen.[4]

Der hier entwickelte Ansatz basiert auf der systemisch-evolutionären Ausrichtung[5] der Managementtheorie. Aus dieser werden folgende spezifische Aspekte im Umgang mit der Komplexität bezüglich des Umfelds und der Ungewissheit der zukünftigen Entwicklung übernommen:

- Lenkung des Gesamtsystems unter Akzeptanz der Komplexität und damit verbundener Unvollständigkeit der Information und des Systemverständnisses
- Erfassung der Systemstrukturen und Hinweis auf verschiedene Verhaltensmöglichkeiten

Das Konzept der systemorientierten strategischen Modelle ist von der Begründung und Erhaltung der Handlungsfähigkeit des Unternehmens mit seiner Umwelt geprägt. Im Mittelpunkt stehen die Interdependenzen des Systems Unternehmen mit dessen Umfeld, Erfassung

[1] Seidenschwarz, Werner/Huber, Christian (2002), S.135
[2] Seidenschwarz, Werner/Huber, Christian (2002), S.135
[3] vgl. Hinterhuber, Hans H. (2004a), S.16-,17
[4] vgl. Scheer, August-W.(2004), S.156
[5] vgl. Eschenbach, Rolf (2003), S.8

der Systemstrukturen und die Analyse der Auswirkungen, Rück- und Wechselwirkungen verschiedener Verhaltensmöglichkeiten. Strategie reduziert sich auf eine Steuerung der (strategischen und operativen) Anpassungsbereitschaft.

Das evolutionäre strategische Management hat die Aufgabe, Unternehmen „in einem maximal adaptionsfähigen Zustand zwischen starrer Ordnung und unberechenbarem Chaos zu halten".

Um den Wettbewerb in turbulenten Umgebungen konkurrierender Unternehmen erfolgreich zu bestehen, muss das Unternehmen seine eigene Adaptions- und Innovationsfähigkeit erhöhen. Dem Management kommt die Aufgabe zu, die Bedingungen optimaler Anpassung zu fördern. Zu den erfolgreichen Managementstrategien in turbulenten und durch schnellen Wandel der Technologien geprägten Umfeldern gehören beispielsweise Projektgruppen, die sich durch eine klare Strukturierung von Prioritäten und Verantwortlichkeiten sowie durch extensive Kommunikation und Gestaltungsfreiheit auszeichnen.[1]

Methodisch muss sich das auf der systemisch-evolutionären Ausrichtung der Managementtheorie basierende strategische IT-Security-Management also auf die Anpassung an das Umfeld sowie die Begründung und Erhaltung der Handlungsfähigkeit des Unternehmens in seinem Umfeld konzentrieren.

Das operative Management hat Ziele und Maßnahmen für die einzelnen Funktionsbereiche des Unternehmens zu konzipieren und zu implementieren sowie Beziehungen zwischen den einzelnen Funktionsbereichen abzustimmen.[2]

So ist die Auswahl und Einführung von Sicherheitsstandards ein wichtiger Teil des IT-Sicherheitsmanagements/operativen IT-Security-Managements. Dabei werden die sicherheitsrelevanten Aspekte des IT-Betriebs an dem Sicherheitsstandard ausgerichtet. Die Einführung des Sicherheitsstandards erfolgt nach dem PDA (Plan-Do-Act) -Vorgehensmodell (umgesetzt z. B. im PDCA-Zyklus der ISO 27001) des gewählten Standards, wobei die einzelnen Schritte verschieden stark ausgeprägt sein können und vor Einführung auf ihre Relevanz geprüft werden müssen.[3]

Ziel des operativen IT-Security-Managements ist es, ein angemessenes, wirtschaftlich vertretbares Niveau der IT-Security für das Unternehmen/die Behörde zu erreichen und zu bewahren.[4]

[1] vgl. Kappelhoff, Peter (2002), S.67,68
[2] vgl. Mieschke, Lutz (2003), S.38
[3] Seidenschwarz, Werner/Huber, Christian (2002), S.135
[4] vgl. Horster, Patrick. (2002a), S.258-270

Mit zunehmender Beschleunigung von Veränderungen und der Notwendigkeit zur Risikobewältigung wird die unternehmerische Flexibilität zur Wahrung der Handlungsfreiheit immer wichtiger. Die unternehmerischen Strategien sind mit den Zielen und Rahmenbedingungen für die Funktionsbereiche und regionalen Einheiten, der Prozess-orientierten Organisation, der operativen Planung und der Motivations- und Überwachungssysteme zu integrieren und zu harmonisieren.[1]

Das hier zu entwickelnde Management der IT-Security soll u. a. die Stabilität des Zustands IT-Security gewährleisten und zum Erreichen und Aufrechterhalten eines angemessenen, wirtschaftlich vertretbaren IT-Security-Niveaus beitragen. Dazu kann sich das operative IT-Security-Management an den Prinzipien zum Management des Unerwarteten orientieren.

5.1 IT-Security-Management-Ansätze

Sicherheitsmanagement bezieht sich auf das Gesamtunternehmen, seine Prozesse und seine Ressourcen. Es erstreckt sich auf alle Bereiche der Sicherheit, vom Objektschutz über die Geschäftsprozesse, die Arbeitssicherheit bis hin zum Personenschutz.[2]

Ziel des IT-Security-Managements ist, die Erreichung der Geschäftsziele so weit, wie der IT dies möglich ist, zu gewährleisten, unabhängig von möglichen negativen internen oder externen Einflüssen oder dem Ausfall von IT-Komponenten. Interne Einflüsse werden von innerhalb der Organisation getroffenen Entscheidungen ausgelöst. Externe Einflüsse resultieren aus der Umgebung, in der die Geschäftsprozesse ablaufen. Aus der Business-Perspektive betrachtet, soll der Security-Management-Prozess ein hohes Maß an Vertrauen erzeugen, sodass das für die Geschäftszwecke und die Geschäftspartner ausreichende Niveau an Vertraulichkeit, Integrität und Verfügbarkeit gewährleistet ist.[3]

Der Security-Management-Prozess gemäß ITIL (IT Infrastructure Libary) umfasst [4]

- Verfahren zur Entwicklung und Implementierung sog. Security-Pläne einschließlich der zugehörigen Prozesse und Handlungsfelder
- Kontroll- und Pflegeverfahren sowie den Prozess zur Nutzung und Implementierung der Auswertungsergebnisse für die Pflege der Security-Pläne

[1] vgl. Hinterhuber, Hans H. (2004a), S.16-,17
[2] Müller, Klaus-Rainer (2003), S.13-14
[3] vgl. Cazemier, Jacques A./Overbeek Paul L./ Peters, Louk M.C. (2004), S.12,13
[4] vgl. Bernhard, Martin G. (2005), S.104-138

- die Struktur des Berichtswesens bzw. Reportings gegenüber den Kunden

Der „Security-Plan“ ist ein Implementierungsplan mit Maßnahmen, die aus der Informationssicherheitspolitik abgeleitet wurden. In ihm sind außerdem Maßnahmen aufgrund der Risikoanalyse und die spezifischen Business Sicherheitsanforderungen beschrieben.

Der Standard ISO/IEC 20000/BS 15000 bietet eine eindeutige Möglichkeit, die Qualität des IT-Service-Managements nach ITIL zu „messen“. Eine Anzahl von Maßzahlen zur Überwachung und Messung des Servicemanagements zu entwickeln, ist durch Verwendung entsprechender ITIL-Kompomenten möglich. Mit der ISO 20000, die sich inhaltlich an ITIL-Prozessen orientiert, wird dem Unternehmen selbst ein Zeugnis ausgestellt. Die Wettbewerbsfähigkeit der IT-Organisation soll so mittels Zertifikat nachweisbar werden. Insgesamt ist das Securitymanagement gemäß ISO/IEC 20000 und ITIL ein professioneller Prozess zur Einführung und dauerhaften Aufrechterhaltung der Informationssicherheit im Unternehmen. Es erfordert – falls nicht vorhanden – den Aufbau von entsprechenden Serviceprozessen über das Organisationsgefüge hinweg.

In diesem Zusammenhang ist der ISO/IEC TR 13335 „Management of information and communications technology security“ (MICTS) (früher „Guidelines on the Management of IT-Security“ (GMITS)) zu erwähnen, der sich als allgemeine Leitlinie für die Initiierung und Umsetzung des IT-Sicherheitsmanagement-Prozesses versteht und die Organisation und Umsetzung von IT-Sicherheit in Form eines Leitfadens behandelt. Er beschreibt die „Konzepte und Elemente von IT-Sicherheit bzw. des IT-Sicherheitsmanagements sowie deren Beziehungen zueinander“, bietet aber keine Lösungsansätze für die Organisation und Umsetzung von IT-Sicherheit. Er soll jedoch eine „Standardisierung der IT-Sicherheit und eine Grundlage für die Bewertung des IT-Sicherheitsniveaus“ schaffen.[1] So stellt der ISO 13335 die Integration des Securitymanagements in das Gesamtkonstrukt „Management“ dar.

Die Sammlung von derzeit drei "Technical Reports" (Information technology – Guidelines for the Management of IT-Security) liefert Hilfen für das IT-Sicherheitsmanagement:

Teil 1 "Concepts and models for information and communications technology security management“ beschreibt

- Konzepte und Modelle der möglichen IT-Sicherheitsstruktur, abhängig von der Form der zu betrachtenden Organisation (Grundbegriffe, Konzepte und Modelle der IT-Sicherheit und grundlegende Aspekte (Bedrohungen, Risiken, Schwachstellen etc.) sowie Prozesse (z. B. Notfallvorsorge, Risikoanalyse, Sensibilisierung)) und

[1] BITKOM (2005), S.17,18

- Aufgaben und Problemstellungen, die eine Organisation behandeln muss, wenn sie ihr IT-Sicherheitsprogramm erstellt oder ändert (verfeinert die Schritte des IT-Sicherheitsprozesses und gibt Hinweise zu Methoden und Techniken, die dafür genutzt werden können).

Teil 2 " Techniques for information security risk management" beschreibt

- das nötige Risikomanagement und Vorgehensweisen zur Ermittlung geeigneter Schutzmaßnahmen auf Basis der gewählten Vorgehensweise (gibt Hinweise zur Planung, Gestaltung und Management des IT-Sicherheitsprozesses, seiner Integration in bestehende Unternehmensprozesse und schlägt eine IT-Sicherheitsorganisation vor),
- Verweise zu detaillierten Hilfsmitteln und Maßnahmenkatalogen, die im Rahmen der gewählten IT-Strategie zur Auswahl kommen können (gibt Hinweise zur Auswahl von Sicherheitsmaßnahmen, welche Maßnahmen für welche Bedrohungen in Betracht kommen und wie z. B. ein angemessenes Grundschutzniveau der Organisation bestimmt werden kann).

Die früheren Teile 3 und 4 sind in den jetzigen Teilen 1 und 2 aufgegangen. Teil 5 „Management guidance on network security“ (gibt Hinweise zum Management der Sicherheit in Netzwerken) wurde im Rahmen der Revision der GMITS zu MICTS dem Projekt "ISO/IEC 2.nd WD 18028-1: 2003, Information technology – Security techniques – IT network security – Part 1: Network security management" hinzugefügt und aus ISO/IEC 13335 entfernt.

Die einzelnen Teile geben keine Vorgehensweisen und Lösungen vor, sondern geben Hinweise, wie diese für das Unternehmen entwickelt und angepasst werden können und welche Methoden und Modelle dafür zur Verfügung stehen. Der Standard beansprucht auch nicht, zur Messung eines IT-Sicherheitsniveaus genutzt oder in anderer Weise zum Nachweis einer Normkonformität herangezogen zu werden, er kann zu diesem Zweck nicht benutzt werden.[1]

Zur Erreichung seiner Ziele hat das Management ein Managementsystem zu entwickeln. Dieses ist durch ein Informationssystem zu unterstützen, das dem Managementsystem die Durchführung seiner Aufgaben ermöglicht.[2] Im Folgenden wird untersucht, welche Konzepte eines Managementsystems zur effektiven Koordination der Aktivitäten einer Organisation bis hin zur Überwachung und Steuerung der Zielvorgabe, Umsetzung und Zielerreichung auf ein solches Informationssystem übertragen werden können.

[1] vgl. Initiative D21 e.V. (2002), S.13
[2] vgl. Leitch, Robert A. (1992), S.21

5.1.1 Orientierungs- und Einordnungsmöglichkeiten in übergeordnete Management-Ansätze

Es ist unbestritten, dass sich auch die IT an der strategischen Ausrichtung des Unternehmens zu orientieren hat. Darüber hinaus kann auch die IT-Security als „Enabler“ von Geschäftsmodellen/-möglichkeiten betrachtet werden (z. B. bezüglich der Möglichkeiten des Internets). Andererseits ist die IT-Security ein Managementprozess. Für diesen Managementprozess ist daher zu überlegen, inwieweit er nach ähnlichen oder den gleichen Konzepten geplant und umgesetzt werden kann, wie die den Geschäftsmodellen/-möglichkeiten zugrunde liegenden Business-Prozesse.

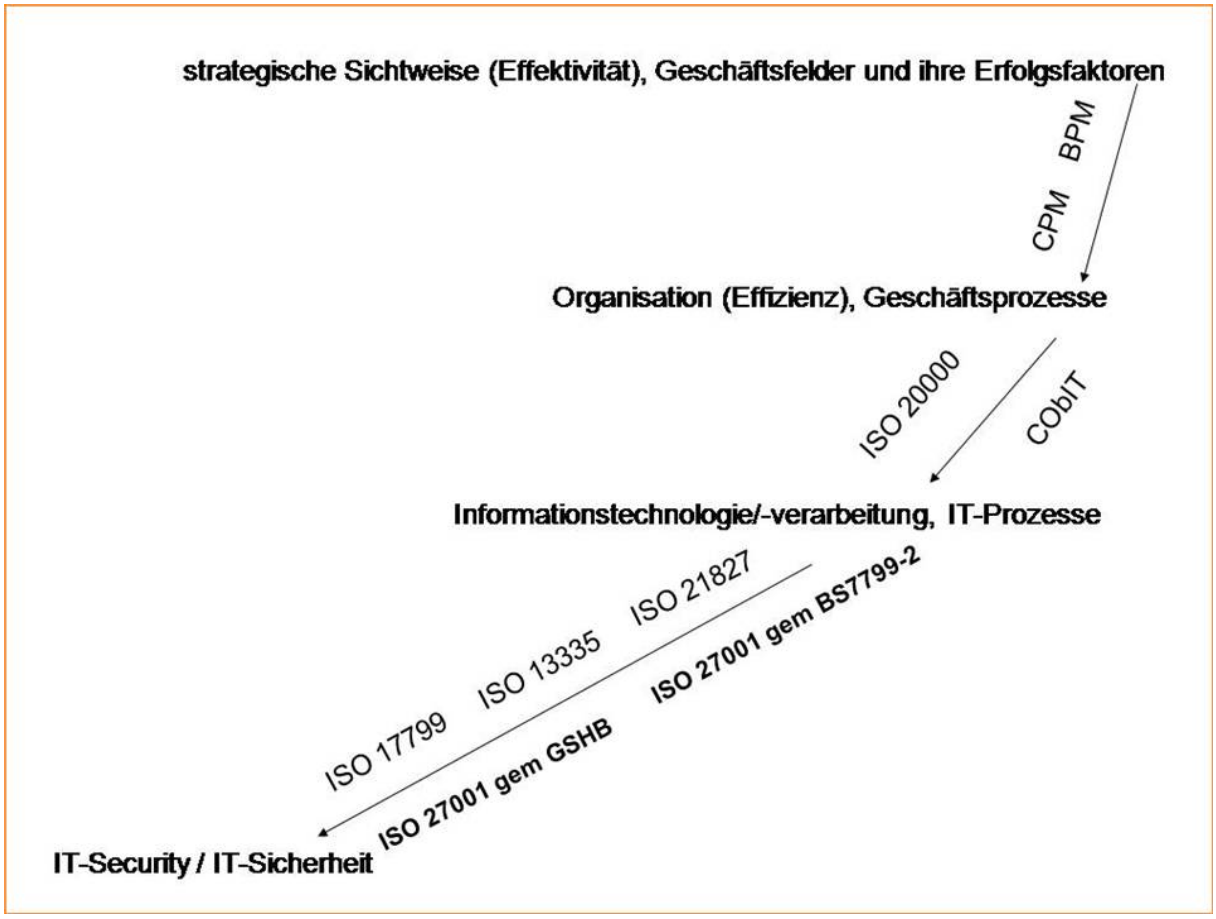


Abb. 11 „Pfad“ von der Strategieebene zur Ebene der IT-Sicherheit

Der klassische „Pfad“ von der Strategieebene zur Ebene der IT-Sicherheit geht über die Ebene der Organisation (Effizienz), Geschäftsprozesse sowie über die Ebene der IT-Prozesse, Informationsverarbeitung, IT-Infrastruktur, Informationstechnologie. Die Ebene der strategischen Sichtweise, der Geschäftsfelder und ihrer Erfolgsfaktoren wird mit der Ebene

der Organisation und der Geschäftsprozesse durch das Business Process Management (BPM) und das Corporate Performance Management (CPM) verbunden.

Existierende Frameworks, die Geschäftsprozesse mit IT-Prozessen (auch unter Berücksichtigung von IT-Sicherheitsanforderungen) verbinden, sind etwa CObIT und ITIL (ISO 20000). Der IT-Security-Managementprozess kann so in das Management von sicherheitskritischen Business-Prozessen eingeordnet werden. Von der Ebene der IT-Prozesse gelangt man schließlich über IT-Sicherheitsstandards wie die Guidelines for Management of IT-Security (ISO 13335), information security management (ISO 17799) und das Grundschutzhandbuch (GSHB) auf die Ebene der IT-Security/IT-Sicherheit. Diese IT-Sicherheitsstandards stellen ihrerseits Anforderungen an die Informationstechnologie/-verarbeitung, welche die IT-Prozesse auf der Ebene darüber unterstützt.

5.1.1.1 Business Integration und Business Process Management

Für ein effektives und effizientes Management neuer und sich schnell verändernder Geschäftsfelder ist die Verbindung der Geschäftsprozesse mit den Unternehmensstrategien entscheidend. Effizienz der Managementprozesse verlangt eine konsequente Umsetzung der Unternehmensstrategien und der strategischen Ziele anhand operativer Maßnahmen. Die internen und unternehmensübergreifenden Abläufe müssen gepflegt und optimiert werden, um Wettbewerbsfähigkeit und das Überleben am Markt zu sichern. Zur Gewährleistung des Unternehmenserfolgs gilt es, auf veränderte Marktanforderungen flexibel reagieren zu können. In diesem Sinne steht Business Process Management für eine kontinuierliche Anpassung der Geschäftsprozesse und damit der Organisation und der IT-Landschaft an die Anforderungen des Marktes. BPM unterstützt den gesamten Lebenszyklus von Geschäftsprozessen. Aufbauend auf der Business Process Strategy erfolgen Design (Gestaltung), Implementierung (Überführung in IT) und Controlling (Messung und Bewertung) von Geschäftsprozessen. Die Business Process Strategy bildet die Grundlage für die Ausrichtung der Geschäftsprozesse an der allgemeinen Unternehmensstrategie. Business Process Management baut auf den Zielsetzungen der Business Process Strategy auf. BPM-Lösungen helfen Unternehmen

- ihre Geschäftsprozesse auf einer einheitlichen technischen Basis zu modellieren
- die Prozesse in ihrer IT-Infrastruktur zu implementieren und
- sie auf Basis Prozess produzierter Daten zu überwachen und zu implementieren

Managementansätze, um ein kontinuierliches und erfolgreiches Strategiemanagement aufzubauen, sind z. B. der Balanced Scorecard (BSC)-Ansatz oder aber der ARIS Value

Engineering (AVE)-Ansatz. Im Sinne des BSC-Ansatzes ist ein klares Design der Strategie und ihrer Ziele aus verschiedenen Perspektiven notwendig. Die in der Business Process Strategy definierten Zielsetzungen lassen sich anhand von Strategy Management-Systemen transparent für das Management darstellen.[1]

Aus Geschäftssicht stellt die IT Applikationen bereit, die die Geschäftsprozesse unterstützen. Applikationen benötigen eine IT-Infrastruktur, damit sie funktionieren können (Hardwarekomponenten, Netzwerke und Software zum Betrieb dieser Hardwarekomponenten sowie Software, die nicht zum Betriebssystem gehört, aber keine direkte Unterstützung der Geschäftsprozesse darstellt).

Entscheidend um schnell und effizient auf Veränderungen an unternehmensrelevanten Märkten reagieren zu können, ist die IT-Infrastruktur. Die Kernprozesse des Unternehmens sollen die Strategie optimal unterstützen („Structure follows strategy"). Geschäftsprozessmodelle sind dabei eine wichtige Voraussetzung, die in der Infrastruktur ablaufenden Geschäftsprozesse zu beherrschen und jederzeit auf Änderungen schnell reagieren zu können. Business Process Management (BPM) verbindet die strategische Sichtweise „die richtigen Dinge tun" (Effektivität) mit der dahinter stehenden Organisation „die Dinge richtig tun" (Effizienz)[2] sowie Geschäftsfelder und ihre Erfolgsfaktoren mit den für die Wertschöpfung notwendigen Geschäftsprozessen und -zielen.[3] Dabei kann BPM als Teil der Business Integration aufgefasst werden. Diese kann in die Schichten Daten-Integration, Applikationsintegration, Business Process Management und den Process Management Portalen (Mensch-Maschine Schnittstelle zu den Geschäftsprozessen) aufgeteilt werden.

Mit Integrationslösungen sollen Informationen und Funktionalitäten vorhandener IT-Systeme in über Applikationen und Geschäftsprozesse hinweg gemeinsam nutzbare unternehmensweite Ressource umgewandelt werden. Es wird ein dynamisches Verfahren benötigt, um zuvor unabhängige Geschäftsprozesse zu standardisieren, zu integrieren und zu verwalten, sodass Unternehmen schnell auf geschäftliche Veränderungen reagieren können. Das Potenzial der implementierten Systeme muss optimiert und die Systeme und Prozesse müssen harmonisiert werden. Die Harmonisierung soll den in vielen Unternehmen vorzufindenden „Wildwuchs der Systeme" eindämmen.[4] Durchgängigkeit und Konsistenz der Harmonisierung von strategischem und operativem Controlling müssen dabei über alle Ebenen der Unter-

[1] vgl. IDS Scheer AG (2005)
[2] vgl. Scheer, August-W (2004), S.20
[3] vgl. Scheer, August-W (2004), S.20
[4] vgl. Mieschke, Lutz (2003), S.29

nehmenssteuerung sichergestellt werden.[1] Dieser Ansatz strebt die Integration aller Managementprozesse und ihrer unterstützenden Systeme zu einer konsistenten Plattform an. Isolierte Datenhaltung abteilungsspezifischer IT-Landschaften ist zu einem konsistenten, Enterprise-wide Datawarehouse zu konsolidieren.[2]

Die Integration der im Unternehmen eingesetzten IT-Lösungen und die unternehmensübergreifende Datenintegration können mittels einer Service-orientierten Architektur (SOA) gelöst werden. Die Anwendungslandschaft soll aus lose gekoppelten Anwendungsbausteinen mit klar modellierten Schnittstellen bestehen, die über wohl definierte Services miteinander kommunizieren.[3] Mit einer Service-orientierten Architektur sowie einer ganzheitlichen Sicht auf Informationen erzielen Unternehmen Effizienzvorteile auf Geschäftsprozessebene. Dabei ist die effiziente und sichere Übertragung von Nachrichten und Informationen ein wesentliches Qualitätskriterium. Dazu muss eine hohe Performance der XML verarbeitenden Systeme durch Bereitstellung entsprechender Ressourcen gewährleistet werden. Um die Daten des Unternehmens gemeinsam und vollständig nutzbar zu machen/einheitliche Sichten auf Daten unterschiedlicher Quellen zu gewährleisten, müssen Informationen mit Metadaten und semantischen Informationen verknüpft werden. Hierfür führen Metadaten fachliche und technische Daten zusammen.[4] Ein Metadaten-Repository enthält Angaben über die Zugriffsrechte und Service-Inhaber. Damit wird innerhalb einer SOA ein durchgängiges und übergreifendes Sicherheitskonzept realisiert.[5]

Business Process Management-Systeme integrieren Applikationen wie das IT-Asset-Management im Rahmen des IT-Service-Managements in Unternehmensgesamtabläufe und bieten damit eine ganzheitliche Prozessdarstellung. Die Kernelemente und Hauptziele von BPM-Systemen (Transparenz, Automation, schnellere Durchlaufzeiten, ganzheitliche Prozesse) können Service-Prozesse entscheidend voranbringen: Für qualitativ hochwertige IT-Services ist es wichtig, Änderungen der Bedürfnisse des Kunden schnell zu erfassen und diese Informationen schnell an die relevanten Prozesse weiterzuleiten. Effizientes IT-Service-Management beseitigt die Barriere zwischen Business und IT, indem es die IT an den Kerngeschäftsprozessen ausrichtet, und trägt so zur Erreichung strategischer Unternehmensziele bei. Grundlage dafür kann neben einem geeigneten Management der relevanten Prozesse in Form einer Business Process Management Software-Lösung zur Integration von Systemen auch ein IT-Asset-Management der relevanten Daten sein. Das IT-Asset-Management verwaltet Hard- und Software-Ressourcen und kommuniziert mit Systemmanagement-Tools und

[1] vgl. Scheer, August-W (2004), S.158
[2] vgl. Scheer, August-W (2004), S.157
[3] vgl. Nandico, Oliver F. (2004)
[4] vgl. Zimmermann, Christian (2005)
[5] vgl. Streiblich, Karl-H../ Parthier, Ulrich (2005)

ERP (Enterprise Ressource Planning)-Systemen (zur Abbildung der sich in den Prozessen des Unternehmens und den dahinterliegenden Daten wiederspiegelnden Wertschöpfungskette, um die Betriebsabläufe zu planen, steuern und auszuwerten) zwecks automatischem Informationsaustausch. Das System fungiert als zentrale Informationsplattform für Daten aus verschiedenen Systemen und ermöglicht einen schnellen Überblick über Soll und Ist. Entscheidend ist dabei die im IT-Asset-Managementsystem enthaltene Datenqualität. Durch die ganzheitliche Prozessabwicklung mithilfe eines BPM-Systems lassen sich Inkonsistenzen in den Daten, aufgrund der unterschiedlichen in die Prozesse eingebundenen Arbeitsschritte und Systeme, vermeiden. Die im IT-Asset-Management geführten Informationen verschaffen z. B. dem Agent des Service-Desk beim Incident Management einen Wissensvorsprung zur Fehlerdiagnose ohne aufwendige Recherche in mehreren Informationsquellen. Auch die vorbeugende Problembehandlung kann vom IT-Asset-Management profitieren, z. B. bei der Überprüfung, welche PCs bei der Einführung eines neuen Software-Release mit zu wenig Arbeitsspeicher ausgestattet sind. Zudem dienen auf die im IT-Asset-Management geführten Informationen aufsetzende „Eskalationsmechanismen“, die den zeitlichen Ablauf der Prozesse überwachen und bei sich anbahnenden Problemen Alarm auslösen oder direkt eine Lösung herbeiführen, dem Ziel der Einhaltung von Service Level Agreements.[1]

Bei den Process Management Portalen sind vor allem Fragen der Information Supply Chain von Bedeutung: Ausgehend von dem unbeschränkten Zugriff auf alle Datenquellen ist ein Lieferungskonzept von den operativen Systemen in das Datawarehouse erforderlich. Die analytischen Anwendungen für die einzelnen Fachabteilungen müssen in ein allgemeines Nutzenkonzept eingebunden werden.[2] Ein „Single Point of Access and Control“ soll den einzelnen Anwendern den Zugang zu allen Anwendungen bieten sowie die Zusammenarbeit und den Informationsaustausch ermöglichen.[3] Dieser Informationsaustausch kann mit web- und Workflow basierten Systemen effizient gestaltet werden. Alle Unternehmensbereiche sollen mit den für sie wichtigen Informationen aus allen relevanten Quellen versorgt werden.[4] Es geht darum, das Wissen im Unternehmen besser nutzbar zu machen und damit gewinnbringender einzusetzen.

Mit den Geschäftsprozessen in einer Organisation wird die Organisation zunehmend von einer gut funktionierenden Informationsversorgung abhängig. In E-Business-Projekten z. B. geht es

[1] vgl. Besemann, Martin (2005)
[2] vgl. Horváth, Peter (2000), S.216
[3] vgl. Scheer, August-W.(2004), S.157
[4] vgl. Horváth, Peter (2000), S.217

u. a. darum, elektronische Dokumente zwischen den Informationssystemen der beteiligten Partner auszutauschen. Für eine Bestellung können dies beispielsweise Anfrage, Angebot, Bestellung und Auftragsbestätigung sein. Die Darstellung, in welcher Reihenfolge welche dieser Dokumente zwischen den zwei beteiligten Systemen ausgetauscht werden, kann hier als Abbildung des gemeinsam durchgeführten Geschäftsprozesses betrachtet werden.

Im BPM-Modell geht es um die Überwachung und Steuerung der Geschäftsprozesse mit Hilfe von Überwachungs- und Steuerungsmetriken.[1] Dabei sind Ablauflogiken laufend anzupassen, damit alle Prozessabläufe verlässlich ineinandergreifen und ein verlässlicher Datenaustausch mit unterschiedlichen Geschäftspartnern entlang gemeinsamer, zielgerichteter Prozessketten zu garantieren. Mitarbeiter kommunizieren und kooperieren über verschiedene IT-Systeme, erbringen und beanspruchen Dienstleistungen, geben Ergebnisse (Informationen, Dokumente, Vorgänge) an andere Prozesse und/oder Mitarbeiter weiter oder fordern diese umgekehrt an. Dazu sind die Prozesse zu bündeln und zu strukturieren, für Vorgänge die richtige Reihenfolge auszuwählen, um die notwendige Transparenz zu schaffen.[2]

Dabei stellt BPM wiederum einen Prozess da, der aus den Phasen Prozessstrategie, Prozessdefinition, Prozessimplementierung und Prozesscontrolling besteht.[3] BPM „im Großen“ hat eine strategische Dimension, eine Geschäftsprozessdimension, eine Architekturdimension und eine Umsetzungsdimension.[4] Während das Unternehmen strategisch in Geschäftsprozessen denkt, handelt die Organisation in Abläufen innerhalb funktional ausgerichteter Abteilungen. Eine ganze Reihe anderer Managementthemen, wie das Projektmanagement[5], Qualitätsmanagement oder das Risikomanagement soll sich über BPM besser darstellen lassen.[6] So haben das Risikomanagement und das IT-Security-Management ebenfalls eine strategische Dimension, eine Geschäftsprozessdimension, eine Architekturdimension und eine Umsetzungsdimension.

Auch BPM ist ein Kreislauf, welcher Planung, Steuerung, Erfolgskontrolle und Anpassung der Prozesse umfasst. Ausgerichtet an den Geschäftszielen erfolgt so die Gestaltung und Steuerung zentraler Geschäftsabläufe.[7] Zum Management des IT-Security-Prozesses bedarf es ebenfalls einer Prozess-orientierten Organisation und eines ganzheitlichen, kontinuierlichen

[1] vgl. Martin, Wolfgang (2004)
[2] vgl. Armbruster, Marcus J. (2005)
[3] vgl. Scheer, August-W. (2004), S.16,17
[4] vgl. Elting, Andreas (2005)
[5] vgl. Melz, Carsten (2005)
[6] vgl. Scheer, August-W. (2004), S.17
[7] vgl. Rother, Tobias (2006), S.53

Ansatzes wie Business Process Management, der organisatorische und technologische Aspekte gleichermaßen behandelt.[1]

5.1.1.2 Business Intelligence und Corporate Performance Management

Unternehmen müssen permanent über alle geschäftlichen Realitäten sowie über Ablauf und Effizienz ihrer Geschäftsprozesse Bescheid wissen, um gezielt agieren zu können. Dies verlangt, dass sämtliche entscheidungsrelevanten Informationen zeitnah und in hoher Qualität verfügbar sind. Zur Ermöglichung effizienter Entscheidungen wird ein Prozess benötigt, der das Zusammenführen und Auswerten von unternehmensweit verfügbaren Daten über Ablauf und Ergebnisse der Geschäftsprozesse ermöglicht.[2] Die Anforderungen der Informationsversorgung, schnelle Beschaffung und Aufbereitung von Informationen, die Sicherstellung, dass die Führungskräfte jederzeit ortsunabhängig auf den jeweils aktuellen Informationsstand zugreifen, und auf dieser Basis schneller und besser entscheiden können, erfordern Informationssysteme, welche unter dem Begriff „Business Intelligence“ zusammengefasst werden.[3] Business Intelligence hat sich in Wissenschaft und Praxis als neue Begrifflichkeit für innovative IT-Lösungen der Unternehmenssteuerung etabliert.[4]

Business Intelligence kann damit umschrieben werden, dass entscheidungsrelevantes Wissen aus Unternehmensdaten oder sonstigen externen Daten mit Hilfe von Informationssystemen aktuell und in hoher Qualität zur Verfügung gestellt werden kann.[5]

Klassische Business Intelligence ist für die Entscheidungsunterstützung im Rahmen strategischer Planung und taktischer Analyse ausgelegt. Aufbauend auf Datawarehouse und Online Analytical Processing (OLAP) als Basistechnologien werden Business Intelligence Systeme als Planungs- und Steuerungsinstrumente zur Unterstützung der Managementprozesse eingesetzt.[6] Es geht dabei neben der Technologieorientierung (Konzepte zur Datenspeicherung oder Analysealgorithmen) um die effiziente Nutzung der Basistechnologien und Werkzeuge zur Überwachung und Verbesserung aller relevanten Geschäftsprozesse.[7]

Es sollen betriebswirtschaftliche Zusammenhänge durch Analysen in unternehmensinternen oder –externen Datenquellen aufgeklärt werden. Unter dem Aspekt der „evolutionären

[1] vgl. Scheer, August-W. (2004), S.16
[2] vgl. Scheer, August-W. (2004), S.156
[3] vgl. Stoi, Roman (2002), S.161
[4] Kemper, Hans-Georg (2006), S.V
[5] vgl. Mieschke, Lutz (2003), S.28
[6] vgl. Scheer, August-W. (2004), S.156
[7] vgl. Scheer, August-W. (2004), S.156

Migration“ ist dabei besonders auf die adäquate Ausgestaltung der betrieblichen IT-Infrastruktur, und der Business Intelligence Quellsysteme zu achten.[1]

Aufsetzend auf der mehrdimensionalen Datenhaltung lassen sich mit OLAP Daten sehr flexibel handhaben und auswerten sowie Szenarien einfach durchrechnen. Bei der Geschäftsabwicklung über das Internet liefert das sog. Web-Log-Mining detaillierte Kundenprofile z. B. zur Planung von Marketingmaßnahmen oder der kundenindividuellen Produktgestaltung.[2]

Der ganzheitliche Business Intelligence Ansatz integriert Planungs-, Budgetierungs- und Controllingprozesse, die mit Instrumenten des Performance Measurement, wie z. B. der Balanced Scorecard verbunden werden.[3] Performance Measurement ist der Prozess der Quantifizierung von Effektivität und Effizienz betrieblicher Leistungen. Als Managementsystem soll die Balanced Scorecard die Strategieimplementierung unterstützen und „Unternehmensziele kaskadenförmig entlang der Organisationsstruktur“ deduzieren.[4]

Dabei erlaubt die Balanced Scorecard dem Management nicht nur verschiedene Perspektiven auf unternehmerische Prozesse, sondern gibt Aufschluss darüber, welche Ursache-/Wirkungsbeziehungen zwischen den Finanzkennzahlen einerseits und den nicht-monetären Kriterien auf der anderen Seite bestehen.[5] Konzepte wie Balanced Scorecard zielen darauf ab, sämtliche Unternehmensaktivitäten in Bezug auf ihre Ergebniswirkung permanent zu überprüfen, zielgerichtet zu bewerten und zu steuern. Es gilt, kontinuierlich die eigene Leistung zu bewerten und flexibel auf Veränderungen reagieren zu können.[6] Die Bewertungszielsetzung dieser Performance Measurement Konzepte ist durch „Aufbau und Einsatz mehrerer und oft zusammenhängender, quantifizierbarer Messgrößen verschiedener Dimensionen (Kosten, Zeit, Qualität, Kundenzufriedenheit), die zur Beurteilung von Effektivität und Effizienz der Leistung und Leistungspotenziale herangezogen werden können“[7], zu erreichen.

Gerade in turbulenten Umfeldern bietet die Balanced Scorecard eine Unterstützung zur Operationalisierung einer neuen oder geänderten Strategie. Dabei erlauben Business Intelligence Anwendungen die Ermittlung und Analyse der einzelnen Kennzahlen. OLAP-Werkzeuge ermöglichen eine mehrdimensionale Auswertung und mit Data Mining können Interdependenzen zwischen den Kennzahlen analysiert werden. Außerdem können Aus-

[1] vgl. Chamoni, Peter (2004)
[2] vgl. Stoi, Roman (2002), S.161
[3] vgl. Scheer, August-W. (2004), S.157
[4] vgl. Wolf, Klaus (2003b), S.85
[5] vgl. Horváth, Peter (2000), S.214
[6] vgl. Scheer, August-W. (2005), S.10
[7] Currle, Michael (2002), S.11

wirkungen der Änderung einer oder mehrerer Maßgrößen auf andere Kennzahlen simuliert werden.[1]

Den gleichen Wert, den Business Intelligence im Bereich der Geschäftsprozesse hat, hat Application Intelligence für die Unternehmens-IT. Application Intelligence hilft IT-Verantwortlichen bei wichtigen Entscheidungen in puncto Anwendungsentwicklung, Wartung, Application Outsourcing und Offshoring.[2]

Im Zuge der Prozessorientierung wird Business Intelligence verstärkt operationalisiert, d. h. vermehrt operative Prozesse einbezogen: Das traditionelle Business Intelligence Paradigma wird immer mehr abgelöst durch einen Analyse-Steuerungs-Regelkreis zur kontinuierlichen, zeitkritischen Abstimmung der Unternehmensziele und Geschäftsprozesse aufeinander. Mit diesem „Corporate (ganzheitlichen) Performance Management“ (CPM) (synonym auch „Business Performance Management“ oder „Enterprise Performance Management“) (nach einer Definition der Gartner Group versteht man darunter „Methodologien, Metriken, Prozesse und Systeme, die dazu dienen, die Geschäftsprozesse eines Unternehmens zu überwachen und zu verwalten“ [3]), wird das Leistungsverhalten der Geschäftsprozesse auf strategischer, taktischer und operativer Ebene geplant, mittels Datenanalyse kurzfristig gesteuert und überwacht. CPM will letztlich eine enge Verbindung von Unternehmensstrategie, Planung, Umsetzung und Controlling schaffen. Die Forderung nach Agilität bedeutet für das Management, Methoden und Werkzeuge zu finden und zu nutzen, um Konsequenzen von Entscheidungen schnell abschätzen und somit flexibel reagieren zu können.[4] Wenn das Erkennen von Ausnahmesituationen zeitkritisch ist, muss CPM dabei im Datenbereich, im Analysebereich und auch im Entscheidungsbereich ausreichend reaktionsschnell sein. Die entsprechenden fachlichen und technischen Konstrukte (Datenintegration, Analyse-Algorithmen und Entscheidungsautomaten) müssen die gewünschte Echtzeit erfüllen können.[5] [6] CPM wird insgesamt als Oberbegriff für nachhaltiges Prozess-orientiertes Denken und Handeln im Unternehmen verstanden.[7]

So wird der gesamte Managementzyklus von der Strategiefindung und entsprechenden Zielableitung bis hin zur Überwachung der Umsetzung betrachtet. In einem kontinuierlichen Prozess werden die eingeleiteten Maßnahmen geplant, mit Hilfe von OLAP sowie Verfahren des Data und Process Mining analysiert und im Rahmen einer Erfolgskontrolle auf ihre Ziel-

[1] vgl. Stoi, Roman (2002), S.165
[2] vgl. Jansen, Dietmar (2006), S.32
[3] Stahlknecht, Peter (2003), S.15
[4] vgl. Scheer, August-Wilhelm (2005), S.V
[5] vgl. Nußdorfer, Richard/Martin, Wolfgang (2005a)
[6] vgl. Nußdorfer, Richard/Martin, Wolfgang (2005b)
[7] vgl. Scheer, August-W. (2005), S.1

erreichung hin gemessen.[1] Im Bezug auf das Management der IT-Sicherheit ist der Regelkreis: Strategische Vorgaben – Konzeptionierung – Umsetzung – Überwachung – Anpassung der Vorgaben. Die praktische Umsetzung der Konzepte und die Überwachung des Einhaltens der Richtlinien können dabei an einen unabhängigen Sicherheitsbeauftragten outgesourct werden, der direkt an die Unternehmensleitung berichtet und Entscheidungsvorlagen erstellt.[2]

Im Prinzip handelt es sich bei den von Business Intelligence Systemen zu erfüllenden Anforderungen der Informationsversorgung um die gleichen Anforderungen wie an die IT-Security, abgeleitet aus den Korrektheitsbedürfnissen der im Unternehmen durchlaufenden Informationen (richtige Informationen sollen zum richtigen Zeitpunkt mit dem notwendigen Genauigkeits- und Verdichtungsgrad am richtigen Ort zur Verfügung stehen). Von daher ist es klar, dass das Management der IT-Security und Business Intelligence Berührungspunkte haben: Prozesse der Beschaffung, Verarbeitung, Speicherung und Übermittlung von Informationen müssen auch den Anforderungen der IT-Security entsprechen, da die Qualität von Planung und Kontrolle von der Qualität der vom Informationssystem bereitgestellten Informationen abhängt.

Darüber hinaus kann der Analyse-Steuerungs-Regelkreis des Corporate Performance Management zur kontinuierlichen, zeitkritischen Abstimmung der Unternehmensziele und Geschäftsprozesse aufeinander auf die dynamische Anpassung des Sicherheitskonzepts eines Unternehmens an die rechtlichen und technischen Anforderungen an die IT-Security, abgeleitet aus den externen und internen Ordnungsmäßigkeitsvorgaben und den potenziellen IT-Bedrohungen, übertragen werden: So sind auch im Bereich der IT-Security in einem kontinuierlichen Prozess die einzuleitenden Maßnahmen zu planen, zu analysieren und im Rahmen einer Erfolgskontrolle auf ihre Zielerreichung zu messen. Als Ergebnis des Zyklus im Regelkreis strategische Vorgaben – Konzeptionierung – Umsetzung – Überwachung – Anpassung der Vorgaben kann so ein gegebenenfalls optimiertes Richtlinienwerk vorliegen.

5.1.1.3 Evolutionärer Anpassungsprozess

Zukunft orientiertes Denken und Handeln erfordert die Möglichkeit, rechtzeitig Anpassungsprozesse einleiten zu können:[3] Auf die laufende Anpassung der Unternehmung an sich ständig ändernde Umstände ist im Grunde genommen auch die Planung auszurichten.[4]

[1] vgl. Scheer, August-W. (2004), S.158
[2] vgl. Kamlah, Bernd (2004b), S.10
[3] vgl. Gadatsch, Andreas (2006), S.3
[4] vgl. Kremin-Buch, Beate/Unger, Fritz/Walz, Hartmut (2004), S.20

Veränderte Markt-/Umfeldbedingungen erfordern von den Unternehmen, auf neue Herausforderungen immer schneller mit entsprechenden Lösungen reagieren zu können. Die IT ist in der Regel Bestandteil dieser Lösungen. Um den Erfolg definierter Maßnahmen nicht zu gefährden, muss daher sichergestellt werden, dass die IT auf geänderte Anforderungen (zeitnah) reagieren kann.[1]

Die Umfeldbedingungen, denen sich Organisationsformen und Unternehmensprozesse dabei anpassen müssen, sind einem ständigen Wandel unterzogen. Zu den Entwicklungen der letzten Jahre, welche die wirtschaftlichen Rahmenbedingungen produzierender Unternehmen gravierend prägen, zählen die Globalisierung und die mit der Dynamisierung der Märkte verbundene stetige Verkürzung der Produktlebenszyklen. Diese gehen einher mit einem durch den technischen Fortschritt bedingten zunehmenden Komplexitätsgrad technischer Systeme. Die Entwicklungen auf dem Gebiet der Informations- und Kommunikationstechnologie schaffen dabei die Voraussetzungen für einen schnellen Informationsaustausch und ein Wirken der Unternehmen über geografische Grenzen hinweg.[2] Das durch die Globalisierung sowie den erhöhten Zeit- und Kostendruck bedingte Risikopotenzial für Fehler im Bereich der Entwicklung und Erstellung von Leistungen, aber auch das durch die Globalisierung und Dynamisierung bedingte Risikopotenzial bei der Formulierung und Umsetzung von Zielen und Strategien nimmt ständig zu. Gleichzeitig steigen die Forderungen der Kunden nach Sicherheit und Zuverlässigkeit z. B. von Produkten. Aber auch das erhöhte Risikopotenzial bei der Formulierung und Umsetzung von Zielen und Strategien stellt höhere Anforderungen. Im Kontext der gegebenen Thematik wird untersucht, wie das erhöhte Risikopotenzial bei der Formulierung und Umsetzung von Zielen und Strategien im Zusammenhang mit IT-Projekten, welche die Geschäftsprojekte und Geschäftsmodelle des Unternehmens unterstützen bzw. ermöglichen sollen, durch die Zuverlässigkeit und Beherrschbarkeit entsprechender IT-Systeme beeinflusst wird.

Die Planung in der Unternehmung – die systematische Gestaltung ihrer Zukunft – hängt weitgehend auch von der Entwicklung ihres Umfelds ab. Die Dynamik dieses Umfelds zwingt u. a. zu höchster Flexibilität bei der Geschäftsfeldplanung, Organisation und Führung. Die Formulierung der Ziele in der Unternehmung unterliegt einem umweltbedingten Wandel.[3] Veränderungen in unseren Umfeldern stellen neue Herausforderungen an entsprechende Führungskonzepte.[4] Es handelt sich dabei um die Ausgestaltung der aus der Koordinations-

[1] vgl. Klement, Peter (2006)
[2] vgl. Dahmen, Jörn (2002), S.15,16
[3] vgl. Hahn, Dietger (2006), S.3-6
[4] vgl. Hahn, Dietger (2006), S.29

funktion des Controllings als Koordination der Führungsaufgabe mit der Umwelt abgeleiteten Anpassungsfunktion.

Der Ausfall wichtiger Geschäftsprozesse kann zu erheblichen Verlusten oder sogar zum Untergang des Unternehmens führen. Die IT hat die Geschäftsprozesse des Unternehmens bestmöglich zu unterstützen.

Der optimale, am besten auf das Umfeld angepasste (best adapted) Einsatz der IT-Technologie wird immer mehr zum Hauptüberlebenskriterium eines Unternehmens. Um das Nutzenpotenzial der IT auf Ebene der Geschäftsprozesse zu erschließen, werden die Strukturen und Prozesse im Unternehmen entsprechend optimiert.[1] Die IT-Services und –Systeme müssen unter Abwägung des technisch-wirtschaftlich Machbaren nach den Kundenanforderungen ausgerichtet werden. Dies ist die Grundidee der IT Infrastructure Library (ITIL) Evolution. Dabei ist ITIL unabhängig von Hardware, Software und Service-Providern. Die Anpassungen (an die individuelle Hard- und Softwareausstattung und Service-Produkte des Unternehmens) bei der organisatorischen Einführung eines ITIL-Prozesses müssen durch das Anwenderunternehmen selbst erfolgen.[2]

Im Zusammenhang mit der enormen Abhängigkeit der Unternehmen von ihrer IT geht es um eine entsprechend optimierte Qualität und Verfügbarkeit der IT-Prozesse. Dieses verlangt ein auf die Anforderungen aus der Umgebung abgestimmtes Maß an IT-Sicherheit. Dieser Prozess, der eine Analyse der Komponenten der Informations- und Kommunikationstechnik (IuK), ihrer Infrastruktur und ihres Umfelds einschließt, evaluiert, welche Sicherheitselemente, Maßnahmen und Konzepte zur Absicherung der IuK u. a. zur Vermeidung von Notfällen und Katastrophen durch Prävention eingesetzt werden können.

Diese so definierte Anpassung des Unternehmens an sich stetig verändernde Umfeldbedingungen, um so die nachhaltige Existenzerhaltung sicherzustellen, ist Aufgabe des kontinuierlichen und dynamischen Risikomanagementprozesses.[3] Unter Berücksichtigung der Risiko- und Ertragspotenziale „die Effektivität und Effizienz eines Unternehmens im Hinblick auf die Sicherung der langfristigen Überlebensfähigkeit zweck- und zielgerichtet zu steuern“ ist Aufgabe des integrierten Risiko- und Ertragsmanagements.[4]

Die Forderung nach Adaptivität bedeutet, vorausschauend agieren sowie schnell und flexibel interne Strukturen und Abläufe ändern zu können. Ziel ist u. a. die

- Verbesserung der Servicequalität und Ausweitung der Serviceverfügbarkeit

[1] vgl. Buchta, Dirk Uwe (2004):, S.15
[2] vgl. Bernhard, Martin G. (2005):, S.96, 97
[3] vgl. Ibers, Tobias (2005), S.71
[4] Keuper, Frank [2005], S.V

- Erhöhung der Wirtschaftlichkeit und Optimierung des Ressourceneinsatzes
- Komplexitätsreduktion und Optimierung der IT-Prozesse

Insgesamt soll eine „größere Flexibilität und Geschwindigkeit in der IT-Organisation sowie schnelle Anpassung an sich ändernde Markt- und Geschäftssituationen“ erreicht werden.[1]

Risikomanagement muss in dem Sinne flexibel sein, dass es auf sich ständig ändernde externe und interne Rahmenbedingungen abgestimmt werden kann. Dies sichert implizit eine angemessene Berücksichtigung von Veränderungen der Risiken bzw. von deren Struktur.[2]

Im Rahmen des Ratings nach Basel II ist für die Banken wichtig zu wissen, welche Betriebe Probleme bei der Anpassung an den Strukturwandel haben. Erfolgreiche Unternehmen müssen die externen Rahmenbedingungen des Betriebs beobachten, analysieren, prognostizieren und daraus neue kreative Problemlösungsansätze ableiten.[3] Dabei ist es nicht mehr ausreichend, auf aktuelle externe Veränderungen durch eine Anpassung der IT nur zu reagieren, sondern die IT proaktiv zu verändern. Als Voraussetzung für einen strukturierten und übersichtlichen Ablauf von Veränderungsprozessen, die i. d. S als Change Management das Unternehmen ständig weiterentwickeln, wird der Aufbau einer Implementierungsarchitektur genannt, der die Implementierung der Veränderungsprozesse quasi standardisiert. Dabei wird die Vorgehensweise zur Erzielung der Veränderung in jeder Prozessphase den Gegebenheiten angepasst.[4] Darüber hinaus muss das Unternehmen sich ständig die Frage stellen, welche Voraussetzungen in der IT gegeben sein müssen, um die Unternehmensstrategie langfristig zu unterstützen.[5] Dazu zählt auch ein adäquates IT-Security-Management. Dieses hat die Umsetzung sich neu ergebender Anforderungen an die IT als Enabler für das Geschäft zu unterstützen (z. B. Ermöglichung schneller Verbindungen zu neu hinzugekommen Unternehmensteilen über mehrsprachige Systeme und offene Architekturen als Voraussetzung für externes Wachstum durch Fusionen und Übernahmen, oder die Unterstützung von E-Business und B2C-Applikationen als Voraussetzung für internes Wachstum durch virtuelle Kundennähe).

Auch das IT-Security-Managementsystem muss sich an relevante Umfeldveränderungen gezielt anpassen. Bei der Beschaffung von Informationen zur Analyse und Prognose von Umfeldveränderungen (für die strategische Planung) kommt dabei dem Aufbau von Früherkennungssystemen eine wichtige Rolle zu. Relevante Umfeldveränderungen sind frühzeitig zu erkennen, um die Strategie rechtzeitig anpassen zu können.

[1] vgl. Heinevetter, Thomas/Schrecklinger, Nicole/Scherf, Alexander (2006)
[2] vgl. Diederichs, Marc (2004), S.57
[3] vgl. Nolte, Bernd (2003), S.79-85
[4] vgl. Kappeller, Wolfgang (2003), S.48-49
[5] vgl. Buchta, Dirk Uwe (2004):, S.17

Evolutionär nennt man z. B. die Entwicklung und Implementierung einer Business Intelligence Lösung (unter Berücksichtigung relevanter Rahmenbedingungen sowie identifizierter Prozesse) durch vertikales Prototyping, wobei jeder Prototyp ein lauffähiges System darstellt. Bevor mit dem eigentlichen Entwicklungsprozess begonnen werden kann, müssen dabei konzeptionelle Vorüberlegungen bestehend aus Umwelt- und Prozessanalysen sowie organisatorischer und fachlicher Konzeption erfolgen. In der Umwelt- und Prozessanalyse werden die externen und die internen Rahmenbedingungen der Systementwicklung sowie deren Einfluss auf das Fachkonzept ermittelt. Der erste Teil des Entwicklungsprozesses entwickelt den ersten Prototypen und besteht aus der Modellierung fachspezifischer Strukturen, deren Implementierung, Schaffung der Infrastruktur und Wahl einer Basisarchitektur.[1]

Auch die Unternehmenskultur (Grundgesamtheit gemeinsamer Wert- und Normvorstellungen sowie geteilter Denk- und Verhaltensmuster) kann nicht willkürlich geformt werden, sondern entwickelt sich evolutionär.

Langfristiges Überleben erfordert ständige Anpassung an sich verändernde Umfeldeinflüsse. Dies bedingt eine Evolution des Planungssystems, das z. B. Unternehmensführung als bewusst gestaltende Aktivität implementiert.[2]

Zwischen Evolutionstheorie[3] und Betriebswirtschaftslehre besteht sowohl bezüglich des Untersuchungsgegenstands (komplexe Systeme) als auch bezüglich des Ziels (Sicherung des langfristigen Überlebens) hinreichend Ähnlichkeiten.[4] Im Folgenden sei angenommen,

- das Unternehmen wird nur solange „überleben“, wie es über eine ausreichende Menge an „organisationalem“ Kapital (Finanzielles Kapital, Soziales Kapital und Humankapital) verfügt.[5]

Unternehmens- und Informationsprozesse sind zunehmend nicht mehr nur auf ein abgegrenztes Informationssystem begrenzt, sondern dehnen sich über System- und teilweise Unternehmensgrenzen hinweg aus. Dabei ist es entscheidend, die be-/verarbeiteten Informationen vor unbefugtem Zugriff zu schützen. Informationsverluste an Wettbewerber bedeuten häufig das Aus für das Überleben am Markt.[6] Weiterhin sei angenommen,

- die IT-Security ist über die Effektivität und Effizienz des IT-Security-Managements ein Bestimmungsfaktor des „organisationalen“ Kapitals.

---

[1] vgl. Goeken, Matthias/Burmester, Lars (2004), S.137-139
[2] vgl. Eschenbach, Rolf (2003):, S.101
[3] vgl. Schreyögg, Georg (2002):, S.116-153
[4] vgl. Sabathil, Kurt (1993), S.62-67
[5] vgl. Woywode, Michael (1998), S.51
[5] vgl. Berninghaus, Siegfied. (2002) , S.270
[6] vgl. Bernhard, Martin G. (2005):, S..95

Mithin kann die Effektivität und Effizienz des IT-Security-Managements das „Überleben“ des Unternehmens beeinflussen.

Im Sinne der Evolution wird nur das Unternehmen überleben (seinen Reproduktionserfolg maximieren), das optimal an seine Umgebung „angepasst“ ist[1] (survival of the fittest, survival of the best adapted).

Nimmt man nun ferner an, dass

- für die Anpassung an die „Umgebung“ die Entwicklung einer IT-Security-Policy – auf Basis derer die IT-Security-Strategie definiert wird, aus der (mit der Aufgabenstellung des IT-Security-Managements) wiederum die benötigte Effektivität des IT-Security-Managements abgeleitet werden – eine wichtige Rolle spielt,

kann eine entsprechende Effektivität des IT-Security-Managements als notwendige Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security bezeichnet werden. Im Folgenden sollen Konzepte zur Gestaltung der Effektivität und Effizienz des IT-Security-Managements hergeleitet werden, sodass die notwendige und gleichzeitig eine noch zu identifizierende hinreichende Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security erfüllt ist. Die hinreichende Bedingung soll an die Effizienz des IT-Security-Managements geknüpft werden.

Business Process Management (BPM) passt die Geschäftsprozesse an die Unternehmensstrategie an. Corporate Performance Management (CPM) „synchronisiert“ die Unternehmensstrategie mit der IT-Strategie. Beide Managementansätze können als evolutionärer Anpassungsprozess gesehen werden.

Einer evolutionären Verbesserung der Geschäftsprozesse dient z. B. das Benchmarking an Geschäftsprozess-Referenzmodellen. Solche Referenzmodelle dienen beim Benchmarking dem methodischen Vergleich des eigenen Geschäftsprozesses mit den sog. „best business practices“. Hierdurch lassen sich Hinweise zur Verbesserung oder gar Optimierung der Geschäftsprozesse gewinnen. Dagegen verlangt eine revolutionäre Änderung der Geschäftsprozesse im Sinne eines dramatischen Veränderungsmodells den innovativen Entwurf neuer Geschäftsprozesse „auf der grünen Wiese“.[2]

Bezüglich des IT-Security-Managements besteht der Anpassungsprozess darin, sich an die aus dem Umfeld des Unternehmens entspringenden IT-Risiken anzupassen. Das Sicherheitskonzept eines Unternehmens erfordert eine dynamische Anpassung an die rechtlichen und

[1] vgl. Berninghaus, Siegfred. (2002) , S.270
[2] vgl. Rosenkranz, Friedrich (2006), S.19

technischen Anforderungen. Es muss konsequent in regelmäßigen Zeitintervallen fortgeschrieben werden.[1]

Auch die Einführung eines generischen IT-Sicherheitsstandards wie dem ISO 17799 im Unternehmen kann als Anpassungsprozess gesehen werden: Der ISO 17799 ist zwar eine umfangreiche Sammlung von Kontrollen und Best-Practices zur IT-Sicherheit, er enthält Standard-Sicherheitsmaßnahmen ohne konkrete Hilfen zur Umsetzung. So werden in den IT-Sicherheitsstandards in Themengebieten Standardsicherheitsmaßnahmen formuliert, die für das einzelne Unternehmen risikoabhängig angepasst werden müssen.

IT-Sicherheit ist keine Konstante im Sinne eines erreichten oder erreichbaren Endzustands. Der Begriff unterliegt einem dynamischen Verständnis. Es handelt sich um einen andauernden Prozess zur Umsetzung der Schutzziele und Anpassung der dabei zu implementierenden Maßnahmen an sich verändernde Umwelt- und Umfeldbedingungen.

Bezüglich der IT-Sicherheit sind neue Systeme so anzupassen, dass sie dem definierten Sicherheitsniveau des Unternehmens entsprechen. Dieses Konfigurationsmanagement sollte auf Grundlage einer konsistenten, unternehmensweiten Sicherheitsarchitektur geschehen. Diese Sicherheitsarchitektur gibt in Form eines technischen Security-Frameworks das gesamte technische Sicherheitsdesign der Infrastruktur des Unternehmens vor. Die Entwicklung dieses Security-Frameworks muss ausgehen von der Geschäftspolitik (die auf Basis der zu erreichenden Geschäftsziele definiert, welche Maßnahmen einzuleiten sind) sowie von Geschäftsregeln und Weisungen, die Sicherheitsmechanismen mit Geschäftsrisiken in Verbindung bringen.

Das IT-Security-Framework, ausgehend von der Geschäftspolitik sowie von Geschäftsregeln und Weisungen, die IT-Sicherheitsmechanismen mit Geschäftsrisiken in Verbindung bringen, verbindet die Strategieebene direkt mit der Ebene der IT-Security/IT-Sicherheit:

Der Analyse und Bewertung der strategischen, zukunftsorientierten Bedeutung der Sicherheit von Informationssystemen auf Basis dieses Frameworks zielt nicht auf die Bewertung der Effektivität oder Effizienz des operativen IT-Security-Managements ab, sondern auf die Beurteilung der Bedeutung der Anforderungen an die IT-Security für die Handlungsfähigkeit/strategisch-operative Beweglichkeit des Unternehmens. Die Handlungsfähigkeit/strategisch-operative Beweglichkeit des Unternehmens zu unterstützen ist Aufgabe des im Folgenden entwickelten strategischen IT-Security-Managements.

[1] vgl. Coester, Ursula/Hein, Matthias (2005), S.97

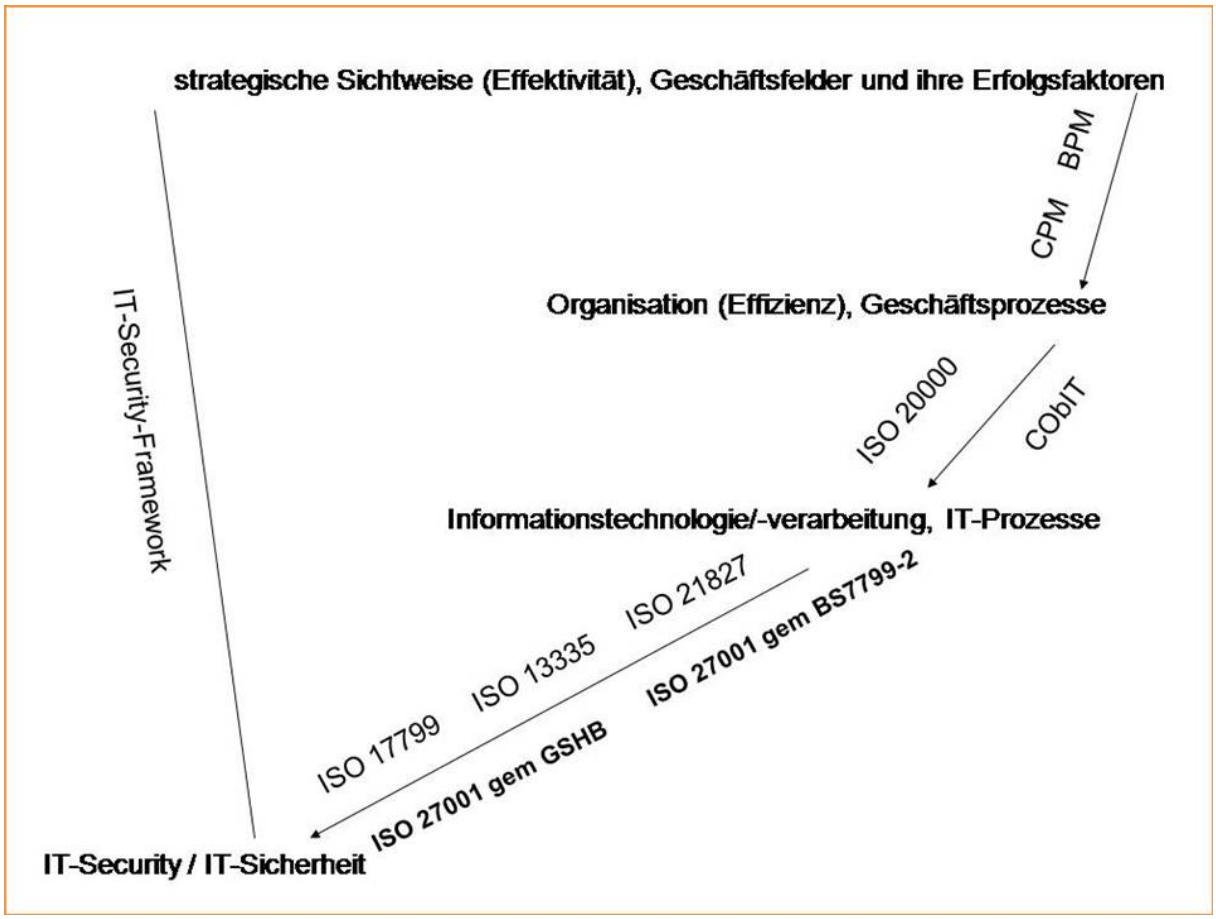


Abb. 12 Direkte Verbindung von der Strategieebene zur Ebene der IT-Sicherheit

Dieses IT-Security-Framework hat die aus der Koordinationsfunktion des Controllings abgeleitete Anpassungsfunktion als Koordination der Führungsaufgabe mit der Umwelt auszufüllen. Konzepte zur Ausgestaltung dieses IT-Security-Frameworks ergeben sich folglich aus Überlegungen zum Anpassungsprozess an das Umfeld des Unternehmens.

Die langfristige Anpassung des Unternehmens an die veränderten Umfeldbedingungen ist auch Ziel der strategischen Unternehmensführung.[1] Es gilt, nicht nur die IT zu verändern, sondern das gesamte Unternehmen einschließlich der Schnittstellen zu Kunden und Lieferanten im Rahmen einer umfassenden „Unternehmenstransformation“ anzupassen, damit die IT ihr Nutzenpotenzial in Bezug auf die Geschäftsprozesse entfalten kann.[2] Das IT-Security-Framework hat diese umfassende „Unternehmenstransformation“ (in Bezug auf die dem Umfeld des Unternehmens entspringenden IT-Risiken) zu unterstützen und einen Rahmen für die Umsetzung dieses Anpassungsprozesses an die Umgebung im Bereich der IT-Security vorzugeben.

[1] vgl. Reichmann, Thomas (2006), S.557
[2] vgl. Buchta, Dirk Uwe (2004), S.16

Diese Umgebung ist durch die zunehmende Digitalisierung von Wirtschaft und Gesellschaft geprägt. So geht es im E-Business aus Sicht des Benutzers um die „webbasierte Digitalisierung von Geschäftsprozessen, mit dem Ziel, schneller und effizienter bessere Produkte und Services für Konsumenten und Kunden, aber auch intern für Mitarbeiter zu identifizieren, zu entwickeln, zu produzieren und zu vertreiben“.[1] Die weltweite digitale Vernetzung macht die Märkte transparent, sie schafft neue Wertschöpfungsketten und Werte, sie ist fester Bestandteil und technische Voraussetzung von E-Commerce, E-Business, E-Procurement (Elektronische Beschaffungssysteme), Colloborative Commerce, Customer Relationship Management und ermöglicht so neue Geschäftsmodelle.[2] Dies fußt auf der IT als Basis für z. B. elektronische Marktplätze, Onlineauktionssysteme, zahlreiche Anwendungen in der Telekommunikation oder im Supply Chain Management (Lieferantenmanagement). So wird die IT zunehmend zum Enabler strategischer Wettbewerbsvorteile. In allen Bereichen des privaten und geschäftlichen Umfelds steigt dabei die Bedeutung des Internets als globale IT-Netzlandschaft. E-Commerce fungiert zunehmend als zusätzlicher Direktabsatzkanal, der den Absatz im klassischen Distanzprinzip übernimmt. Versicherungsunternehmen z. B. führen immer schneller neue Produkte am Markt ein, die durch die IT abgebildet werden müssen. So ist insbesondere ein optimaler Absatz von Services möglich, die ohnehin in digitalisierter Form vorliegen (z. B. Download von Software). Dies senkt einerseits die Marktzugangsbarrieren. Dem stehen jedoch hohe Vertrauensbarrieren gegenüber (z. B. unsichere und komplizierte Bezahlung).[3]

Das Arbeitsumfeld in der virtuellen Welt des Internets bildet die Software, die auf den Netzwerkcomputern läuft. Gegenmaßnahmen bezüglich Gefährdungen dieses Arbeitsumfelds werden auch für virtuelle Bedrohungen auf Computerziele entwickelt (z. B. Firewalls).[4]

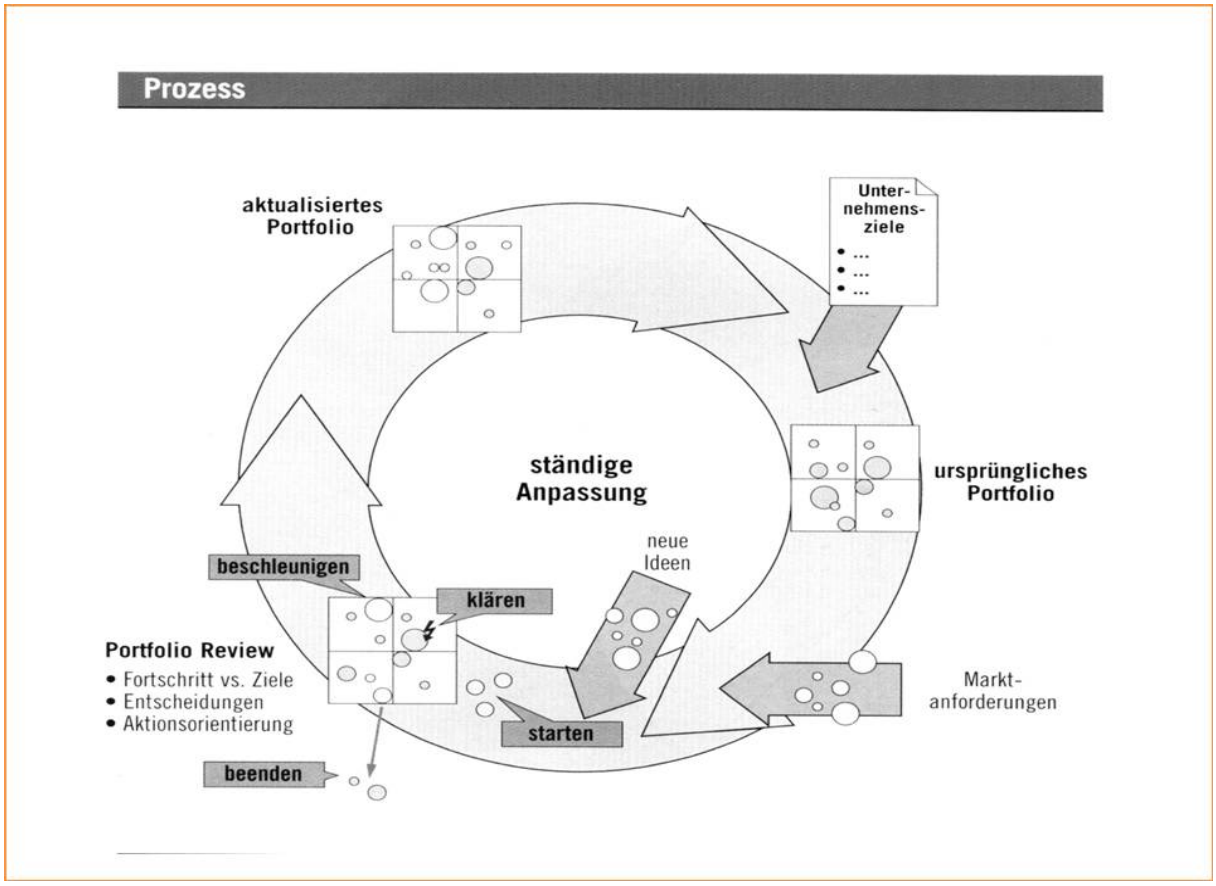
Viele Webanwendungen schaffen mit einer Form von Sessionmanagement eine an den Benutzer angepasste Umgebung. Aus Security-Sicht ist dort die Verknüpfung von Sessions mit Authentifizierung und Autorisierung (Angriffe auf die Integrität der Session) besonders kritisch.[5]

Dabei bietet das Internet nicht mehr nur neue Beschaffungs- und Absatzmärkte für Informationen. Ganze Prozesse können per Internet reengineered werden (z. B. Public Relations zu Online Relations).[6] Mit dem Wunsch nach weltweiter Kommunikation und unbegrenztem Zugriff auf Informationen wachsen etwa die Branchen Mobilfunk und Internet

[1] Dietrich, Lothar (2004), S.305
[2] vgl. Keuper, Frank. (2003), S.251
[3] vgl. Pepels, Werner (2005), S.166
[4] vgl. Schneier, Bruce (2000), S.275-277
[5] vgl. Meisel, Alexander (2006)
[6] vgl. Hermanns, Arnold (2001), S.265-270

zum Mobile Commerce zusammen. Die Endgeräte müssen dabei eine ständige Verfügbarkeit der gewünschten Dienste sicherstellen.[1]

Diese neuen Geschäftsmodelle sind größtenteils mit erhöhten IT-Bedrohungen und IT-Risiken verbunden. Geschäftsprozesse sind vermehrt nicht mehr nur auf das eigene Unternehmen beschränkt. Galt die IT in Managementkreisen früher als Technologie-Center, so hat sie sich zum Competence-Center gewandelt. Geschäftsprozesse binden zunehmend externe Partner wie Kunden, Lieferanten und Provider ein und sind als Ende-zu-Ende Verbindung zu gestalten und müssen von der IT durchgängig unterstützt werden. Die IT-Abteilung wird hier als Berater für die Fachgruppen und das Top-Management aktiv. Die interne IT tritt dabei quasi wie ein externer IT-Service-Provider oder Application-Service-Provider auf, die alle Anwender wie Kunden behandelt.[2]



(Quelle: Betz, Martin (2006), S.11)

Abb. 13 Permanente Anpassung des IT-Projekt-Portfolios

Im Allgemeinen hat das IT-Security-Management eine Vielzahl von organisatorischen und technischen IT-Security-Maßnahmen zu steuern/zu koordinieren. Dabei müssen in der

[1] vgl. Hermanns, Arnold (2001), S.55-64
[2] vgl. Elsässer, Wolfgang (2005), S.113-117

Planung und in der Steuerung Zusammenhänge zwischen entsprechend parallel laufenden IT-Security-Projekten berücksichtigt werden. Im Gegensatz zum allgemeinen IT-Projekt-Portfolio-Managemt[1] besteht zwar kaum die Gefahr, dass die IT-Security-Projekte ihre grundsätzlichen Ziele verfehlen. Konflikte können aber dann entstehen, wenn die innerhalb des Projekts umzusetzenden organisatorischen bzw. technischen Maßnahmen nicht aufeinander abgestimmt sind. Bei technischen Maßnahmen ist im Fall der Nicht-Überschneidungsfreiheit eine unnötige Mehrfachabsicherung und damit eine Unwirtschaftlichkeit zu befürchten.

Das Management dieses Portfolios ist ein Prozess, der in Form eines Regelkreises dieses Maßnahmen-Portfolio permanent anpasst.

Da das IT-Security-Framework von Geschäftsregeln und Weisungen ausgehend zu entwickeln ist, die IT-Sicherheitsmechanismen mit Geschäftsrisiken in Verbindung bringen, soll im Rahmen dieser Überlegungen der funktionale Aspekt des IT-Security-Frameworks als die Aufgabenstellung eines Risiko orientierten zukunftsbezogenen IT-Security-Managements definiert und spezifiziert werden.

Die Effektivität des IT-Security-Managements ist deshalb nicht auch eine hinreichende Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security, weil bei den möglichen Randbedingungen des Umfelds zufallsbestimmte Verhaltensrisiken, welche vor allem die Effizienz (korrekte Ausführung/Umsetzung) beeinflussen können, nicht berücksichtigt werden.

Bei der Betrachtung von nicht zufallsbestimmten Verhaltensrisiken hängt das strategische Verhalten der „Mitakteure“ (Hacker, Angreifer, Saboteure) im Wesentlichen davon ab, was diese über die Ziele und die Strategie der betreffenden Institution zu wissen glauben.[2]

Als strategisches Verhalten der „Mitakteure“ sei ein Angriff (Versuch, unautorisierten Zugang zu einem System zu erhalten mit dem Ziel, Informationen zu verändern, zu zerstören oder zu stehlen oder die Verfügbarkeit eines Dienstes zu unterbrechen) auf das Unternehmen betrachtet: Erster Schritt eines erfolgreichen Angriffs ist die Identifizierung des spezifischen Angriffsziels und Einholen von Informationen über dieses Ziel. Dies ist einfach, wenn die Website des Ziels und/oder Internetdatenbanken alle möglichen Informationen enthalten. Angreifer benutzen dabei viele Techniken, um das Zielnetz auszuspionieren: z. B. Ping-Scans, Port-Scans usw., um herauszufinden, aus welcher Hardware die Computer zusammengesetzt

[1] vgl. Betz, Martin (2006)
[2] vgl. Güth, Werner/Peleg, Bezalel (1997), S.2

sind, welche Software auf ihnen läuft, und welche Dienste sie zulassen.[1] Können die für den Angriff benötigten Informationen nicht eingeholt werden, so kann der Angriff logischerweise auch nicht erfolgreich sein.

Bezüglich der Anpassung an die Umgebung kommt es also zu „survival of the fittest", unabhängig von der Struktur des Umfelds generell (also unabhängig vom Betrachtungsstandpunkt) rational dann, wenn „Mitakteure" nicht auf subjektive Strategieänderungen anderer reagieren, was insbesondere bei völliger Unkenntnis anderer über die eigenen Ziele zutrifft.[2] Dies sei als eine hinreichende Bedingung für die Anpassung an die Umgebung bezeichnet.

Diese hinreichende Bedingung wird aber im weiteren Verlauf nicht betrachtet. Sie wird vielmehr durch die Betrachtung der Effizienz eines strategischen IT-Security-Managements ersetzt, das die organisatorisch-technische Absicherung der optimalen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume gestalten, d. h. die Absicherung der korrekten Ausführung/Umsetzung entsprechender IT-Projekte gewährleisen soll.

Kenntnisse über das wirtschaftliche und rechtliche Umfeld des Unternehmens spielen auch bei der externen Revision durch den Wirtschaftsprüfer im Rahmen der handelsrechtlichen Abschlussprüfung eine wichtige Rolle. Nach IDW PS 230 umfasst dieses Umfeld „die besonderen Merkmale und Verhältnisse – d. h. die bedeutsamen wirtschaftlichen und rechtlichen Rahmenbedingungen – der Branche, in der das zu prüfende Unternehmen tätig ist". Kenntnisse über dieses Umfeld sind für den Abschlussprüfer wichtige Grundlage u. a. für „die Risikobeurteilung und die Identifikation möglicher Problemfelder" sowie „die sachgerechte Prüfungsplanung und -durchführung", beispielsweise bezüglich des Risikofrüherkennungssystems. Diese Kenntnisse sollen mit dazu beitragen, dem Abschlussprüfer u. a. eine Identifikation der „den Erfolg der (Unternehmens-)Strategie möglicherweise gefährdenden Geschäftsrisiken und der Reaktionen des Unternehmens auf diese Risiken" zu ermöglichen.[3]

Einen wichtigen Teil der „Umgebung" des Unternehmens stellen die externen Compliance-Anforderungen dar. Der andere Teil dieser „Umgebung" ist das IT-Umfeld. Dieses ist durch die Infrastruktur, die Applikationen und Business-Prozesse beschrieben.

Der IDW PS 330 („Abschlussprüfung bei Einsatz von Informationstechnologie") definiert dieses IT-Umfeld im weiteren Sinne im Zusammenhang mit der Erhebung rechnungslegungsrelevanter IT-Systemelemente als die Bereiche IT-Umfeld im engeren Sinne, IT-Organisation,

[1] vgl. Schneier, Bruce (2000), S.265-267
[2] vgl. Berninghaus, Siegfied. (2002) , S.270
[3] IDW (2000b):, PS 230

IT-Infrastruktur, IT-Applikationen und IT-Geschäftsprozesse. Auch dem Bereich IT-Umfeld im engeren Sinne soll wie den Bereichen IT-Organisation, IT-Infrastruktur, IT-Applikationen und IT-Geschäftsprozesse ein IT-Überwachungssystem zugeordnet werden.

Dabei ist die interne IT-Organisation für die Zweckmäßigkeit eingekaufter IT-Leistungen verantwortlich, d. h., dass die IT-Services auf die Anforderungen des Business zugeschnitten sind. Dazu sind z. B. ein entsprechender Servicekatalog und eine detaillierte Spezifikation der einzukaufenden Teilleistungen zu entwickeln.[1]

Für das IT-Umfeld im engeren Sinne werden folgende rechnungslegungsrelevante IT-Systemelemente angegeben:[2]

- Grundeinstellungen zum Einsatz von IT-Systemen, beispielsweise dokumentiert im IT-Sicherheitskonzept (Unternehmensleitlinien, IT-Sicherheitshandbücher u. a.)
- verbindlich niedergelegte IT-Strategie, abgeleitet aus der Unternehmensstrategie
- High Level Controls

Eine „angemessene Grundeinstellung zum Einsatz von IT und ein Problembewusstsein für mögliche Risiken aus dem IT-Einsatz“ werden als Voraussetzung für ein „geeignetes“ IT-Umfeld benannt. Als Teil eines geeigneten IT-Umfelds wird das „Bewusstsein für Sicherheit in der Unternehmensorganisation“ angegeben. Dieses ist auch eine „wesentliche Bedingung für eine angemessene Umsetzung des IT-Sicherheitskonzepts“.[3] Soweit kein hinreichendes Sicherheitsbewusstsein vorhanden sei, bestehe die Gefahr, dass die zur Vermeidung der Geschäftsprozessrisiken umgesetzten Maßnahmen unwirksam blieben.[4]

High Level Controls werden als Ausprägung Prozess unabhängiger Kontrollen definiert, welche „im besonderen Auftrag der gesetzlichen Vertreter oder durch diese selbst vorgenommen werden“.[5] Hier können auch Compliance-Anforderungen eine Rolle spielen.

Die Control Objectives for Information and Related Technology (CObIT) definieren als ”High Level IT Revision” die Arbeitsabläufe/Prozesse, die erforderlich sind, die IT auf die Erreichung der Unternehmensziele abzustimmen. Die CObIT beschäftigen sich aber nicht mit Detailprüfungshandlungen zu den IT-Ressourcen. Diese Lücke kann durch das IT-Grundschutzhandbuch des BSI geschlossen werden.

Der IDW RS FAIT 2 („Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Electronic Commerce“) macht eine Einteilung in rechtliches sowie technisches und organisatorisches Umfeld. Das rechtliche Umfeld wird durch die geltenden rechtlichen Anforderungen speziell

[1] vgl. Grawe, Tonio (2005b)
[2] vgl. IDW (2002b), PS 330,49-50
[3] IDW (2002a), RS FAIT 1,77
[4] vgl. IDW (2003): RS FAIT 2,54
[5] IDW (2001): PS 260, 6

beim E-Commerce zur Gewährleistung der Rechtssicherheit und der informationellen Selbstbestimmung beschrieben. Das technische und organisatorische Umfeld betrifft die technischen und administrativen Rahmenbedingungen sowie die technisch-organisatorische Abwicklung der Geschäftsprozesse.[1] Entsprechend soll hier eine Anpassung an das rechtliche, das organisatorische und das technische Umfeld unterschieden werden.

Die Anpassung an das rechtliche Umfeld liefert mit der Compliance einen Teil der notwendigen Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security. Der andere ergibt sich aus Überlegungen zur Anpassung an das organisatorische und das technische Umfeld. Beide werden von der Revision der IT-Security angestrebt. Überlegungen zur Anpassung an das organisatorische und das technische Umfeld müssen darüber hinaus die hinreichende Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security ableiten.

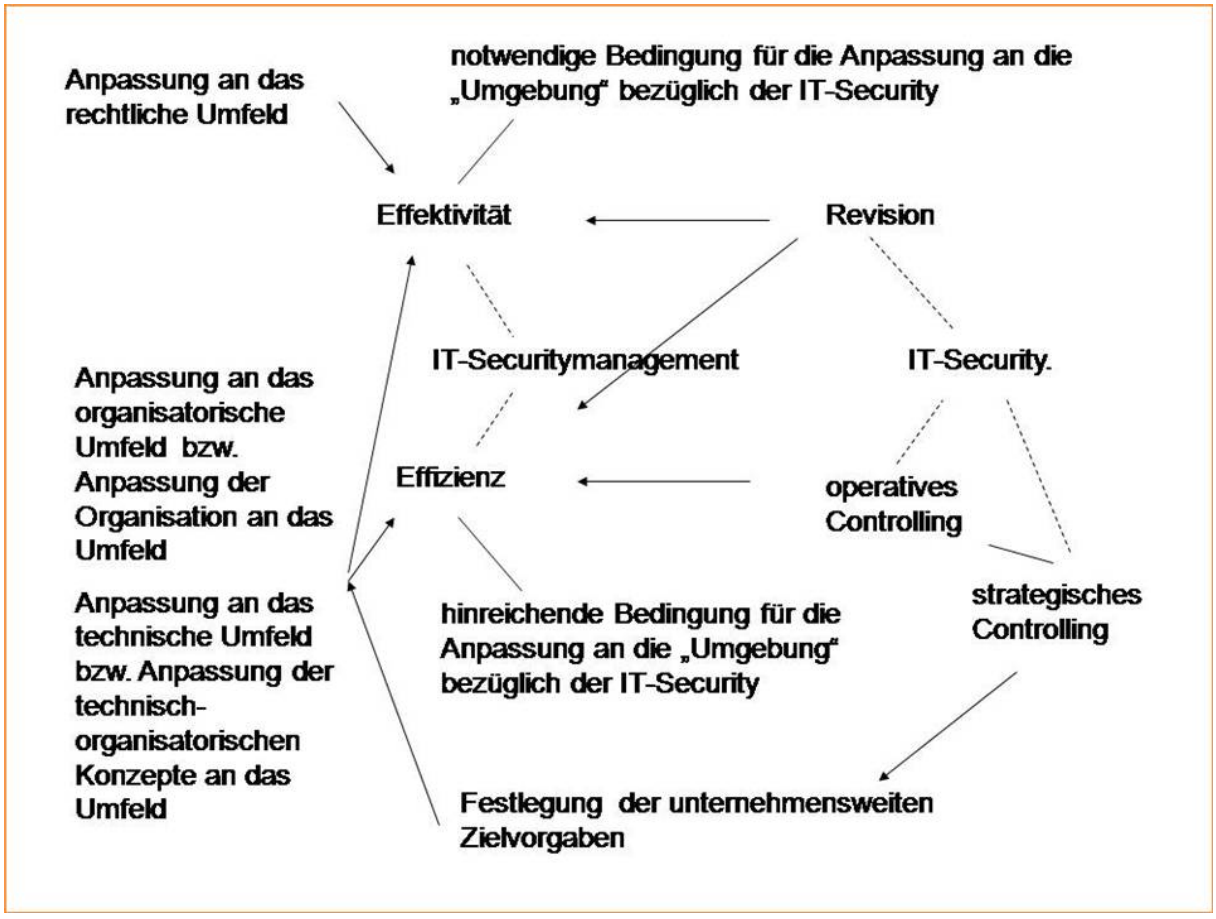


Abb. 14 Einordnung IT-Security-Management und Revision sowie Controlling der IT-Security

Der Prozess zur Formulierung und Umsetzung der strategisch-operativen Zielsetzungen des Unternehmens ist ständig an das Unternehmensumfeld anzupassen. Die Bedeutung der IT-Security für Formulierung und Umsetzung der strategisch-operativen Zielsetzungen des

[1] vgl. IDW (2003): RS FAIT 2,12-17

Unternehmens liegt u. a. darin begründet, dass der entsprechende Anpassungsprozess auch einen Anpassungsprozess an die Umgebung bezüglich der IT-Security umfasst.

5.1.1.3.1 Anpassung an das rechtliche Umfeld

Die rechtlichen Rahmenbedingungen und die Umwelt an sich sind neben externen Erfolgsfaktoren, die den Markt betreffen, zu betrachten. Hierunter werden Faktoren wie die innere Sicherheit und das Rechtssystem verstanden.[1]

Die Konformität mit Compliance-Anforderungen (z. B. gemäß KonTraG oder SOX) stellt einen wichtigen Teil der notwendigen Bedingung für die Anpassung an die „Umgebung" bezüglich der IT-Security dar.

Die Compliance-Anforderungen für die IT-Security verlangen, dass sich das Unternehmen an diese „Rechtskomponente" anpasst (analog der Auffassung im Diskurs um evolutionäre Ansätze in der Rechtswissenschaft, dass der „Rechtsorganismus" verlange, dass die Gesellschaft sich an ihn anpasse[2]). Dazu werden z. B. die Systeme und Geschäftsprozesse der Organisation (auch an zu erwartende neue) Regelungen angepasst.

Zur Anpassung an das rechtliche Umfeld etwa im Bereich Datenschutz werden auf technischer Ebene Datenschutz fördernde Techniken (engl.: "Privacy Enhancing Technologies (PET)") entwickelt. Dies sind Techniken, die Datenschutz so weit wie möglich fördern und durchsetzen, zumindest aber unterstützen sollen. Maßnahmen dazu sind etwa Protokolle für Anonymität, aber auch tief in den Systemen eingebettete Datenschutz-Funktionen. Diese müssen die Kriterien und Grundsätze Datenvermeidung und Datensparsamkeit (Reduktion personenbezogener Daten in einem IT-System), Systemdatenschutz (bereits technisch im System implementierte und organisatorisch verankerte Datenschutzmaßnahmen), Selbstdatenschutz (Maximum an Steuerungsmöglichkeiten durch den Nutzer) sowie Transparenz und andere vertrauensbildende Maßnahmen abdecken. Um etwa Personendaten zu schützen, z. B. persönliche Zahlungsdaten zu verschlüsseln, kommen kryptografische Hilfsmittel und digitale Signaturen in Betracht. Weitere Sicherungsmaßnahmen wären etwa Smart Cards oder biometrische Verfahren. [3]

Im Bereich Datenschutz muss das Unternehmen sich in dieses rechtliche Umfeld vollständig integrieren, da dieses Umfeld durch internationale Harmonisierung geprägt ist und alle Informationssysteme des Unternehmens betrifft. Die entsprechenden datenschutzrechtlichen

[1] vgl. Reichling, Peter (2003), S.210
[2] vgl. Lenzen, Manuela (2003), S.121
[3] vgl. UIMCert PS 102, TZ 28-30

Anforderungen führen zu unmittelbaren Umsetzungskonsequenzen auf organisatorischer und technischer Ebene.

Zur Anpassung/Vorbereitung auf die Konsequenzen für die Unternehmen im Zusammenhang mit Basel II sollten bereits im Vorfeld einer Bonitätsprüfung Maßnahmen ergriffen werden, die zu einem positiven Ratingurteil beitragen können. Zu diesen Maßnahmen gehört neben einer ausführlichen Dokumentation der wirtschaftlichen Lage die „Präsentation eines überzeugenden Gesamtkonzepts für die Geschäftsstrategie“.[1]

Anpassung an das organisatorische und technische Umfeld ist in dem Sinne gemeint, dass Unternehmen ihre IT-Ressourcen, Systeme und Geschäftsprozesse ständig anpassen und neu konfigurieren müssen, um einen optimalen, am besten auf das Umfeld angepassten Einsatz der IT-Technologie zu erreichen.

Diese Anpassung an das organisatorische und das technische Umfeld ist von einem geeignet zu gestaltenden strategisch-operativen Controlling der IT-Security zu gewährleisten.

5.1.1.3.2 [i]Anpassung an das organisatorische Umfeld

Bei der Anpassung an das organisatorische Umfeld ist die organisatorische Abwicklung der Geschäftsprozesse (also die Ablauforganisation) mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume zu gestalten. Dies ist durch die Umgestaltung der IT-Landschaft möglich.

Ziel ist es, durch eine neue Sichtweise mehr Effektivität und Transparenz bei gleichzeitiger Kostenreduzierung zu gewinnen, um so „die Zukunft aktiv mitzugestalten“.[2] Ohne Verständnis für flexible, sich schnell ändernde Geschäftsprozesse und deren Anpassung wird die IT immer nur reagieren, statt zu agieren. Ohne eine gründliche Analyse des Prozesses und seiner Mängel ist es schwierig, das mögliche Ausmaß der Verbesserungen zu ermitteln.[3]

Der aus den Überlegungen zur Anpassung an das organisatorische Umfeld bzw. Anpassung der Organisation an das Umfeld abgeleitete Teil der notwendigen Bedingung sowie die hinreichende Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security beziehen sich auf Aufbauorganisation und Ablauforganisation:

[1] vgl. Reichling, Peter (2003), S.86
[2] vgl. Wagner, Siegfried (2005), S.39
[3] vgl. JNet Quality Consulting (2007):,S.36

Nach DIN EN ISO 8402, 1995-08 Ziffer 1.2 ist unter einem Prozess ein Satz von in Wechselbeziehungen stehenden Mitteln und Tätigkeiten« zu verstehen, die Eingaben in Ergebnisse umgestalten. Die Ablauforganisation bestimmt, wie diese Aufgaben im Unternehmen abgearbeitet werden. Die Umsetzung erfolgt durch die Vorgabe von Regeln, z. B. in Form von Arbeitsanweisungen. Die Anpassung der Organisation an das Umfeld betrifft neben Ablauforganisation auch die Aufbauorganisation. Die durch die Aufgabenerteilung bestimmte Struktur der Unternehmensorganisation ist z. B. durch die Verteilung von Weisungsrechten zu konkretisieren. Die Effizienz der Aufgabenerfüllung wird nicht nur durch die Ablauforganisation bestimmt, sie setzt auf die vorhandene Aufbauorganisation auf. Diese muss an den Unternehmenszweck angepasst sein, um die Erfüllung von Aufgaben nicht zu erschweren (z. B. in Form zu langer Durchlaufzeiten, langer Entscheidungswege und von Abstimmungsproblemen, Doppelarbeit und Bearbeitungsfehlern). Darüber hinaus ist es wichtig, dass die Organisation auf Umwelteinflüsse flexibel reagieren kann. So wird eine unflexible Ablauforganisation bei einem Wandel der Rahmenbedingungen schnell zum Hemmschuh für den Unternehmenserfolg.[1]

Einen Beitrag für die notwendige Bedingung für die Anpassung an die „Umgebung“ liefern die mit Aufbauorganisation und Ablauforganisation in Verbindung stehenden internen Ordnungsmäßigkeitsvorgaben.

Die hinreichende Bedingung für die Anpassung an die „Umgebung“ kann an die, ebenfalls mit Aufbauorganisation und Ablauforganisation in Verbindung stehende Optimierung der Aufgabenerfüllung geknüpft werden, die mit entsprechenden Nutzenpotenzialen der IT in Verbindung steht.

Als evolutionäre Weiterentwicklung etwa der Business orientierten Entwicklung von IT-Lösungen kann die Integration von Geschäftsprozessmodellen mit Servicemodellen ausgebaut werden: Geschäftsarchitektur und IT-Architektur (bestehend aus Servicearchitektur, Anwendungsarchitektur und Infrastrukturarchitektur) werden durch Definition von Beziehungen zwischen den jeweiligen Architekturmodellen gezielt und explizit verbunden. Im Rahmen der sog. integrierten Unternehmensarchitektur erfolgt dann die Festlegung auf Abbildungen von Architektur-Metamodellen (mit ihren Beziehungen), die auf ihre Transformierbarkeit ineinander untersucht werden. Diese integrierte Unternehmensarchitektur soll den „gemeinsamen Rahmen für die IT-Lösungsentwicklung“ schaffen. Der letzte Schritt ist die

[1] vgl. Reichling, Peter (2003), S..204,205

Transformation in (Generierung von) Code (Model To Text Transformation). Das obige Framework wird als Basis angesehen, um den Mehrwert des sog. „Integrated Business Driven Developement“ von Verbesserungen in den Bereichen Geschwindigkeit, Kosten und Qualität für das Unternehmen deutlich herauszuarbeiten. Über diese evolutionäre Weiterentwicklung der IT-Lösungsentwicklung soll schließlich ein verbessertes Business-IT-Alignment und gesteigerte IT-Agilität erreicht werden.[1] Dabei wird unter Business-IT-Alignment die Ausrichtung der IT am Geschäft, der bestmögliche Einsatz der IT-Ressourcen, mit denen die Geschäftsziele des Unternehmens erreicht werden sollen, verstanden.[2] Um die IT-Strategie im Sinne eines effizienten Business-IT-Alignments zukunftsorientiert und konsequent an den strategischen Geschäftszielen auszurichten, bieten sich dabei die beiden Frameworks CObIT und ITIL an, wobei es möglich ist, beide Sichtweisen effektiv miteinander zu integrieren, wodurch sich bei der Ausrichtung der IT-Prozesse auch die Anforderungen an die Ordnungsmäßigkeit erfüllen lassen.[3]

Strategische Handlungsspielräume im Sinne der flexiblen Anpassung an Kundenwünsche erfordert die effiziente Verbindung der Geschäftsprozesse mit Nutzer bezogenen Kommunikationsprozessen. In diesem Sinne flexible Geschäftsprozesse sollen darüber hinaus die schnelle Kommunikation zwischen dem Unternehmen und seinen Lieferanten und die effiziente Zusammenarbeit zwischen Mitarbeitern verschiedener Abteilungen ermöglichen. Solche flexiblen Geschäftsprozesse können durch sog. Portale abgebildet werden, die dort ansetzen, wo „durch die Optimierung von Prozessen ein großer Nutzen für das Unternehmen entsteht“.[4]

Die Überwachung sowie langfristige und zukunftsorientierte Steuerung einer Vielzahl von Prozessen durch das Management ist nur mithilfe leistungsfähiger IT-Anwendungen möglich, die diese Prozesse abbilden. Durch seine übergeordnete Struktur ermöglicht ein Portal die Aufbereitung (Erfassung, Analyse, Optimierung, praxisgerechte Implementierung)/die effektive Abbildung von Prozessen. In konventionellen Applikationen erstellen Entwickler verschiedene Funktionen und fassen diese über eine gemeinsame Bedieneroberfläche zusammen. Portale verfolgen einen ähnlichen Ansatz, aber auf die Gesamt-IT bezogen. Portale (zur Abbildung z. B. von Identity-Management, Single Sign-on Verfahren etc.) fassen alle Daten und Anwendungen zu einer logischen Einheit zusammen und ermöglichen den benutzerspezifischen Zugriff auf alle Funktionen, Programme und Daten, die der Anwender für

[1] vgl. Klement, Peter (2006)
[2] vgl. Schwarze, Lars (2006), S.33
[3] vgl. Engl, Roland (2006)
[4] Essigke, Andreas (2005)

seine Arbeit benötigt.[1] Das Portal wird wie eine zusätzliche logische Schicht über die bereits vorhandenen Applikationen gelegt. Prozess orientierte Fachportale sollen bei einer großen Anzahl von Anwendungen, die alle einen Teil der Aufgaben abdecken, Transparenz und die Kommunikation zwischen den Prozessbeteiligten fördern. Dazu sollen sie abhängig von der jeweiligen Rolle im Unternehmen allen Beteiligten einen zentralen Zugang zum Zugriff auf alle benötigten Daten und Informationen gewähren. Portalorientierte Anwendungen sollen dabei die von den Benutzern Applikations- und Daten übergreifend benötigten Informationen unter bestmöglicher Nutzung vorhandener Backend-Systeme auf den Prozess bezogen zur Verfügung stellen.[2] [3]

Die Umsetzung der „Portalidee“ ist eine anspruchsvolle Integrationsaufgabe auf technischer Ebene: Aus allen relevanten Anwendungen im vorhandenen Prozess, die portalfähig und erhaltenswert sind, müssen neue Dienste mit transparenten Schnittstellen geschaffen werden. Angefangen von der Verwaltung von Rechten und Rollen über Applikationen hinweg (welche dafür sorgt, dass Benutzer flexibel und effizient verwaltet werden können), bis hin zur Steuerung wichtiger Prozesskennzahlen, muss die Portallösung zentralen Zugang zu allen benötigten Daten und Anwendungen bereitstellen.

Dabei soll das Fachportal modular und flexibel aufgebaut sein, um an neue Anforderungen angepasst werden zu können. Durch die Vorgaben der IT-Governance müssen die Voraussetzungen für eine effiziente Weiterentwicklung und Pflege geschaffen werden.

Eine große Herausforderung ist die umfassende Sicherung eines solchen Unternehmensportals (Härtung aller Portalkomponenten). Unter den Stichworten Verfügbarkeit, Ausfallsicherheit, Applikations- und Netzwerksicherheit ist ein detaillierter Einblick in die Infrastruktur eines Portals notwendig, und verschiedene Methoden und Verfahren (Monitoring & Logging, Benutzermanagement, Authentifizierung, Single Sign-on, Rollen und Berechtigungen sowie Knowledge Management) zu betrachten.[4]

Das Portal wird so zur Grundlage einer serviceorientierten Nutzung der vorhandenen IT-Infrastruktur. Diese Portale entsprechen auf technischer IT-Security-Ebene den Security Gateway Plattformen (siehe unten).

Mit diesen Portalen wird eine Konsolidierung von dezentralen Anwendungen mit überlappenden Anforderungen auf eine zentrale Plattform ermöglicht, womit die IT des Unter-

[1] vgl. Bieberstein, Norbert (2006)
[2] vgl. Grimm, Sebastian (2005), S.17
[3] vgl. Drecker, Norbert (2006):
[4] vgl. Schmitz, Ulrich (2007)

nehmens effizienter gestaltet wird, was wiederum eine zentrale Nutzenkomponente der IT darstellt. Auf operativer Ebene hat die IT-Sicherheit in dieser „Portalumgebung“ die effiziente Verbindung der Geschäftsprozesse mit Nutzer bezogenen Kommunikationsprozessen und die schnelle Kommunikation zwischen dem Unternehmen und seinen Partnern/Lieferanten/Kunden und die effiziente Zusammenarbeit zwischen Mitarbeitern verschiedener Abteilungen zu unterstützen/zu ermöglichen.[1]

Um bestehende IT-Landschaften flexibler zu gestalten, die IT-Infrastruktur schnell und nahtlos an sich ständig verändernde Ansprüche und neue Geschäftsabläufe anzupassen, kann eine adaptive Infrastruktur angestrebt werden, die Systeme, Applikationen und Services zu einem homogenen Ganzen integriert. Alle Kapazitäten werden zusammengefasst und bedarfsgerecht zugeteilt. Im Fokus steht die Bereitstellung einer höchstmöglichen Verfügbarkeit. Eine solche weitestgehend automatisierte und virtualisierte IT-Plattform schafft den Rahmen für die Umsetzung neuer, zukunftsträchtiger Konzepte. [2]

5.1.1.3.3 Anpassung an das technische Umfeld

Moderne IT-Umgebungen und das IT-Management befinden sich in einer ständigen Anpassungsphase an den Einsatz immer neuer Technologien, Methoden und Anwendungen sowie wachsender Anforderungen an die IT-Services. Die Dynamik des technischen Umfeldes ist durch den schnellen technologischen Wandel und ständig auftauchende neue IT-Bedrohungen gekennzeichnet. IT-Infrastrukturen müssen somit immer effizienter weiterentwickelt und gesteuert werden. Änderungen in der Technologie und ihrer Einsatzmöglichkeiten führen auch zu neuen Anforderungen an die Sicherheit und somit zur Notwendigkeit eines Sicherheitsmanagements. Die IT-Prozesse müssen dabei an den Anforderungen der Geschäftsprozesse ausgerichtet werden. Vorgaben und Anregungen, mit denen das IT-Management diese Anpassungen effizient realisieren kann, liefert z. B. ITIL als Modell zur Abdeckung von IT-Veränderungsprozessen. [3] Prozess-Frameworks wie ITIL müssen permanent weiter entwickelt und ausgebaut werden. In ITIL werden ständig neue Service-Gebiete beschrieben und vorhandene angepasst.

Das IT-Management muss sich an den Einsatz neuer Technologien, Methoden und Anwendungen (z. B. für das Roaming zwischen verschiedenen Netzen) sowie wachsender Anforderungen an die IT-Services auch bezüglich Sicherheitsaspekten anpassen. Betrachtet man

[1] vgl. Drecker, Norbert (2006):
[2] vgl. Rumsauer, Klaus (2007), S.48
[3] vgl. Elsässer, Wolfgang (2005), S.6,7

IT-Security-Management als IT-Management der mit den Anforderungen an die IT-Security in Verbindung stehenden IT-Ressourcen, Systeme und Geschäftsprozesse, so folgt auch theoretisch ableitbar, dass sich auch das IT-Security-Management an den Einsatz neuer Technologien, Methoden und Anwendungen anpassen muss, (z. B. an die Etablierung von Webservices in verteilten IT-Strukturen).

Einen Beitrag für die notwendige Bedingung für die Anpassung an die „Umgebung“ liefern die mit dem Einsatz von Technologien, Methoden und Anwendungen zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse in Verbindung stehenden internen Ordnungsmäßigkeitsvorgaben z. B. in Form der zu verwendenden Standards.

Zur Anpassung an das technische Umfeld im Bereich IT-Sicherheit gehört etwa die ständige Verbesserung und Anpassung von Schutzvorrichtungen und -mechanismen an neue Angriffs-szenarien und -möglichkeiten. Mit neuen Anforderungen an Businessprozesse kommen neue Anforderungen auf (z. B. Vermittlung zwischen verschiedenen Technologiewelten (Inter-operabilität) mithilfe XML-basierter Web-Services mit den Standards SOAP (Simple Object Access Protokoll), WSDL (Web Services Description Language) und SAML). Die Security Assertion Markup Language (SAML) ist eine XML-basierte Auszeichnungssprache für Sicherheitsbestätigungen. Sie stellt Funktionen bereit, um sicherheitsbezogene Informationen zu beschreiben und zu übertragen.

Die Notwendigkeit für die Entwicklung von Standards wie SAML ergibt sich aus der Etablierung von Webservices in verteilten IT-Strukturen. Im Gegensatz zu herkömmlichen Anwendungen, die Menschen als Endnutzer voraussetzen, richten sich Anwendungen im „Service-Net“ primär an andere Anwendungen bzw. Dienste. Das „Service-Net“ ist also nichts anderes als ein Netzwerk unterschiedlichster Anwendungen, die als Dienst anderen Anwendungen zur Verfügung stehen. Durch den Gedanken der losen Kopplung und des fehlenden menschlichen Endanwenders scheidet die übliche Authentifizierung z. B. mittels Login-Masken aus. An dieser Stelle soll SAML die sichere Authentifizierung auch zwischen Diensten möglich machen.

Die mit neu entstandenen Funknetzen (z. B. UMTS) verbundenen technischen Möglichkeiten und der IP-Communication-Bereich schaffen die Voraussetzungen für neue mobile Kommunikationslösungen. Es ist mit Lösungen zu rechnen, die den besten Kommunikations-weg (schnellste oder billigste Verbindung) realisieren. Dazu müssen die Endgeräte die unter-schiedlichen Netze natürlich unterstützen und es muss eine dynamische Netzwahl (ohne dass

das Gespräch unterbrochen wird) möglich sein. Das Roaming zwischen verschiedenen Netzen (wie GMX, UMTS, WLAN) erfordert dabei geeignete Technologien, die die relevanten Sicherheitsaspekte (Zugriffssicherheit und Abhörschutz) gewährleisten.[1]

Systeme, Netzwerkkomponenten und Applikationen werden zumeist in Grundkonfigurationen ausgeliefert. Bezüglich der IT-Sicherheit sind die neuen Systeme so anzupassen, dass sie dem definierten Sicherheitsniveau des Unternehmens entsprechen. Voraussetzung für dieses Konfigurationsmanagement ist eine konsistente, unternehmensweite Sicherheitsarchitektur. Ausgehend von der Geschäftspolitik (die definiert, welche Maßnahmen einzuleiten sind, um die Geschäftsziele zu erreichen) und den Geschäftsregeln und Weisungen, die Sicherheitsmechanismen mit Geschäftsrisiken in Verbindung bringen, ist ein technisches Security-Framework zu entwickeln, das das gesamte technische Sicherheitsdesign der Infrastruktur des Unternehmens vorgibt. Aufgabe des Risikomanagements ist es (aufsetzend auf einer Klassifikation der Sachwerte, insbesondere der IT-Systeme, etabliert in einer aktuellen Datenbank der Owner der vorhandenen Systeme, Netzwerke, Applikationen und Informationen), festzustellen, wie kritisch und sensitiv gewisse Sachwerte und Prozesse sind und zu evaluieren, welche Sicherheitsmaßnahmen zu deren Schutz notwendig sind. Neben der Funktion als Berater in Sicherheitsfragen hat die Revision die Risikobeurteilung und die Umsetzung der Maßnahmen periodisch zu prüfen.[2]

Die hinreichende Bedingung für die Anpassung an die „Umgebung“ kann an den optimalen Einsatz und die optimale Implementierung/Umsetzung der Technologien, Methoden und Anwendungen zur Ausrichtung der IT-Prozesse an die Anforderungen der Geschäftsprozesse geknüpft werden, welcher mit entsprechenden Nutzenpotenzialen der IT in Verbindung stehen.

Ein zentraler Aspekt bei der technischen Anpassung ist die Integration neuer IT-Akquisitionen in die bestehende IT-Infrastruktur bzw. die entsprechende Konfiguration der in der IT-Infrastruktur zusammenwirkenden IT-Komponenten. Dabei ist es im ersten Schritt notwendig, die Anforderungen an elektronische Geschäftsprozesse wirkungsvoll umzusetzen, ohne die bestehenden funktionierenden IT-Infrastrukturen verändern zu müssen. Die Integration neuer Technologien und Lösungen in bestehende IT-Infrastrukturen unter Produktivitäts- und Kostengesichtspunkten erfordert ein schlüssiges Gesamtkonzept, um den

[1] vgl. Essigke, Andreas (2005)
[2] vgl. Horster, Patrick (2002b), S.106-109

Veränderungsaufwand bei der Integration in bestehende Netzstrukturen so gering wie möglich zu halten. Als Grundlage dieser Aufgabe wird der Einsatz einer zentralen Security Gateway Plattform vorgeschlagen, die sich in bestehende IT-Netzlandschaften integriert und geforderte Dienste und Services bereitstellt, sodass minimaler Adaptionsaufwand seitens des Anwenders gefordert wird. Die notwendigen Security-Features werden entsprechend den spezifischen Anforderungen bedarfsgerecht bereitgestellt. Auf Grundlage einer Security Gateway Plattform in verschiedenen Ausprägungen, als Authentication Gateway (für das ID-Management), Signature Server und Secure E-Mail Gateway wird ein zentraler Ansatz zur Authentisierung von Abläufen und Services unter Berücksichtigung spezifischer Arbeits- und Organisationsabläufe und gewachsener Infrastrukturen im Unternehmen umgesetzt.[1] Die Security Gateway Plattform wird so zur Grundlage einer serviceorientierten Nutzung der IT-Infrastruktur, welche Security-Featuress entsprechend den spezifischen Anforderungen bedarfsgerecht bereitstellt.

Ein wesentliches Prinzip für höhere Sicherheit ist die Absicherung über mehrere Sicherheitsstufen. Zum Schutz von Web-Anwendungen beispielsweise werden WebShields in die IT-Infrastruktur integriert. Dabei ergibt sich ein höherer Aufwand als z. B. bei Netzwerk-Firewalls, da die Lastanforderungen (Performance-Einbußen durch permanente Prüfung des Datenverkehrs) und die Abhängigkeiten zu anderen Systemen, wie Load-Balancern oder Proxys deutlich höher sind.[2]

Bei der Integration im Rahmen der Anpassung an das technische Umfeld müssen Anwendungen oft unter der Nebenbedingung integriert werden, Geschäftspartnern oder auch Kunden einen direkten Zugang zu Informationen und eine einheitliche Sicht auf die sie betreffenden Daten in einer meist heterogenen Systemumgebung zu gewähren. Um diese Bedingung zu erfüllen, hat sich als Architekturansatz eine Sammlung von Prinzipien, die serviceorientierte Architektur (SOA) (auf Grundlage untereinander kommunizierender Webservices) durchgesetzt, die über den Einsatz von Middelware hinausgeht. Letztere gibt es in breiter Auswahl, die unterschiedliche Protokolle, Datenformate und weitergehende Funktionalitäten etwa im Bereich Sicherheit oder Management verwenden. Bei der SOA werden die zu integrierenden Anwendungen als Services aufgesetzt, die dann auch andere Anwendungen nutzen können (sog. Widerverwendbarkeit). Dieses Design bietet mehr Flexibilität als etwa eine Reihe Punkt-zu-Punkt Verbindungen zwischen verschiedenen Anwendungen. Letztlich sollen dadurch alle Einschränkungen und Grenzen zwischen verschiedenen Programmiersprachen, Betriebssystemen und Middelware-Produkten überwunden

[1] vgl. Horster, Patrick (2002b), S.110-121
[2] vgl. BSI & Secure Net GmbH (2007), S.25

werden.[1] Als führendes Architekturparadigma orientiert sich SOA dabei an Standards, die Kommunikation, Design und Administration von Integrationslösungen vereinfachen. Gremien wie die Standardisierungsorganisation OASiS (Organisation for the Advancement of Structured Information Standards) oder das W3C (World Wide Web Consortium) entwickeln dazu etablierte Standards, „um eine SOA mit konkreter Technologie zu untermauern und Spielräume so weit wie möglich auszuräumen“ Aus Gründen der Ausfallsicherheit soll das in diesem Zusammenhang entstandene Integrationsprodukt ESB (Enterprise Service Bus) immer weniger zentrale Komponenten (etwa das für die Service-Beschreibungen notwendige Metadaten-Repository) verwalten, sondern über Komponentensysteme auf die Endpunkte der Verbindungen verteilen. Dies garantiert den Fortlauf der Integration zum Teil auch dann, wenn zentrale Komponenten ein aktuelles Verfügbarkeitsproblem haben.[2]

Mit zunehmender Globalisierung und Dynamisierung steigt auch der Bedarf nach neuen Nutzungsdimensionen der IT und entsprechenden Geschäftsmodellen/Geschäftsmöglichkeiten. Ein Geschäftsmodell, welches aus der Anpassung an diese Entwicklung entsteht, ist das Geschäftsmodell Service-Integrator. Dabei muss die IT-Abteilung für die internen Kunden (die Fachabteilungen) verschiedene Teilleistungen (ob extern eingekauft oder von internen Organisationseinheiten) aufeinander abstimmen, ihr Zusammenspiel sicherstellen. Die Qualitätssicherung von IT-Services kann dabei nicht als zeitlich begrenzter Prozess aufgefasst werden, sondern muss erfolgen, während die Dienstleistung erbracht wird. Dazu sind bei der Service-Konfiguration detaillierte Kenntnisse über die Funktionalität und das Zusammenspiel der Service-Komponenten nötig. Entsprechend dem Prinzip der Widerverwendbarkeit bei der Integration von Anwendungen in einer serviceorientierten Architektur kann mit aufeinander abgestimmten, integrierbaren Service-Komponenten, bei der Entwicklung neuer Service-Komponenten auf bereits bestehenden Komponenten aufgesetzt werden, die nur im Detail angepasst werden müssen.[3] Dies gilt auch für Entwicklung, Bereitstellung und Qualitätssicherung von Security-Features im Rahmen einer Security Gateway Plattform. Eine Service-Architektur ist „Enabler“ für das Geschäftsmodell IT-Service-Integrator, die IT-Security in vielerlei Hinsicht Voraussetzung für die Entwicklung, Bereitstellung und Qualitätssicherung aufeinander abgestimmter, bedarfsgerechter IT-Services. Zum Beispiel müssen transparente Schnittstellen geschaffen, angefangen von der Verwaltung von Rechten und Rollen über Applikationen hinweg muss, wie bei der Portal-

[1] vgl. Baker, Sean (2005)
[2] Schröder, Christian (2007)
[3] vgl. Fähnrich, K.P./Grawe, Tonio (2005)

lösung, zentraler, zuverlässiger Zugang zu allen benötigten Services bereitgestellt werden. Mithin ist die IT-Security „Enabler“ des Geschäftsmodells IT-Service-Integrator.

Ein technisches Security-Framework ausgestaltet als serviceorientierte Architektur kann, wie oben dargestellt, als sog. Security Gateway Plattform umgesetzt werden. Dieses soll sich in bestehende IT-Netzlandschaften integrieren und geforderte Dienste und Services bereitstellen. Dabei müssen die notwendigen Security-Features entsprechend den spezifischen Anforderungen der Geschäftsprozesse bedarfsgerecht bereitgestellt werden. In verschiedenen Ausprägungen, als Authentication Gateway, Signature Server und Secure E-Mail Gateway soll so ein zentraler Ansatz zur Authentisierung von Abläufen und Services unter Berücksichtigung spezifischer Arbeits- und Organisationsabläufe und gewachsener Infrastrukturen im Unternehmen umgesetzt werden.

Wichtiger funktionaler Aspekt einer solchen IT-Security Gateway Plattform ist die Abbildung der Aufgabenstellung eines Risiko orientierten zukunftsbezogenen IT-Security-Managements. Ausgangspunkt dafür ist die Untersuchung der Ungewissheit bezüglich Umfeldentwicklungen mit dem Ziel der Entwicklung von Strategieoptionen in die Richtungen mögliche Randbedingungen des Umfelds und eigene Handlungsmöglichkeiten. Die möglichen Randbedingungen des Umfelds und die eigenen Handlungsmöglichkeiten werden dabei auf den Planungsebenen für eine geschäftsübergreifende Unternehmensstrategie untersucht. Eigene Handlungsmöglichkeiten und Handlungsbefähigung trotz Unsicherheit werden gleichgesetzt. Bezüglich nicht-antizipierbarer Risiken sind dann die Anforderungskriterien an die IT-Sicherheit (aus Sicht des IT-Systems die Verlässlichkeit (beurteilt nach den Kriterien Verfügbarkeit, Integrität und Vertraulichkeit) und aus Sicht der Betroffenen (Anwender/Benutzer) die Beherrschbarkeit des Systems (beurteilt nach den Kriterien Nachprüfbarkeit und Rechtssicherheit)) in den Kontext der Handlungsbefähigung trotz Unsicherheit zu projizieren. Letztere Aufgabenstellung kann als funktionaler Aspekt der Aufgaben eines IT-Security-Controllingsystems (welche alle IT-Security bezogenen Aktivitäten zur Sicherung der Koordinations-, Reaktions- und Adaptionsfähigkeit der Führung umfassen) konkretisiert werden.

Das IT-Security-Framework, welches die Aufgabenstellung eines Risiko orientierten zukunftsbezogenen IT-Security-Managements abbildet, hat also, unter Berücksichtigung möglicher Randbedingungen des Umfelds, IT-Security bezogene Aktivitäten zur Sicherung der Koordinations-, Reaktions- und Adaptionsfähigkeit der Führung auf den Planungsebenen für eine geschäftsübergreifende Unternehmensstrategie festzulegen. Umgesetzt wird ein solches Security-Framework auf technisch-organisatorischer Ebene mittels entsprechender Maßnahmen. Zum Beispiel als IPT-Security-Framework, um die Sicherheit der traditionellen

Telekommunikation auch bei der IP-Telefonie zu erreichen. Die Kernelemente dieses Security-Frameworks betreffen:[1]

- Security für Server (mit Viren-Scannern und Intrusion Detection/Prevention Systemen, speziell optimierte und „gehärtete“ Server und Betriebssysteme für die Telefonie-Server),
- Security für die Netzwerk-Infrastruktur (logische Teilung der Sprach- und Datennetze in virtuelle LANs mit (für besonders hohe Sicherheitsanforderungen) einer Firewall zwischen den logisch getrennten Netzen und mittels Verschlüsselungstechnologien (IPsec, MLS) gesicherten End-to-End-Verbindungen),
- Security für die Endgeräte (mit Hardware-Betriebssystemen für „gehärtete“ Endgeräte, Viren-Scanning, eindeutige Ausweispflicht (Authentifizierung) von Endgeräten am Netz, Einsatz einer Personal-Firewall und Verschlüsselung aller Daten).

Im weiteren Verlauf soll das IT-Security-Management zwecks Überwachung/Steuerung in ein auf die Sicherstellung von Potenzialen bzw. Strategien zur Ausnutzung operativer Flexibilität und zur Steigerung von Managementflexibilität abzielendes, als strategisch-operatives Risiko Controlling bezeichnetes Konzept integriert werden. Dieses strategisch-operative Risiko-Controlling soll die Effektivität und Effizienz des IT-Security-Managements überwachen, das IT-Security-Management koordinieren/steuern und auf die Herstellung/Unterstützung der strategisch-operativen Beweglichkeit/Handlungsbefähigung des Unternehmens ausrichten.

5.1.1.4 Strategisch-operatives Risiko-Controlling

Risiko-Controlling hat ein wirkungsvolles Instrumentarium zur Identifikation, Beurteilung und Steuerung unternehmerischer Risikopotenziale zu entwickeln und bereitzustellen, um Prozess-begleitend bei der methodischen Umsetzung des Risikomanagements zu unterstützen.[2] Es richtet den Risikomanagementprozess an der Risikopolitik des Unternehmens aus, koordiniert ihn und bezieht mit Frühwarnsystemen künftige Unternehmensentwicklungen frühzeitig ein.[3] Allgemein formuliert besteht die Zielsetzung des Risiko-Controllings in der Gewährleistung der Reaktions-, Anpassungs- und Koordinationsfähigkeit im Rahmen der jeweiligen unternehmerischen Risikosituation.[4]

[1] vgl. Damovo (2006)
[2] vgl. Diederichs, Marc (2004), S.26
[3] vgl. Ibers, Tobias (2005), S.71
[4] Diederichs, Marc (2004), S.25

Das mit „management control“ bezeichnete Controlling fordert die Bereitstellung von Systemen zur Unterstützung der Strategieformulierung und -umsetzung. CObIT und ITIL sind als Hilfsmittel für das operative IT-Controlling zu sehen und können in großen Teilen auch im operativen Risikomanagement/Sicherheitsmanagement Anwendung finden. Im Folgenden geht es primär um Konzepte zum Management und Controlling von strategischen Risiken, d. h. hauptsächlich um Risiken, die auf der Ungewissheit der zukünftigen Entwicklungen im Umfeld des Unternehmens und daraus resultierender Ungewissheit über die konkreten Zielvorgaben des IT-Security-Prozesses basieren. Die konkreten Zielvorgaben des IT-Security-Prozesses werden ersetzt durch die angestrebte strategisch-operative Beweglichkeit/Handlungsbefähigung im Kontext der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse. Es wird dann versucht, die im Verlauf dieser Arbeit herausgearbeiteten Konzepte zum Management und Controlling von strategischen und operativen Risiken für den Aufbau eines auf die strategisch-operative Beweglichkeit/Handlungsbefähigung abzielenden „management control“ heranzuziehen, welches auch die Einhaltung sicherheitsrelevanter Aspekte zu gewährleisten hat. „auf die strategisch-operative Beweglichkeit/Handlungsbefähigung abzielend“ ist in dem Sinn gemeint, dass in (durch eine permanente Variation der Umweltbedingungen und damit die Notwendigkeit zur permanenten Handlungsfähigkeit gekennzeichneten) unternehmerischen Entscheidungssituationen, die Entscheidungsfreiheit zu unterstützen ist.

Ein solches Risiko-Controlling wird in dieser Arbeit als "strategisch-operatives" Risiko-Controlling bezeichnet; dadurch soll zum Ausdruck gebracht werden, dass die strategische und die operative Sicht eng miteinander verknüpft werden. Bei dem im Weiteren dargestellten strategisch-operativen IT-Security-Management, welches auf dem strategisch-operativen Risiko-Controlling aufsetzt, wird das noch deutlicher: Der operative Teil knüpft an die Phase "Do" des vom strategischen Teil des IT-Security-Managements gesteuerten strategischen IT-Security-Prozesses an, repräsentiert quasi das Operative im Strategischen.

Auf Basis dieses strategisch-operativen Risiko-Controllings kann eine ex-ante Revision der IT-Security in der Einsatzumgebung des IT-Systems konzipiert werden. Anknüpfungspunkt ist die Annahme, dass für die Beurteilung des Einflusses der IT-Security für die Erreichung der Unternehmensziele/strategisch-operativen Zielsetzungen des Unternehmens, die Bedeutung der IT-Security für eine entsprechende Handlungsbefähigung/Flexibilität/strategisch-operative Beweglichkeit (bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und der Geschäftsprozesse/des IT-Security-Prozesses aufeinander) analysiert werden kann.

Die zielorientierte Führung einer Organisation erfordert, dass das Management Ziele festlegt und das Erreichen dieser Ziele gewährleistet. In beiden Fällen müssen Entscheidungen getroffen werden.[1] Formulierung und Umsetzung der Unternehmensstrategie kann mithilfe des Konzepts des strategischen Performance Managements gemanagt werden. Die Implikationen der Ungewissheit der zukünftigen Entwicklungen im Umfeld des Unternehmens bedeuten, dass die Aktivitäten zur zielgerichteten Umsetzung von der permanenten Variation der ungewissen Umweltbedingungen abhängen. Daher sind durch ein geeignetes Risiko-Controlling entsprechende Entscheidungs-/Handlungsoptionen zu unterstützen.

5.1.1.4.1 IT-Governance, strategisches/operatives Performance Management

Die prozessualen und organisatorischen Maßnahmen, die die Führung und Steuerung der IT unterstützen, werden unter IT-Governance subsumiert. Hauptziel der IT-Governance ist die Steuerung des effektiven und effizienten[2], zweckgerichteten Einsatzes der IT, das Verständnis der strategischen Bedeutung von IT, um so bessere Strategien für die zukünftige Erweiterung des Geschäftsbetriebs zu schaffen.[3] IT-Governance soll sicherstellen, dass die IT den optimalen Beitrag zur Wertschöpfung des Unternehmens in Bezug auf die Gewährleistung der Unternehmensstrategie und der Unternehmensziele liefert.[4] Für eine übergreifende und ausgewogene Steuerung der IT sind eine Reihe von Strukturen und Regeln festzulegen.[5] Eine wirksame unternehmensübergreifende IT-Governance-Struktur gilt als Voraussetzung zur Beherrschung der Komplexität in einer IT-Organistion mit hoher Flexibilität in den IT-Prozessen. Neben dem Aspekt der Kontrollmechanismen, wie sie im Rahmen von CObIT definiert sind, umfasst IT-Governance die Aufgabe des Top-Managements zur Steuerung und Führung der IT-Funktionen und –Mitarbeiter.[6] Durch Etablierung entsprechender Führungskreisläufe, Organisationsstrukturen und Prozesse soll erreicht werden, dass die IT-Strategie die übergeordnete Unternehmensstrategie unterstützt.[7]

Führung beinhaltet einen Entscheidungs-/Planungsprozess sowie einen Steuerungs- und Kontrollprozess. Es geht um die Erarbeitung, Vorgabe und Überwachung von Zielen, Maßnahmen und Ressourcen. Verstanden als ein System vermaschter Entscheidungs-, Steuerungs- und Kontrollprozesse ist Führung stets ein mehrstufiger, teils in Form eines Regelkreises ablaufender Prozess, ein Informationsverarbeitungsprozess mit einer Vielzahl von Ab-

[1] vgl. Kütz, Martin (2005), S.1
[2] vgl. Buchta, Dirk Uwe (2004), S.89
[3] vgl. Pausch, Karl (2005)
[4] vgl. Redenius, Jens O. (2005)
[5] vgl. Buchta, Dirk Uwe (2004), S.90
[6] vgl. Schwarze, Lars (2006), S.32
[7] vgl. Zarnekow, Rüdiger (2005), S.71

stimmungsprozessen strategischer und operativer Art.[1] Strategische Führung (strategisches Denken und Handeln) und Global Strategic Management schließen sich in der Entwicklung von der langfristigen Planung über die strategische Planung an. Diese Konzepte sollen der systematischen Behandlung von grundlegenden Aufgaben der Zukunftssicherung von Unternehmen dienen.[2] Strategische Führung beinhaltet einen weit umfassenderen Aufgabenkomplex als nur die strategische Planung. Sie beinhaltet auch Strategieformulierung und Umsetzung.[3]

„Governance" bedeutet im Grunde die verantwortungsvolle Unternehmenssteuerung durch die Geschäftsführung. Diese soll sich auf den Aufbau einer Organisationsstruktur und damit verbundener Prozesse stützen, welche sicherstellen, „dass die Unternehmensziele und Strategien unter Beachtung anzuwendender Vorgaben umgesetzt, gemessen und überwacht werden". Hieraus abgeleitet umfasst die „Information Security Governance" ein für Planungs-, Kontroll- und Überwachungsprozesse in Bezug auf den sicheren und ordnungsgemäßen Betrieb der Informationstechnik verantwortliches Sicherheitsmanagement. Außerdem soll sie sicherstellen, dass die Unternehmensziele und die IT-Strategie aufeinander abgestimmt sind. Diese Ziele werden durch die Etablierung eines Rahmenwerks erreicht.[4]

Konzepte, die über den Aspekt der Leistungserstellung hinaus einen generellen Managementansatz zur Operationalisierung der Unternehmensstrategien und –ziele und deren Überführung in ein permanentes Führungssystem anstreben, werden als Performance Management bezeichnet.[5] Im Folgenden wird ein entsprechendes Konzept zum Management der IT-Security abgeleitet, um daraus ein strategisch-operatives Controlling der IT-Security als ein dem Management der IT-Security übergeordneten Baustein zu entwerfen. Dabei geht es u. a. darum, wie Risiken im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen (aus Sicht des IT-Systems der Kontext Verlässlichkeit (beurteilt nach den Kriterien Verfügbarkeit, Integrität und Vertraulichkeit), und aus Sicht der Betroffenen (Anwender/Benutzer) der Kontext Beherrschbarkeit des Systems (beurteilt nach den Kriterien Nachprüfbarkeit und Rechtssicherheit) in den Kontext der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume und umgekehrt abgebildet werden können.

Um den Strategie- Formulierungs- und Umsetzungsprozess bezüglich der IT-Security zu managen, und ein übergreifendes strategisch-operatives Controlling zu entwickeln, wird das

[1] vgl. Hahn, Dietger (2006), S.30,31
[2] vgl. Hahn, Dietger (2006), S.V,XI
[3] vgl. Hahn, Dietger (2006), S.32,33
[4] vgl. Füser, Karsten (2006)
[5] vgl. Currle, Michael (2002), S.11,12

strategische Performance Management als wichtigstes Konzept der strategischen Unternehmensführung (und auch ein noch zu definierendes operatives Performance Management) auf die Planungs- und Lenkungsaufgabe bezüglich des IT-Security-Prozesses (IT-Security-Management) angewandt. Dazu wird das strategische Performance Management auf Sicherheitsstrategien, verstanden als Führung der Sicherheitssysteme des Unternehmens, übertragen:

Führung vollzieht sich vor allem in Führungsprozessen (wie Zielbildung, Planung, Entscheidung). Darüber hinaus schafft sie Systeme, die der Koordinierung dieser Prozesse dienen. Im Fokus der strategischen Unternehmensführung stehen betriebliche strategische Entscheidungen. Diese zielen auf den Aufbau und die Sicherung von Erfolgspotenzialen.

Unternehmensstrategie wird unterteilt in Formulierung (Strategiefindungsprozess) und Implementierung. Im Rahmen der Formulierung werden strategische Entscheidungen formuliert und getroffen. Dabei sind u. a. auch Risiken und Schwachstellen zu identifizieren. Im Rahmen der Implementierung werden die zuvor festgelegten strategischen Ziele durch- und umgesetzt.[1] Art, Ausmaß und den Umgang mit bei der Strategieumsetzung zulässigen Risiken regelt die Risikostrategie. Im Gegensatz zur Risikopolitik, die weitgehend frei von operativen Zielen ist, erfolgt bei der Risikostrategie die Umsetzung auf die unternehmensspezifischen Gegebenheiten. Darüber hinaus werden durch das strategische Risikomanagement die Rahmenbedingungen für das operative Risikomanagement festgelegt.[2] Im Zusammenspiel zwischen Strategieentwicklung und -implementierung (bei der Strategieumsetzung an sich) sind dabei im Fit zwischen Strategie und Organisation und dem entsprechenden unternehmerischen Weiterentwicklungsprozess elementare Verbesserungschancen gegeben.[3]

Die Strategieimplementierung ist so weit wie möglich von Zufälligkeiten, Unzulänglichkeiten und Bedrohungen frei zu halten.[4] Langwierig ausgearbeitete Konzepte können dabei durch sog. „Launch & Learn“ Ansätze abgelöst werden, bei denen die Strategie in einem dynamischen Prozess während der Implementierung laufend angepasst, erweitert und verfeinert wird.[5]

In der Kontrollphase des Strategiefindungsprozesses wird konzeptionell in Planfortschrittskontrolle anhand von Meilensteinen, Prämissenkontrolle – also laufendes Hinterfragen, ob die

[1] vgl. Eschenbach, Rolf (2003), S.9-10
[2] vgl. Ibers, Tobias (2005), S.50-
[3] vgl. Seidenschwarz, Werner/Huber, Christian (2002), S.123-125
[4] Vgl. Piser, Marc (2004), S.28
[5] Stoi, Roman (2002), S.156

für die strategische Entscheidung relevanten Planungsprämissen noch Gültigkeit besitzen – sowie ungerichtete strategische Überwachung untergliedert.[1]

Die Prämissen der Strategie müssten sämtlich mit der Prämissenkontrolle regelmäßig auf ihre auch zukünftige Gültigkeit untersucht werden, was mit sehr hohem Aufwand verbunden wäre. Daher ist eine Fokussierung auf die wichtigsten Prämissen notwendig.[2] Zur Kompensation der Selektionsrisiken der Planung dienen die strategische Durchführungskontrolle und die strategische Überwachung. Diese haben frühzeitig Informationen zu beschaffen, die eine Evaluation der gewählten Strategie auf Veränderungsbedarf ermöglichen.

Dazu soll die strategische Überwachung Informationen über die Abweichung von strategischen Prämissen bereitstellen. Die Auswirkungen unvorhergesehener Störungen in der zukünftigen Entwicklung können als Abweichungen mit der strategischen Durchführungskontrolle sichtbar gemacht werden.[3] Dabei sind alle Informationen zu sammeln, die auf zukünftige Umsetzungsgefahren hindeuten, und dem Management die Ergreifung geeigneter Maßnahmen zu ermöglichen.[4]

Die strategische Kontrolle (strategische Durchführungskontrolle und strategische Überwachung) beschafft und verarbeitet Informationen, die bei der strategischen Planung nicht berücksichtigt wurden oder nicht bekannt waren. Die strategische Kontrolle überprüft also die Planung auf Vollständigkeit und Konsistenz. Kritische Informationen über die Unternehmensumwelt können zeigen, dass die bisherigen Ergebnisse des strategischen Managementprozesses einer Revision bedürfen. Wichtig sind steuerungsrelevante Informationen, wenn nicht mehr korrekturfähige oder korrekturwürdige Zustände erreicht werden, die eine Fortführung der Strategieimplementierung als nicht mehr sinnvoll erscheinen lassen[5] Durch Selektion strategierelevanter Informationen lassen sich auch die Kostenrechnung, die Buchhaltung und die Finanzrechnung für die strategische Durchführungskontrolle nutzen.[6]

Das strategische Performance Management steuert die Formulierung und Realisierung von Strategien. Dazu dienen strategische Prämissenkontrolle, strategische Durchführungskontrolle und strategische Überwachung. Das Corporate Performance Management dient zur Abstimmung der Unternehmensziele und Geschäftsprozesse aufeinander, kann als operatives Performance Management aufgefasst werden, und bestehend aus operativer Prämissenkontrolle, operativer Überwachung und operativer Durchführungskontrolle modelliert werden.

[1] vgl. Eschenbach, Rolf (2003), S.14
[2] vgl. Piser, Marc (2004), S.44
[3] vgl. Piser, Marc (2004), S.48
[4] vgl. Piser, Marc (2004), S.48
[5] vgl. Piser, Marc (2004), S.49
[6] vgl. Piser, Marc (2004), S.50

Die im Kontext der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume relevanten Risiken der IT-Security werden gemanagt, indem das strategische Performance Management auf die strategische Planungs- und Lenkungsaufgabe bezüglich des IT-Security-Prozesses (IT-Security-Management) übertragen wird. Die im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen relevanten Risiken werden gemanagt, indem das operative Performance Management auf die operative Planungs- und Lenkungsaufgabe bezüglich des IT-Security-Prozesses (abgeleitet aus der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander) übertragen wird.

Zwecks Informationssammlung bei der Überwachungsaufgabe sollte im Unternehmen ein möglichst breites Netzwerk an Sensoren aufgebaut werden. Dieses Netzwerk muss über alle Hierarchieebenen und Funktionen gespannt sein. Die Informationsverarbeitung hat sicherzustellen, dass die strategierelevanten Informationen an die entscheidenden Personen weitergeleitet werden. Die Informationsbearbeitung und -verarbeitung muss jederzeit beherrschbar sein und die „Best Practices“ des Kerngeschäfts müssen auch im IT-Bereich umgesetzt werden.[1] Ständig beherrschbar sein verlangt eine entsprechende IT-Sicherheit.

5.1.1.4.2 Kritikalitäts- und Kontext-orientiertes Management

Durch die Untersuchung der Ungewissheit bezüglich Umfeldentwicklungen in zwei Richtungen getrennt voneinander, wird der Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse in eine auf das System bezogene Seite (eigene Handlungsmöglichkeiten) und eine auf die Umwelt bezogene Seite (mögliche Randbedingungen des Umfelds) differenziert/zerlegt (Kap 4.1 Abb. 9). Dies dient dem Zweck der Operationalisierung der Aufgabe des strategisch-operativen Risiko-Controllings bezüglich des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume: Die ungewissen konkreten Zielvorgaben des IT-Security-Prozesses können so durch die angestrebte Handlungsbefähigung/strategisch-operative Beweglichkeit ersetzt werden.

Um das Modell in Kapitel 4.1 (->Abb. 9) zu verfeinern, wurde an der zweiten Richtung angesetzt, in der die Ungewissheit bezüglich Umfeldentwicklungen untersucht wurde: mögliche Randbedingungen des Umfelds (-> Abb. 10 Kapitel 4.2). Auf Ebene der auf das System bezogenen Kontextseite der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse stehende Ziele bezüglich der Unterstützung strategisch-operativer Handlungsspiel-

[1] vgl. Rentschler, Peter (2005b)

räume sollen in entsprechende Anforderungen auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen projiziert werden. Auf Basis des Modells in Kapitel 4.2 (-> Abb. 10) wird im Folgenden ein Modell für das strategisch-operative Risiko-Controlling entwickelt.

Die proaktive Berücksichtigung von umweltbedingten Unsicherheiten ist, in Konsequenz der Planungs- und Lenkungsaufgabe bezüglich des IT-Security-Prozesses, strategisch-operative Aufgabe der IT-Security bezogenen Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse. Dies soll vom zu entwickelnden strategisch-operativen IT-Security-Management basierend auf dem strategisch-operativen Risiko-Controlling umgesetzt werden.

Risiko und Sicherheit charakterisieren zwei unterschiedliche Blickwinkel auf die gleichen Objekte. Aufgabe des Risikomanagements ist es, festzustellen, wie kritisch und sensitiv die Sachwerte (vorhandene Systeme, Netzwerke, Applikationen und Informationen) und Prozesse sind, und zu evaluieren, welche Sicherheitsmaßnahmen (bezüglich der Anforderungskriterien der IT-Sicherheit) zu deren Schutz notwendig sind.

Es entwickelt sich eine Abbildung des IT-Security-Frameworks, das in Form einer Transformation die Ebene der IT-Sicherheit unter der Ebene der IT-Infrastruktur mit der strategischen Sichtweise ((Effektivität), Geschäftsfelder und ihre Erfolgsfaktoren) verbindet.

Abb. 15 Strategisch-operatives Risiko-Controlling

Dieses Modell ermöglicht, die strategisch-operative, zukunftsorientierte Bedeutung der Sicherheit von Informationssystemen Risiko-orientiert zu analysieren. Dabei sollen die Anforderungen zur Ausgestaltung der - auf die Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit (bei der Durchsetzung/Umsetzung/ Implementierung der Unternehmensstrategie und Abstimmung der Unternehmensziele und der Geschäftsprozesse/des IT-Security-Prozesses aufeinander) abzielenden - strategisch-operativen Sicherheit von Informationssystemen im technisch-operativen Kontext der IT-Sicherheit von Systemen beschrieben werden können.

In dieses Modell werden die Komponenten des strategischen und operativen Performance Managements integriert. Damit soll das Modell – neben dem oben beschriebenen Aspekt - die vom „management control“ gefordertem Systeme zur Unterstützung der Strategieformulierung und -umsetzung abbilden.

Die strategische Prämissenkontrolle soll die für Formulierung und Realisierung von Strategien gesetzten Prämissen, die Annahmen, wie relevant die Konformität mit entsprechenden Ordnungsmäßigkeitsvorgaben ist, regelmäßig auf ihre auch zukünftige Gültigkeit überprüfen. Die operative Prämissenkontrolle soll die für die Abstimmung der Unternehmensziele und Geschäftsprozesse/des IT-Security-Prozesses aufeinander gesetzten Prämissen, die Annahmen, wie relevant die Konformität mit entsprechenden Ordnungsmäßigkeitsvorgaben ist, regelmäßig auf ihre auch zukünftige Gültigkeit überprüfen. Im hier entwickelten Modell, wo die Handlungsbefähigung/strategisch-operative Beweglichkeit als Voraussetzung für die effiziente Realisierung/Umsetzung von Strategien und Abstimmung der Unternehmensziele und Geschäftsprozesse/des IT-Security-Prozesses aufeinander im Mittelpunkt steht, geht es um Ordnungsmäßigkeitsvorgaben zur Erreichung der angestrebten Handlungsbefähigung/ strategisch-operativen Beweglichkeit.

Die strategische Prämissenkontrolle betrifft die Planung im Zusammenhang mit der Effektivität, wurde daher an die Ebene der strategischen Sichtweise, eigene Handlungsmöglichkeiten/Flexibilität/Handlungsbefähigung anschließend eingetragen. Die operative Prämissenkontrolle betrifft die Planung im Zusammenhang mit der Effizienz, insbesondere der notwendigen Verlässlichkeit und Beherrschbarkeit der von der Abstimmung der Unternehmensziele und Geschäftsprozesse/des IT-Security-Prozesses aufeinander betroffenen bzw. notwendigen IT-Systeme und implementierten Maßnahmen, wurde daher an die Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen anschließend eingetragen.

Die Ordnungsmäßigkeitsvorgaben sollen sich auf die festgelegten Standards und Best Practices sowie die Kritikalität/Sensitivität entsprechender Sachwerte und Prozesse, auf die von den betroffenen Systemen bzw. implementierten Maßnahmen zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse eingesetzten Technologien, Methoden und Anwendungen sowie der entsprechenden Aufbau- und Ablauforganisation beziehen. Die internen Ordnungsmäßigkeitsvorgaben zielen ab auf die Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume.

Umsetzungsrisiken werden auch als Risiken aus prozessualen Werttreibern bezeichnet; sie stehen im Mittelpunkt der Prozesssteuerung und charakterisieren sich durch einen stark intern gerichteten Fokus (Geschäftsprozessfokus).[1]

Neben Risiken im Kontext Handlungsbefähigung/strategisch-operative Beweglichkeit (z. B. aufgrund mangelnder Flexibilität des Managements), kann auch die Projektion der Sicht der Betroffenen zur Beurteilung der Beherrschbarkeit des Systems, sowie die Projektion der Sicht zur Beurteilung der Verlässlichkeit des Systems in den Kontext der Handlungsbefähigung auf Strategie-Umsetzungsgefahren/Gefahren bei der Abstimmung der Unternehmensziele und Geschäftsprozesse/des IT-Security-Prozesses aufeinander, hindeuten.. Dies scheint geeignet, unvorhergesehener Störungen in der zukünftigen Entwicklung aufzeigen, und wird identifiziert als die Aufgabe der (strategischen bzw. operativen) Durchführungskontrolle, die Informationen bereitzustellen hat, die auf zukünftige Strategie-Umsetzungsgefahren hindeuten. Die strategische Durchführungskontrolle soll direkte Risiken im Kontext Handlungsbefähigung/strategisch-operative Beweglichkeit aufdecken. Die operative Durchführungskontrolle soll dagegen primär Gefahren bei der Abstimmung der Unternehmensziele und Geschäftsprozesse/des IT-Security-Prozesses aufeinander aufdecken, welche sich über die Projektion der Sicht der Betroffenen zur Beurteilung der Beherrschbarkeit des Systems, sowie die Projektion der Sicht zur Beurteilung der Verlässlichkeit des Systems, im Kontext Handlungsbefähigung ergeben.

Nicht nur Risiken selbst, sondern auch die Prozesse zu deren Erfassung, Bewertung und Steuerung sind auf Effektivität und Effizienz zu überprüfen, wobei eine – auf die Optimierung der Effektivität abzielende – strategische, und eine – auf die Optimierung der Effizienz abzielende – operative Überprüfung unterschieden werden kann.

[1] Vgl. Wolf, Klaus (2003b), S.177

Die negative Beeinflussung einer geplanten Zielsetzung kann in Form einer Verfehlung der strategischen Ziele oder einer direkten operativen Ergebniswirkung auftreten.[1] Entsprechend ist die strategische Überprüfung auf die strategischen Ziele und die operative Überprüfung auf die operativen Ergebnisse ausgerichtet. Dabei sind Leistungs- und Zielgrößen immer aus der Strategie abzuleiten.

In der Finanz-orientierten Perspektive wäre ein strategisches Ziel z. B. eine Eigenkapitalausstattung über dem Branchendurchschnitt und ein zugehöriges operatives Ziel eine überdurchschnittliche Liquiditätsvorsorge trotz starkem Umsatzrückgang. In der Kunden-orientierten/Markt-orientierten Perspektive wäre ein strategisches Ziel z. B. die Marktführerschaft bei bestimmten Produkten/Ausbau der Marktposition, und ein zugehöriges operatives Ziel die Kundenzufriedenheit durch z. B. verbessertes Qualitätsmanagement. Und in der Prozess-orientierten Perspektive wäre ein strategisches Ziel z. B. eine integrierte Prozesskette beim gesamten Wertschöpfungsprozess und ein zugehöriges operatives Ziel die Integration der Lieferanten und Logistikpartner in den Unternehmensablauf.[2] Dabei gilt es, Wirkungszusammenhänge zwischen den Strategien und den kritischen Erfolgsfaktoren aufzuzeigen. Diese sind wichtig für Planung und Steuerung der Unternehmensprozesse[3], auch für den IT-Security-Prozess. Es stehen die Ursache-Wirkungs-Beziehungen, die Zusammenhänge und Abhängigkeiten zwischen den Erfolgsfaktoren und den strategischen Zielen im Vordergrund. Dabei geht es nicht um die Perspektiven Finanz-orientierte Perspektive, Kunden-orientierte/Markt-orientierte Perspektive, Prozess-orientierte Perspektive, sondern um die Perspektive „Umfeld“, welche als „Äußeres Umfeld“ auch (neben der Finanz-orientierten Perspektive, Mitarbeiterperspektive, Kunden-orientierten/Markt-orientierten Perspektive, Prozess-orientierte Perspektive) die Perspektiven der „orginären“ Balanced Scorecard bezüglich Risikomanagement erweitert.[4]

Im Modell zum strategisch-operativen (Risiko-)Controlling der IT-Security sind die operativen Ergebnisse im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen die optimierte Verlässlichkeit und die optimierte Beherrschbarkeit der von der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und Geschäftsprozesse/des IT-Security-Prozesses aufeinander betroffenen bzw. notwendigen IT-Systeme und implementierten Maßnahmen. Diese kritischen Erfolgsfaktoren (Verlässlichkeit und Beherrschbarkeit) können auch als Frühwarnindikatoren aufgefasst werden.

[1] vgl. Kirchner, Michael (2002), S.16
[2] vgl. Kirchner, Michael (2002), S.60-63
[3] vgl. Kirchner, Michael (2002), S.65
[4] vgl. Kirchner, Michael (2002), S.66-70

Die (strategische und operative) Überwachung wird mit der Aufgabe identifiziert, mögliche Abweichungen von Prämissen – also Fehleinschätzung, wie kritisch und sensitiv die Sachwerte und Prozesse sind und wie relevant die Konformität mit entsprechenden Ordnungsmäßigkeitsvorgaben ist – aufzuzeigen, orientiert an der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume. Die strategische Überwachung betrifft Fehleinschätzungen auf Ebene der strategischen Sichtweise, eigene Handlungsmöglichkeiten/Flexibilität/Handlungsbefähigung und deren Auswirkungen im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen (Effizienz); sie. wurde daher vor der Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen aufsetzend eingetragen. Die operative Überwachung betrifft Fehleinschätzungen auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen und deren Auswirkungen in der strategischen Sichtweise, eigene Handlungsmöglichkeiten/Flexibilität/Handlungsbefähigung (Effektivität), sie wurde daher vor der Ebene der strategischen Sichtweise, eigene Handlungsmöglichkeiten/Flexibilität/Handlungsbefähigung aufsetzend eingetragen.

Die im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen zu analysierenden IT-Risiken entsprechen den – in Anlehnung an das Konzept des strategischen bzw. operativen Performance-Managements – definierten Risiken. Dies sind die Prämissen- bzw. Selektionsrisiken der Planung (Irrtumsrisiken der Selektions- und Filterkriterien bei der Fokussierung auf die wichtigsten Prämissen der Strategie) sowie die möglichen zukünftigen Strategie-Umsetzungsgefahren/Gefahren bei der Abstimmung der Unternehmensziele und der Geschäftsprozesse/des IT-Security-Prozesses aufeinander. Diese Analyse orientiert sich an der Bedeutung für die Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume.

Neben den aktuellen und potenziellen Risiken und den Prozessen sind auch verschiedene Prämissen einem Kontrollvorgang zu unterziehen. Beim Risiko-Controlling fallen in diese Kontrolle vor allem die festgelegten Ziele in Bezug auf die Risikoposition des Unternehmens sowie die Ursachen-Risiken-Verknüpfungen.[1] Prämissen- bzw. Selektionsrisiken der Planung, Irrtumsrisiken der Selektions- und Filterkriterien bei der Fokussierung auf die wichtigsten Prämissen der Strategie resultieren hauptsächlich aus einer Fehleinschätzung, wie kritisch und sensitiv gewisse (Sach)Werte (vorhandene Systeme, Netzwerke, Applikationen und Informationen) und Prozesse sind. Sie beziehen sich auf die Qualität der Prämissenfestlegung. Die Prämissen sind also die Annahmen, wie relevant die Konformität mit entsprechenden

[1] vgl. Burger, Anton/Buchhart, Anton (2002), S.65

Ordnungsmäßigkeitsvorgaben ist, und wie kritisch und sensitiv gewisse (Sach)Werte und Prozesse sind.

Die aus Fehleinschätzungen der Kritikalität/Sensitivität der Sachwerte und Prozesse sich ergebenden Prämissen- bzw. Selektionsrisiken der Planung beziehen sich auf die festgelegten Ziele und Ursachen-Risiken-Verknüpfungen (Kausalketten). Diese Fehleinschätzungen sind Hinweise zur Beurteilung/Erfolgskontrolle/Überwachung der Zielerreichung und sollen mit der strategischen und operativen Überwachung aufgedeckt werden.

Die mit der strategischen und operativen Überwachung aufzudeckenden Planungsrisiken (Prämissen- bzw. Selektionsrisiken der Planung) entsprechen im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen den IT-Risiken, die sich daraus ergeben, dass

- aufgrund von Prämissen-Fehleinschätzungen keine adäquaten Maßnahmen bestimmt werden und somit auch nicht implementiert werden können.

Strategie-Umsetzungsgefahren beziehen sich auf den das Problemlösungsverhalten bestimmendem Input. Sie bestehen einerseits potenziell bei mangelnder Flexibilität vor allem im Hinblick auf organisatorische, Management-spezifische und personelle Fragestellungen. Diese Risiken sollen mit der strategischen Durchführungskontrolle aufgedeckt werden. Umsetzungsgefahren resultieren andererseits aus unzureichender Verlässlichkeit und Beherrschbarkeit der von der Abstimmung der Unternehmensziele und der Geschäftsprozesse/des IT-Security-Prozesses aufeinander betroffenen Systeme und zu implementierenden Maßnahmen. Diese Risiken sollen in den Kontext der Handlungsbefähigung/strategisch-operativen Beweglichkeit abgebildet und speziell mit der operativen Durchführungskontrolle aufgedeckt werden.

Die mit der strategischen und operativen Durchführungskontrolle aufzudeckenden Umsetzungsrisiken entsprechen im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen den IT-Risiken, die sich daraus ergeben, dass

- die notwendige Verlässlichkeit und Beherrschbarkeit der von der Abstimmung der Unternehmensziele und Geschäftsprozesse/des IT-Security-Prozesses aufeinander betroffenen Systeme bzw. der zu implementierenden Maßnahmen nicht gegeben ist.

Das Überwachungsrisiko ist das Risiko, dass die der Strategie zugrunde liegenden Prämissen ex-ante nicht mehr gültig sind. Die regelmäßige Überprüfung der der strategischen und operativen Planung zugrunde liegenden Prämissen auf ihre auch zukünftige Gültigkeit ist

Aufgabe der strategischen und der operativen Prämissenkontrolle. Überwachungsrisiken sollen also mit der strategischen und der operativen Prämissenkontrolle aufgedeckt werden.

Die mit der strategischen und operativen Prämissenkontrolle aufzudeckenden Überwachungsrisiken entsprechen im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen den IT-Risiken, die sich daraus ergeben, dass

- die Relevanz der von den betroffenen Systemen bzw. implementierten Maßnahmen zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse eingesetzten Technologien, Methoden und Anwendungen sowie der entsprechenden Aufbau- und Ablauforganisation ex-ante nicht korrekt bestimmt wird.

Über obige Komponenten soll die Abbildung des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in die auf das System bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume (bezüglich Effektivität und Effizienz) optimierbar gemacht werden. So wird die im Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume betrachtete wirkungsbezogene Risikokomponente in Abhängigkeit der im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen betrachteten ursachenbezogenen Risikokomponenten analysiert. Wirkungsbezogene und auch ursachenbezogene Risikokomponenten beruhen im Allgemeinen auf lenkbaren wie auch nicht lenkbaren Größen. Im Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume sollen sich lenkbare Risikokomponenten ergeben. Im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen spielen lenkbare wie auch nicht lenkbare Größen eine Rolle. Nicht lenkbare Größen sind im Kontext Verlässlichkeit (beurteilt nach den Kriterien Verfügbarkeit, Integrität und Vertraulichkeit) anzufinden, während der Kontext Beherrschbarkeit (mit den Aspekten Komplexitätsreduktion und Kontrollierbarkeit) gerade die Lenkbarkeit widerspiegelt.

Die Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in die auf das System bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume muss gleichzeitig eine Spezialisierung der Anpassung des gesamten Unternehmens einschließlich der Schnittstellen zu Kunden und

Lieferanten im Rahmen einer umfassenden Unternehmenstransformation (damit die IT ihr Nutzenpotenzial in Bezug auf die Geschäftsprozesse entfalten kann) darstellen. Das IT-Security-Framework auf Basis des strategisch-operativen Risiko-Controllings soll einen Rahmen für die Umsetzung dieses Anpassungsprozesses an die Umgebung im Bereich der IT-Security vorgeben.

Das strategische Performance Management steuert die Formulierung und Realisierung von Strategien, das operative Performance Management stimmt die Unternehmensziele und die Geschäftsprozesse aufeinander ab. Strategisch-operative Beweglichkeit/Handlungsbefähigung wird im Modell zum strategisch-operativen Risiko-Controlling als durch Realoptionen abzubildende Entscheidungsfreiheit modelliert. Bei der Formulierung und Umsetzung von Strategien sowie der Abstimmung der Unternehmensziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander muss das Management des Unternehmens entsprechende Entscheidungsfreiheiten haben. Bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und der Geschäftsprozesse aufeinander benötigt das Unternehmen eine entsprechende strategisch-operative Beweglichkeit/Handlungsbefähigung. Die Gefährdung für Formulierung und Umsetzung der strategisch-operativen Zielsetzungen des Unternehmens durch IT-Risiken liegt u. a. darin begründet, dass die (als Voraussetzung zum Erreichen der strategisch-operativen Zielsetzungen des Unternehmens angesehene) strategisch-operative Beweglichkeit/Handlungsbefähigung auch von der IT-Sicherheit entsprechender IT-Systeme abhängt.

Des Weiteren kann die Realisierung/Umsetzung der Unternehmensstrategie bzw. die Abstimmung der Unternehmensziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander auf die Realisierung/Umsetzung der IT-Security-Strategie bzw. Abstimmung der Unternehmensziele und des IT-Security-Prozesses bzw. Abstimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander spezialisiert werden. Dazu soll in die Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in die auf das System bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse, in Form der Komponenten (strategische und operative) Prämissenkontrolle, (strategische und operative) Durchführungskontrolle und (strategische und operative) Überwachung) ein Anpassungsprozess an die „Umgebung“ bezüglich der IT-Security integriert werden. Dazu sind geeignete Anforderungen zur Gestaltung von (strategischer und operativer) Prämissenkontrolle, (strategischer und operativer) Durchführungskontrolle und (strategischer und operativer) Überwachung zu stellen. So kann der IT-Security-Prozess gemanagt, gesteuert und gelenkt werden.

IT-Sicherheitsorganisation und IT-Sicherheitskonzept sind die Werkzeuge des Managements zur Umsetzung ihrer IT-Sicherheitsstrategie.[1] Die IT-Sicherheitsorganisation umfasst Regeln, Anweisungen, Prozesse, Abläufe und Strukturen. Die wie oben beschriebene (strategische und operative) Prämissenkontrolle, (strategische und operative) Durchführungskontrolle und (strategische und operative) Überwachung können als Teil dieser IT-Sicherheitsorganisation aufgefasst werden.

Indem die Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security in das, auf die strategisch-operative Beweglichkeit/Handlungsbefähigung abzielende Modell zum strategisch-operativen Risiko-Controlling integrier werden, soll das Modell zum strategisch-operativen Risiko-Controlling einen Anpassungsprozess an die „Umgebung“ bezüglich der IT-Security enthalten, der dieses Modell auf die Strategie konforme und IT-Nutzenpotenzial absichernde Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume ausrichtet.

Das strategische und das operative Performance Management im Modell zum strategisch-operativen Risiko-Controlling bilden diesen Anpassungsprozess an die „Umgebung“ bezüglich der IT-Security und einen PDCA-Zyklus im Sinne der ISO 270001 ab (-> Kap. 5.1.3).

Aus den Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security (im Zusammenhang mit dem rechtlichen, organisatorischen und technischen Umfeld) ergeben sich Anforderungen zur Gestaltung der Komponenten des strategischen Performance Managements (strategische Prämissenkontrolle, strategische Überwachung und strategische Durchführungskontrolle) und des operativen Performance Managements (operative Prämissenkontrolle, operative Überwachung und operative Durchführungskontrolle).

Dieses Modell stellt eine Abbildung des Frameworks, das in Form einer Transformation die Ebene der IT-Sicherheit/IT-Security mit der strategischen Sichtweise verbindet, mithilfe von Konzepten des strategischen (und operativen) Controllings dar. Es geht davon aus, dass die wesentlichen Inhalte der IT-Strategie, welche

- Formulierung eines zukünftigen Sollzustands
- Aufzeigen des Handlungsbedarfs
- Ermittlung von Handlungsoptionen
- Setzen von Zielen und Definieren von Maßnahmen
- Festlegung der Verantwortung
- Bestimmung von Messgrößen

[1] BSI (2006), S.25

umfassen,[1] auch für ein strategisch-operatives IT-Security-Management gelten. Strategiegestaltung fordert, dass gerade in Zeiten dynamischer Veränderungen die unternehmerische Handlungsfähigkeit im Bezug auf strategisch relevante Aktivitäten (z. B. Investitionsentscheidungen) stets gewährleistet sein muss.[2] So rückt das hier entwickelte Modell die Betrachtung der Bedrohung der Handlungsfähigkeit des Unternehmens in den Mittelpunkt, und zielt so ab auf die Analyse von Realoptionen (Managementansatz zur proaktiven Berücksichtigung von umwelt- und wettbewerbsbedingten (hier umfeldbedingten) Unsicherheiten). Diese Unsicherheiten beziehen sich auf mithilfe geeigneter IT-Projekte umzusetzende und zu optimierende Geschäftsprozesse und Geschäftsmodelle des Unternehmens bei der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse.

Das entwickelte strategisch-operative Risiko-Controlling ist nicht Teil des Prozesses zur Identifikation, Bewertung, Steuerung und Überwachung von Risiken, sondern ein übergeordneter/unabhängiger Baustein zur Risikosteuerung, am ehesten in Form der Risikokompensation (Risikoakzeptanz). In Kap. 5.1.3 geht es um die Steuerung des IT-Security-Managements mithilfe des Modells zum strategisch-operativen Risiko-Controlling. Damit soll die Effektivität und Effizienz des IT-Security-Managements, welche die strategisch-operative Beweglichkeit/Handlungsbefähigung des Unternehmens unterstützen soll, gewährleistet werden.

Im Sinne der Szenario-Software geht es darum, sich dem Wandel und vorgegebenen Strukturen anzupassen und diese umzusetzen. Die Szenario-Software wird quasi in die Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in die auf das System bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume eingebaut. So bildet das Performance-Management, das in die Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in die auf das System bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse eingefügt wurde, im Prinzip die entsprechende Szenario-Software ab. Allerdings werden in der auf das System bezogenen Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse keine Alternativen entwickelt, sondern es wird davon ausgegangen, dass entsprechende Optionen/Flexibilitätspotenziale für die strategisch-operative Beweglichkeit/Handlungsbefähigung des Unternehmens als Voraussetzung für die effiziente Umsetzung der Unternehmensstrategie und Abstimmung der Unter-

[1] vgl. Gadatsch, Andreas (2004), S.54,55
[2] vgl. Ehrmann, Thomas (2006), S.1

nehmensziele und der Geschäftsprozesse aufeinander bzw. Umsetzung der IT-Security-Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses bzw. Abstimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander gegeben sein müssen.

In Kapitel 5.1.3 und 6.3 werden hierzu keine neuen Modelle entwickelt, sondern das hier entwickelte Modell aus verschiedenen Sichten betrachtet: In Kapitel 5.1.3 wird das Modell zum strategisch-operativen Risiko-Controlling zur Konzeptionierung eines strategisch-operativen IT-Security-Managements herangezogen und in einen strategischen und einen operativen Teil zerlegt. In Kapitel 6.3 wird das Modell zum strategisch-operativen Risiko-Controlling zur Analyse, Bewertung und Optimierung auf den Ebenen der Unternehmensplanung herangezogen. So werden die Anforderungen konkretisiert, die - wenn die auf die strategische Zielsetzung einwirkenden und deren Erreichung gefährdenden Risiken nicht vorhersehbar/abschätzbar sind - zur Umsetzung der strategischen Zielsetzung notwendig sind und sich auf die Objekte beziehen, für die man eigentlich eine Risikoanalyse durchführen müsste. Aus diesen Anforderungen können Maßnahmen abgeleitet werden, die die entsprechend der Kritikalität der betreffenden IT-Objekte relevanten Anforderungen präventiv abdecken. So wird die Alternative zur Antizipation von Risiken auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen operationalisiert.

Zunächst wird jedoch dargestellt, welche Ziele und Aufgaben das (IT)-Risikomanagement hat, um zu zeigen, dass das entwickelte strategisch-operative Risiko-Controlling dazu geeignet ist, diese Ziele und Aufgaben zu überwachen/zu steuern.

5.1.2 IT-Risikomanagement

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), das Bilanzrechtsreformgesetz (BilReG), das Bilanzkontrollgesetz (BilKoG), Basel II u. a. Vorschriften wie die MaRisk sowie vermehrte Schadensereignisse in den letzten Jahren mit damit einhergehenden Haftungsproblematiken erfordern ein wirksames Risikomanagement und wirksame Frühwarnsysteme. Bestandteil eines Risikomanagement-Systems ist nach herrschender Meinung ein sog. Überwachungssystem. Frühwarnsystem sowie Controlling (welches die

Kontinuität des Risikomanagements sicherstellen soll[1]) sollen dem Risikomanagement-System als ergänzende Komponenten beistehen.[2]

Risikomanagement steht für den „aktiven Umgang mit unerwünschten Nebenfolgen menschlicher Aktivitäten“ und ist ein „Zeugnis für die Transformation von ursprünglich extern wahrgenommenen Gefahren in bearbeitbare, sozial beeinflussbare und steuerbare Aktivitäten zur Begrenzung von unerwünschten Handlungsfolgen“. Dabei werden als extern gesehene Gefahren als in intern regelbare Risiken transformiert aufgefasst.[3] Der Zweck des Risikomanagements besteht in der systematischen Handhabung von Risiken, um eine erfolgreiche Umsetzung der Unternehmensziele zu ermöglichen. Ein Risikomanagement-System dient „als Subsystem der Unternehmensführung der Verfolgung der unternehmerischen Zielsetzung“.[4] In diesem Sinne wird Risikomanagement in einem projektorientierten Anwendungsleitfaden der DIN IEC 56/629/CD als die „systematische Anwendung von Managementgrundsätzen, Verfahren und Praktiken zwecks Feststellung, Analyse, Behandlung und Überwachung von Risiken, sodass Organisationen Verluste minimieren und Chancen optimieren können“, definiert.[5]

Nach berufsständiger Auffassung des IDW erfasst das Risikomanagement „die Gesamtheit aller organisatorischen Regelungen und Maßnahmen zur Risikoerkennung und zum Umgang mit den Risiken unternehmerischer Betätigung“.[6]

Risikomanagement soll ermöglichen, erfolgsorientierte, rational begründete Entscheidungen im Umgang mit Risiken zu treffen.[7] Für die Sicherstellung einer kontinuierlichen Weiterentwicklung und Qualität des Früherkennungs-/Überwachungssystems ist größtenteils die Interne Revision verantwortlich.[8]

Dabei kann die Risikosituation eines Unternehmens nur dann umfassend erfasst werden, wenn man auch die Komplexität der Vernetztheit (mit dem Umfeld) und das System als Ganzes analysiert.[9] Geht man von Risiko im Sinne des KonTraG als Verlustgefahr aus, was im Zusammenhang mit IT-Sicherheit zumeist nur gesehen wird, so kann man „erfolgsorientiert“ folgendermaßen interpretieren: Das Hauptziel des Risikomanagements ist Stabilität, definiert als die „Fähigkeit von Geschäftsvorgängen, Organisationen und technischen Systemen, im Fall von Störungen, unvorhergesehenen Ereignissen und Unfällen das Geschäft weiterzu-

[1] vgl. Wolf, Klaus (2003b). S.5
[2] vgl. Wolf, Klaus (2003b), S.3
[3] vgl. Hölscher, Reinhold (2002), S.76,77
[4] Kirchner, Michael (2002), S.18
[5] vgl. Dahmen, Jörn (2002), S.17
[6] vgl. Hölscher, Reinhold (2002), S.98
[7] vgl. Finke, Robert (2005), S.23
[8] vgl. Wolf, Klaus (2003b), S.8
[9] vgl. Romeike, Frank (2005, S.31

führen und ihre Substanz wirksam vor Schaden zu bewahren …, grob gesagt, im Fall von Schwierigkeiten zu überleben“.[1] Risikomanagement muss dabei in die Geschäftsprozesse eines Unternehmens integriert werden.

Aus dem Ziel der Existenzsicherung ergibt sich für das Risikomanagement die Aufgabe, die Unternehmensführung bei der Erreichung aller definierten Ziele zu unterstützen. So muss sichergestellt werden, dass die vom Unternehmen zu tragenden Risiken auf ein akzeptables Maß begrenzt bleiben. Risikomanagement als Bestandteil der Unternehmensführung stellt also die Integration aller organisatorischen Maßnahmen, risikopolitischen Grundsätze, sowie aller führungsunterstützenden Planungs-, Koordinations-, Informations- und Kontrollprozesse dar, die auf eine systematische und kontinuierliche Identifikation, Beurteilung, Steuerung und Überwachung der unternehmerischen Risikopotenziale abzielen und eine Gestaltung der Risikolage des Unternehmens mit dem Ziel der Existenzsicherung dienen. Das Risikomanagement muss dabei ständig an die sich stetig verändernde Unternehmensumwelt angepasst und weiterentwickelt werden.[2]

Das in Deutschland gesetzlich vorgeschriebene Risikomanagement (Risikofrüherkennung) umfasst nur einen Teil des betrieblichen Risikomanagements. Letzteres beinhaltet organisatorische Regelungen und Maßnahmen zur Risikoerkennung als auch zum Umgang mit den Risiken unternehmerischer Betätigung allgemein. Risiko i. S. d. KonTraG betrachtet reine Verlustrisiken, wohingegen das betriebliche Risikomanagement Verluste als auch das mit dem bewussten Eingehen von Risiken verbundene Chancenpotenzial betrachtet.

Das Risikomanagement muss die Frage beantworten, welches Risiko für welchen Erfolg noch akzeptabel ist. Ziel ist die Formulierung eines Zusammenhangs zwischen zu erwartetem Erfolg und den dazu gezielt zu übernehmenden Risiken sowie die Einleitung von Maßnahmen zur gleichzeitigen Optimierung beider Größen.[3]

Nach berufsständischer Rechtsauslegung des IDW ist das Risikomanagement als Ganzes aber kein Prüfungsgegenstand i. S. v. § 317 Abs. 4 HGB. Die Prüfung erstreckt sich ausschließlich auf das nach § 91 Abs. 2 geforderte Risikofrüherkennungs- und Risikoüberwachungssystem. Die Qualität der Handlungen zur Risikobewältigung ist nicht Gegenstand der Prüfungspflicht.

Im Zusammenhang mit der gegebenen Thematik geht es jedoch nicht um Frage Pflichtprüfung (z. B. im Rahmen der Jahresabschlussprüfung) oder freiwillige Prüfung, da Revision als projektbegleitende Aufgabe (und Aspekt der Überwachung) gesehen wird.

[1] Wieczorek, Martin (2003), S.14
[2] vgl. Diederichs, Marc (2004), S.14-16
[3] vgl. Finke, Robert (2005), S.24

Im Zusammenhang mit der IT-Sicherheit ist als Erfolg die Stabilität von Geschäftsvorgängen, Organisationen und technischen Systemen gezielt zu analysieren. Gezielt bedeutet, inwieweit Risiken der IT-Sicherheit Auswirkungen auf das Erreichen der unternehmerischen Zielsetzung haben.

Erforderlich für die Einbindung von Informationssicherheit in das Risikomanagement ist zunächst die Analyse und Bewertung von Sicherheitsrisiken. Tritt ein Risiko ein, das die Verfügbarkeit, Vertraulichkeit oder Integrität der IT-Infrastruktur einschränkt, so laufen die entsprechenden Applikationen in dieser IT-Infrastruktur nicht mehr verlässlich, was sich wiederum auf die unterstützten Geschäftsprozesse und damit das Geschäft auswirkt. Daneben existieren in die Geschäftsprozesse verankerte Kontrollziele des Geschäfts. Auch hier ergeben sich durch den IT-Einsatz Risiken, die die IT-Kontrollen einschränken und eine direkte Auswirkung auf die Geschäftsprozesse haben.

Ein Ansatz zur Durchführung des IT-Risikomanagements leitet sich daraus ab, Risiken mit den Schwachstellen eines IT-Systems zu identifizieren. Die Identifizierung setzt voraus, dass vorher Sicherheitsziele und Sicherheitsstrategien festgelegt wurden. Ist dies nicht der Fall, muss eine Analyse der Strategie des Unternehmens, seiner Stärken, Schwächen, Chancen und Gefahren, sowie seines Umfelds vorgeschaltet werden.[1] Das Risikomanagement wird dann durch Schwachstellenbeseitigung betrieben.[2]

Ein Risikomanagement-Projekt soll die IT-Sicherheitsfragestellungen einer Institution abhandeln. Dabei sollen alle entsprechend der Risikopolitik als nicht tragbar erkannten Risiken möglichst weitgehend beseitigt werden.[3] Ziel der Risikopolitik ist es, die Sicherheit zu erhöhen bzw. ein definiertes Sicherheitsniveau zu erreichen, was durch die Beseitigung bzw. die Veränderung der Risikoursachen einerseits und die Vorsorge für den Fall des Schadenseintritts andererseits versucht wird. Die Risikopolitik formuliert unabhängig von den operativen Gegebenheiten abstrakt die risikobezogenen Grundgedanken, bevor mit dem Risikomanagementprozess konkrete Maßnahmen eingeleitet werden können. Dazu werden z. B. risikopolitische Ziele (risikofreudig, risikoneutral, risikoscheu) festgelegt.[4] Risikopolitische Grundsätze sind auf das Sicherheitsziel ausgerichtete Verhaltens- und Handlungsanweisungen.[5]

[1] Seidel, Uwe M. (2002(, S.64
[2] vgl. Vossbein, Reinhard (2004a) ,S.5
[3] vgl. Vossbein, Reinhard. (2004b)
[4] vgl. Ibers, Tobias (2005), S.49
[5] Diederichs, Marc (2004), S.17

Die Forderungen nach einem integrierten Risiko-Management werden z. B. durch KonTraG oder Sarbanes-Oxley-Act immer stärker. Mit den ÖNR 49000 als Vorlage für eine entsprechende ISO-Norm wurde den Unternehmen als erster Schritt erstmals eine Lösung an die Hand gegeben. Der IT-Bereich muss die sich aus dem Business ergebenden, auf die Zukunft bezogenen Anforderungen an die IT erkennen und umsetzen. Dazu müssen die eingesetzten Methoden zur Herstellung der IT-Sicherheit in ein Risikomanagement-System strategisch integriert werden.[1].

Risikomanagement /Risk-Management wird unterteilt in strategisches Risikomanagement und operatives Risikomanagement. Risk-Management wird auch als eine Form der Unternehmensführung gesehen, welche auf die Reduktion von Risiken abzielt, indem sie die Risiken erfasst, begleitend überwacht und entsprechende Handlungsstrategien entwickelt.[2]

Das strategische Risikomanagement ist die Basis für den weiteren Risikomanagementprozess. Es geht vor allem um die Formulierung von Risikomanagementzielen in Form einer Risikopolitik sowie die Grundlagen der Organisation des Risikomanagements.

Die Risikomanagement-Organisation definiert den aufbauorganisatorischen Rahmen des Risikomanagements. Im Rahmen des strategischen Risikomanagements erfolgt die organisatorische Einbettung in ein Unternehmen sowie die Kommunikation der risikopolitischen Grundsatzentscheidungen. Erforderlich ist eine genaue Identifizierung und Analyse von Potenzialen bzw. Strategien zur Ausnutzung operativer Flexibilität und zur Steigerung von Managementflexibilität.[3] Dabei kann ein adaptiver Strategiefindungsansatz helfen, durch den die Unternehmen ihre Flexibilität erhöhen, indem sie ihre Strategie auf mehrere Szenarien zuschneiden (entsprechend dem strategischen Grundsatz der Bewahrung der Flexibilität). Ein wesentlicher Erfolgsfaktor ist dabei die Früherkennung.[4] Ein Strategiefindungsansatz, der auf dem risikoreichsten Szenario aufbaut, wird im Rahmen der Krisenplanung angewandt.[5]

Das auf der systemisch-evolutionären Ausrichtung der Managementtheorie basierende strategische IT-Security-Management, welches sich auf die Anpassung an das Umfeld sowie der Begründung und Erhaltung der Handlungsfähigkeit des Unternehmens mit seiner Umwelt konzentriert, ist eine Ausprägung des strategischen Risikomanagements, für das eine genaue

[1] vgl. Rentschler, Peter (2005c):
[2] vgl. Kappeller, Wolfgang (2003), S.321
[3] vgl. Hommel, Ulrich (2001):, S..213,214
[4] vgl. Fink, Alexander (2001), S.154
[5] vgl. Fink, Alexander (2001), S.152

Identifizierung und Analyse von Potenzialen bzw. Strategien zur Ausnutzung operativer Flexibilität und zur Steigerung von Managementflexibilität erforderlich ist.

Das operative Risikomanagement beinhaltet den Prozess der systematischen und laufenden Risikoanalyse des Unternehmens und der Geschäftsabläufe. Aufgabe des operativen Risikomanagements/Risikocontrollings ist die „vollständige Erfassung aller Risikofelder des Unternehmens“. Die Interne Revision prüft die vollständige Erfassung.[1]

Gegenstand der Betrachtung sind die Risiken, die unmittelbar aus den Abläufen im Unternehmen, aus den Kern- und Unterstützungsprozessen resultieren, die zum Aufrechterhalten des Geschäftsbetriebs notwendig sind. Dabei zielen eine Reihe standardisierter Vorgehensweisen auf die Sicherheit operativer Prozesse ab:[2]

- das Qualitätsmanagement prüft im Zusammenhang mit der Produkthaftung, ob den untersuchten Prozessen spezifizierte Ziele vorgegeben sind, und ob und wie die Übereinstimmung der Ergebnisse mit diesen Sollvorgaben festgestellt wird
- das Umweltmanagement prüft im Zusammenhang mit der Umwelthaftung die Konformität von Prozessen mit gesetzlichen Auflagen zum Umweltschutz
- ähnliches gilt für Arbeitssicherheit, Brandschutz usw.

Das operative IT-Security-Management, welches ein angemessenes, wirtschaftlich vertretbares Niveau der IT-Security für das Unternehmen/die Behörde erreichen und bewahren soll, ist das auf die IT-Security bezogene operative Risikomanagement, dessen Ziel die betriebswirtschaftlich optimale Sicherheit und nicht die maximal zu erreichende Sicherheit ist.

Aufgabe der Risikoanalyse ist die Ermittlung der Ursachen und Interdependenzen der identifizierten Risiken.[3]

Das Risikomanagement-System besteht aus Risikofrüherkennungssystem und internem Überwachungssystem, welches wiederum aus Interner Revision, IKS und Risikocontrolling besteht.[4] Controlling erfasst die „zielorientierte Koordination von Planung, Informationsversorgung, Kontrolle und Steuerung“.[5]

Kontrolle ist eine

- mit dem betrieblichen Ablauf verbundene Überwachung und soll möglichst vor Beendigung eines Teilprozesses Fehler aufdecken bzw. verhindern.

[1] vgl. Schreiber, Ottokar R. (2003), S.8
[2] vgl. Hölscher, Reinhold (2002), S.241
[3] vgl. Martin, Thomas A. (2002), S.96
[4] vgl. Lentfer,Thies (2003), S.13
[5] vgl. Hölscher, Reinhold (2002), S.98

Kontrollen werden an einer Vielzahl von Stellen und Vorgängen durchgeführt. Da die Kontrolle von verschiedenen Funktionsträgern wahrgenommen wird, spricht man im Rahmen der innerhalb des Unternehmens erfolgenden Kontrolle vom „Internen Kontrollsystem“ (IKS). Der Umgang mit Risiken erfordert mindestens die Einrichtung eines angemessenen und funktionsfähigen internen Kontrollsystems.

Dieses IKS kann in organisatorische Sicherungsmaßnahmen (Verfahrensdimension) und Kontrollen (Ergebnisdimension) unterteilt werden. Zunächst hat das IKS für eine Ablauf- und Aufbauorganisation (unternehmerische Grundgefüge mit der Verteilung der Funktionen und Vernetzung der Funktionseinheiten) zu sorgen, die eine einheitliche Bearbeitung gleichartiger regelmäßig sich wiederholender Geschäftsvorfälle durch die Sachbearbeiter gewährleistet. Im Rahmen der EDV-gestützten Bearbeitung von Geschäftsvorfällen zählen zu den organisatorischen Sicherungsmaßnahmen beispielsweise Zugriffsbeschränkungen, System-programmierungen und elektronische Unterschriften. Kontrollen können dem jeweiligen Arbeitsvorgang vor-, nach- oder gleichgeschaltet sein. Insbesondere sind programmierte Sicherheitsvorkehrungen und Kontrollen zu nennen, die meist schon in den Standard-versionen der verschiedenen Buchhaltungsprogramme vorhanden sind. Merkmale eines vor-handenen IKS sind u. a. dokumentierte Organisationsanweisungen und Handlungsrichtlinien sowie Zugriffsbeschränkungen im Rahmen eines abgestuften Berechtigungsverfahrens für IT-Systeme und Anwendungen. Die organisatorischen Maßnahmen sollen die Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit sicherstellen. Es geht um die Überwachung von Prozessabläufen.[1] Das IKS wird im Sinne der GoB/GoBS als ordnungsgemäß angesehen, wenn die Erfassung und Bearbeitung aller Prozesse im Zusammenhang mit buchungs-pflichtigen Geschäftsvorfällen die Kriterien Vollständigkeit, Richtigkeit, Übersichtlichkeit und Zeitnähe erfüllen.[2] Ein allgemeines Ordnungsmäßigkeitskriterium für das IKS wäre, dass die Erfassung und Bearbeitung aller für die Geschäftstätigkeit wichtigen/kritischen Prozesse die Kriterien Vollständigkeit, Richtigkeit, Übersichtlichkeit und Zeitnähe erfüllen. Je nach Wichtigkeit der entsprechenden Geschäftsvorfälle ist eine Abstufung der Kriterien Übersicht-lichkeit und Zeitnähe denkbar.

Jedes IT-System zur Unterstützung der Geschäftsprozesse hat Einfluss auf die Rechnungs-legungssysteme und die Abbildung von Geschäftsprozessen. Sowohl Unternehmensleitungen als auch externe Revision müssen die sachgerechte Transaktionsabwicklung im Rechnungs-legungssystem unter Einhaltung nationaler und internationaler Anforderungen gewährleisten. Vor dem Hintergrund einer Geschäftsprozess-orientierten Vorgehensweise wird zur Analyse

[1] vgl. Kamlah, Bernd (2004c)
[2] vgl. Lentfer,Thies (2003), S.14

und Bewältigung von E-Business Risiken im „IFAC-Guideline E-Business and the Accountant: Risk-Management for Accounting-Systems in an E-Business Environment“ ein Rahmenkonzept mit best practice guidelines sowie Prinzipien und Kriterien für die Sicherheit und Ordnungsmäßigkeit von Rechnungslegungssystemen vorgeschlagen.[1]

Die IFAC ist der bedeutendste „International Standard-Setter“ der Wirtschaftsprüfung. Die Tätigkeit der IFAC zielt darauf ab, einen harmonisierten internationalen Berufsstand der "Accountants" zu entwickeln und permanent zu verbessern, um qualitativ hochwertige Prüfungsleistungen anbieten zu können. Die Normen der IFAC gehören zu den fachlichen Regeln i. S. von § 4 Abs. 1 Berufssatzung der Wirtschaftsprüfer. Sie sind gemäß § 43 Abs. 1 Wirtschaftsprüferordnung von einem gewissenhaft tätigen Wirtschaftsprüfer grundsätzlich heranzuziehen.

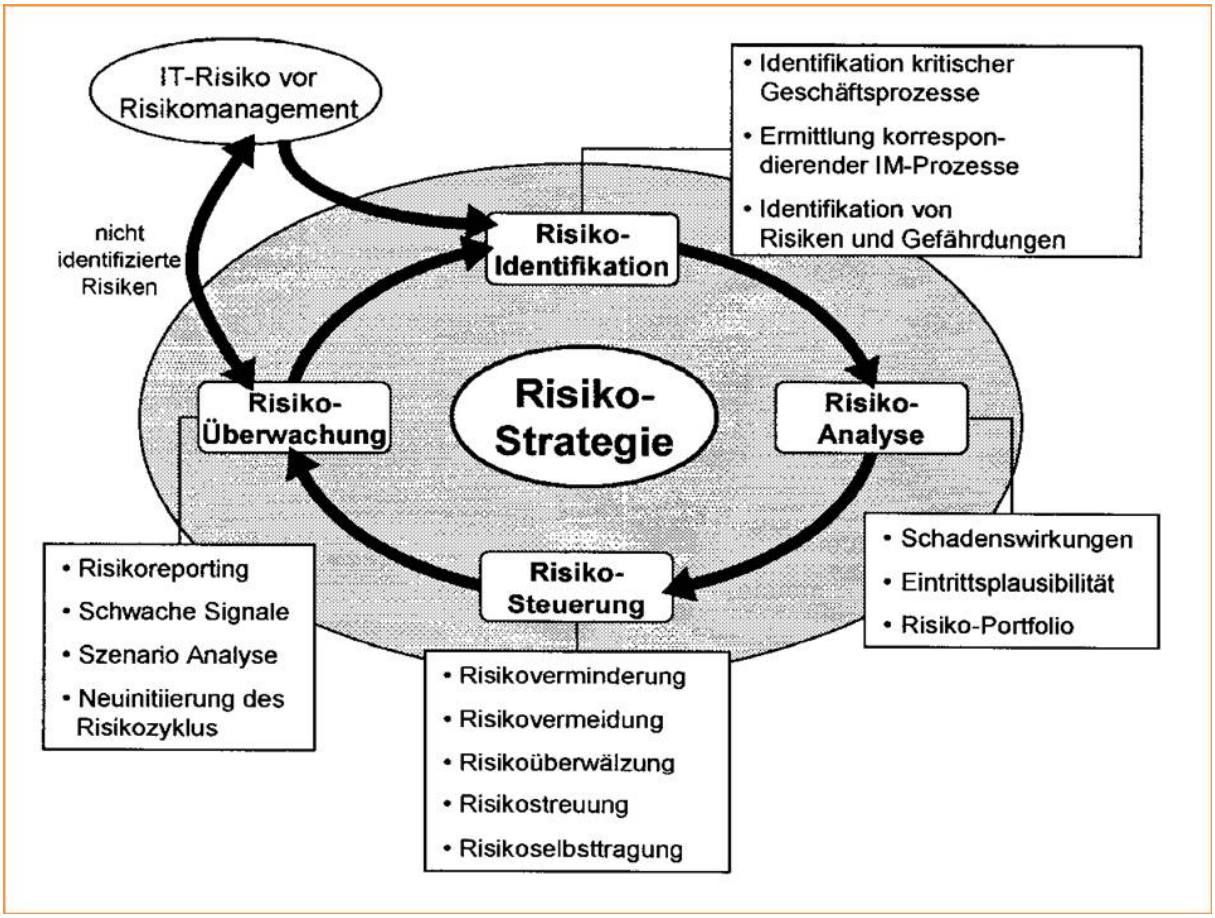
Methodisch kann die Risikofrüherkennung und Risikoüberwachung im Prinzip durch Erweiterung eines EIS (Executive Information System) -Konzepts in Richtung von OLAP (Online Analytical Processing) zur Überwachung kritischer Kennzahlen, Integration statistischer Methoden und Simulationsmodelle ermöglicht werden. Dabei können Data-Mining-Konzepte benutzt werden, um z. B. mittels statistischer Auswertungen und Prognosen aus vorhandenen Informationen neue Informationen zu erzeugen. Bei IT-Risiken sind statistische Auswertungen und Prognosen aber nicht sinnvoll. Daher werden im Folgenden die obigen operativen Aspekte des Risikomanagements nicht weiter verfolgt, sondern ein strategisch-operatives IT-Security-/Risikomanagement konzipiert.

Ein fest in die Unternehmensorganisation eingebetteter Risikomanagementprozess bedeutet neben einer Verbesserung und Erweiterung der Planungsprozesse auch eine permanente kritische Auseinandersetzung mit Risiken und potenziellen Steuerungsmaßnahmen im Unternehmen.[2]

Wichtig ist, dass es sich beim Risikomanagement Prozess um einen geschlossenen Regelkreis handelt, der zu einer „Optimierung der Risikosituation des Unternehmens führen soll“.[3] Neben den Risiken ist dabei auch der Regelkreis mit seinen einzelnen Phasen zu überwachen und an sich ändernde Gegebenheiten im Umfeld des Unternehmens anzupassen, um die „Effektivität bzw. Effizienz des Risikomanagement-Regelkreises aufrechtzuerhalten bzw. zu verbessern“. Die Ergebnisse des strategischen Risikomanagements fließen in die Ziele des

[1] vgl. IDW (2002c)
[2] Hölscher, Reinhold (2002), S.106
[3] Burger, Anton/Buchhart, Anton (2002), S.31

operativen Risikomanagements ein. Darüber hinaus haben die für das strategische Risikomanagement anzuwendenden Konzepte auch Konsequenzen für ein effizientes operatives Risikomanagement. Der Risikomanagement Prozess, welcher zyklisch die Phasen Risikoidentifikation (Aufspüren möglicher Gefährdungen), Risikoanalyse/-beurteilung (Ermittlung möglicher Schadenshöhen und Eintrittsplausibilitäten), Risikosteuerung/-begrenzung (aktive Beeinflussung der Risikosituation auf ein gewünschtes Risikoniveau) und Risikoüberwachung durchläuft,[1]



(Quelle: Krcmar, Helmut/Junginger, Markus (2003, S.256)

Abb. 16 Der Risikomanagementprozess

repräsentiert den Prozess des operativen Risikomanagements zur systematischen und laufenden Risikoanalyse des Unternehmens und der Geschäftsabläufe. Er ist im Prinzip, auf die IT-Security bezogen, im PDCA-Zyklus der ISO 27001 wieder zu finden.

Zunächst werden im Folgenden Konzepte/Instrumente zur Umsetzung des wie oben dargestellten operativen Risikomanagements und strategischen Risikomanagements dargestellt.

[1] vgl. Krcmar, Helmut/Junginger, Markus (2003), S.256

5.1.2.1 Beurteilung der Risikolage/Risikomapping, -analyse, -diagnose

Ein häufig eingesetztes Instrument für das Risikomanagement/Sicherheitsmanagement ist die auf einer Bedrohungs- und Schwachstellenanalyse basierende Risikoanalyse. Diese bestimmt, welche Schwachstellen das System aufweist und welche unterschiedlichen Bedrohungen auf das System einwirken. Unter einer Schwachstelle in IT-Infrastrukturen versteht man dabei grundsätzlich alles, was einem Angreifer ermöglicht, die IT-Sicherheit eines Systems/einer Anwendung zu beeinträchtigen, z. B. Fehlkonfigurationen, fehlerhafte Planung der Netzinfrastruktur, unachtsamer Umgang mit sensiblen Daten durch die eigenen Mitarbeiter. Eine Schwachstellenanalyse kann im White- oder Black-Box Verfahren erfolgen. Bei der Black-Box Variante sind keinerlei Informationen über die zu testende Infrastruktur bekannt. Diese Situation entspricht der des typischen Internethackers, der sein Ziel erst auskundschaften muss, bevor ein gezielter Angriff erfolgen kann. Beim White-Box Test werden Informationen über das Ziel vorgegeben, z. B. IP-Adressen, Informationen über verwendete Applikationen, organisatorischer Background (Handlungskonzepte, Backupszenarien …).[1]

Darauf aufsetzend kann bestimmt werden, welche Sicherheitsanforderungen erfüllt sind, und wo zusätzliche Maßnahmen zu installieren sind. Die für eine solche Risikoanalyse zunächst durchzuführende Schwachstellen- und Bedrohungsanalyse liefert einen Überblick über mögliche Gefahrenpotenziale, um so relevante, aber nicht offensichtliche und nicht vorhersehbare Risiken zu identifizieren. Es sind auch Risiken zu identifizieren, die auf den ersten Blick z. B. nicht als Bedrohung erkennbar sind: So sind etwa Operationelle Risiken (mögliche Gefahren aufgrund unerwarteter mangelhafter interner Abläufe (z. B. mangelnde Sorgfalt von Mitarbeitern oder Fehlfunktionen von Systemen) oder unerwarteter externer Beeinträchtigungen der internen Abläufe (z. B. Hackerangriffe oder Naturkatastrophen)) kaum zu identifizieren und zu quantifizieren. Die „Messung“ und verständliche Darstellung der Risiken ist aber Voraussetzung für deren Steuerung, Minimierung oder Beseitigung.

Die Risikoidentifikation stellt die erste Stufe in einem Risikomanagement-System dar, ist Grundlage für den Risikomanagementprozess und damit bestimmend für dessen Effizienz.[2] Diese Phase soll alle auf das Unternehmen einwirkenden Risiken identifizieren, unabhängig davon, ob diese von der Unternehmung bereits kontrolliert bzw. beeinflusst werden können.

[1] vgl. Burkhard, Markus (2006), S.42
[2] vgl. Wolf, Klaus (2003b), S.6

Generell bietet sich dabei eine Erfassung entlang der Wertschöpfungskette an, die sämtliche auf einen betrieblichen Leistungsprozess einwirkenden Faktoren berücksichtigt.[1]

Startpunkt der Risikoidentifikation und damit der gesamten Risikoanalyse ist die eindeutige Definition des Analyseobjekts. Hierzu ist das zu betrachtende System bzw. Subsystem und in die Analyse einzubeziehenden Prozesse, Sub-Prozesse und Teilschritte festzulegen. Um Systemgrenzen sinnvoll und eindeutig zu definieren, muss zunächst die Struktur des Systems transparent gemacht werden. Neben der Zerlegung in Haupt- und Unterkomponenten oder einer hierarchischen Strukturierung entsprechend der Funktionalitäten können die Prozesse der Wertschöpfungskette durch die Unterteilung in Prozesse, Sub-Prozesse und Teilschritte strukturiert werden.[2] Die einzubeziehenden Prozesse, Sub-Prozesse und Teilschritte werden dabei drei unterschiedlichen Betrachtungsfeldern zugeordnet. In Anlehnung an die Unterscheidung zwischen Problem-, Wirkungs-, Eingriffs- und Lösungsbereich im Systems-Engineering können in der Risikoanalyse die drei Bereiche Ursachen-, Wirkungs- und Eingriffsbereich unterschieden werden. Dem Eingriffsbereich werden diejenigen Prozesse bzw. Schritte zugeordnet, in denen die Möglichkeit risikopolitischer Maßnahmen besteht.[3]

Für die Identifikation von Risiken gibt es unabhängig davon zwei prinzipielle Vorgehensweisen: Der Top-down-Ansatz geht von der Geschäftsstrategie, Standards und einem Überblick über das Gesamtgeschehen aus. Der Bottom-up-Ansatz geht vom täglichen Geschehen, der Quelle der Risiken aus und soll eine enge Beziehung zwischen Ereignissen, Personen, Prozessen und Technologie gewährleisten. Zumeist wird eine Art Gegenstromverfahren angewandt, das das von der strategischen Ebene vorgegebene Raster im operativen Bereich inhaltlich ausfüllen soll. Auf Basis des top-down Analyseverfahrens werden bottom-up Einzelrisiken erfasst, klassifiziert und selektiert. Gleichzeitig dienen die operative inhaltliche Ausgestaltung und die Selektion der Risiken der Entwicklung und Verbesserung der Analyseraster auf der strategischen Ebene. Diese Vorgehensweise benötigt somit die Vorgabe eines strategischen Rahmens.[4]

Die in der Praxis angewandten Methoden zur Risikoidentifikation können prinzipiell in Kollektions- (Checklisten, Self-Assessment, Risiko-Identifikations-Matrix, …) und Suchverfahren unterteilt werden. Suchverfahren (Morphologische Verfahren, Fehlermöglichkeits- und

[1] vgl. Reichling, Peter (2003), S.219
[2] vgl. Dahmen, Jörn (2002), S.55
[3] vgl. Dahmen, Jörn (2002), S.56
[4] vgl. Burger, Anton/Buchhart, Anton (2002), S.33

Einflussanalyse bzw. Ausfalleffektanalyse, Brainstorming, …) sind auf die Identifikation zukünftiger, bisher unbekannter Risikopotenziale (proaktives Risikomanagement) fokussiert.[1]

Das Entstehen einer Bedrohung bzw. eines Risikos kann mit Hilfe von Ursache-Wirkungsketten aufgezeigt werden, an dessen Ende ein Ereignis steht, das unmittelbar die Prozesse im Unternehmen schädigen oder stören kann. Die Erfassung von Risiken ist dabei auch auf die Zukunft gerichtet (potenzielle Risiken). Bei der Risikobewertung werden die identifizierten Risiken bezüglich ihres Gefährdungspotenzials bewertet.

Insbesondere bei einer großen Anzahl kreativ ermittelter Risiken sollten diese vor der Diskussion und Dokumentation strukturiert werden. Zu den bekanntesten Strukturierungsmöglichkeiten zählt das Ursache-Wirkungsdiagramm, aufgrund seiner grafischen Darstellung auch als Fischgräten-Diagramm bezeichnet. Einer, durch einen horizontalen Pfeil dargestellten Wirkung werden mögliche Ursachen an kleineren, auf den Hauptpfeil gerichteten Pfeilen zugeordnet. Diese Ursachen können wiederum durch weitere Verästelungen detailliert werden.[2] Die Strukturierung und Verzweigung wird aufgrund logischer Zusammenhänge zu erstellen versucht.

In diesem Zusammenhang ist die Anpassungsfunktion des Risiko-Controllings wichtig, welche Prämissen bei der Geschäftsprozess-bezogenen Risikoerfassung, -selektion und -bewertung, sowie Konzepte der Risikosteuerung an sich ändernde Gegebenheiten im Umfeld des Unternehmens anpassen soll.

Häufig wird die Schwachstellenanalyse dabei der Risikoanalyse zugerechnet. Die Bedrohungs- und Risikoanalyse eines Systems wird dann in vier Phasen unterteilt:[3]

In der ersten Phase wird das zu untersuchende System aus den Sichten der

- physikalischen Ebene (Hardware, Gebäude, Infrastruktur),
- logischen Ebene (Daten, Software, Protokolle),
- organisatorischen Ebene (Abteilungen, Personen, Rollen) und
- Ablaufebene (Kompetenzen, Funktionen, Arbeitsabläufe) modelliert.

Dabei wird das System in Objekte zerlegt, die über Beziehungen (ist enthalten in, ist verbunden mit, bearbeitet …) miteinander verbunden sind. Dies ist vergleichbar mit der Erhebung und Strukturierung der gesamten Informations- und Kommunikationstechnologie am

[1] vgl. Romeike, Frank (2004), S.174-178
[2] vgl. Dahmen, Jörn (2002), S.61
[3] vgl. Horster, Patrick (2002b), S.222-240

Anfang der Planungen zur Umsetzung des Grundschutzprozesses. In der zweiten Phase werden Sicherheitsanforderungen definiert, die die Systemobjekte (Rechner, LAN, Rollen …).einzeln, aber auch im Zusammenspiel der Systemobjekte erfüllt sein müssen. In der dritten Phase wird die Auswirkung der Bedrohungen auf das System untersucht. Basis hierfür ist ein Risikomodell, das beschreibt, welche Risiken durch die Bedrohungen entstehen und wie Sicherheitsmechanismen diesen Risiken entgegenwirken können. In der vierten Phase schließlich wird das System so modifiziert, dass alle Sicherheitsanforderungen erfüllt werden. Dies kann dadurch geschehen, dass die Struktur des Systems auf der logischen, organisatorischen oder der Ablaufebene angepasst wird (ohne zusätzliche physikalische Sicherheitsmechanismen zu installieren) oder, wenn das nicht reicht, zusätzliche physikalische Sicherheitsmechanismen in das System integriert werden.

Voraussetzung und Ausgangspunkt für einen effizienten Risikomanagementprozess ist eine möglichst vollständige Risikoidentifikation. Nach der Risikoidentifikation geht es bei der Risikobewertung darum, die erkannten Risiken zu quantifizieren oder zumindest qualitativ zu gewichten. Wird die Risikoanalyse nicht oder unzureichend durchgeführt, so könnte ein großer Anteil des Gesamtrisikos bei den nicht identifizierten Risiken versteckt sein, sodass auch der Nutzen der Risikosteuerung und -kontrolle von geringerem Wert ist.

Alle Erkenntnisse der Risikoanalyse (Risikoidentifikation und -bewertung) sollen entweder in ein Risikoinventar oder in ein sog. „RiskMap“ fließen, welches das „Gesamtrisiko des Unternehmens strukturiert“.[1] In komprimierter und übersichtlicher Form werden die Risiken eines Unternehmens abgebildet, um so den Entscheidungsträgern einen Überblick über die Risikolage des Unternehmens und insbesondere die wirtschaftliche Bedeutung zu geben. Die Aufstellung aller Risiken sollte Erkenntnisse über Risikoursachen, Informationen zur Bewertung der Risiken sowie für Entscheidungen über zu treffende Maßnahmen für eine zielgerichtete Risikobehandlung ermöglichen. Dazu wird in der Risiko-Map neben den Einzelrisiken häufig auch die individuelle Akzeptanz- bzw. Wesentlichkeitslinie abgebildet. Diese soll zeigen, ab wann Handlungsbedarf ausgelöst wird und die Erstellung einer Prioritätenliste ermöglichen. Risiken, die unter der Wesentlichkeitslinie liegen, kann mit beschränkten Mitteln begegnet werden. Gleichwohl sollen solche Risiken überwacht und regelmäßig neu bewertet werden.[2] Wichtig in diesem Zusammenhang ist das Ziel der betriebswirtschaftlichen optimalen Sicherheit.[3]

[1] Reichling, Peter (2003), S.218
[2] vgl. Reichling, Peter (2003), S.226
[3] vgl. Wieczorek, Martin (2003), S.18

Zu einem bewussten und gezielten Beheben von Schwachstellen kann man durch systematisches Erfassen und Bewerten von Verwundbarkeiten (vulnerability-management) kommen. Verwundbarkeiten sind die Türen, durch die Hacker, Viren und Würmer in Systeme und Netze eindringen. Verwundbarkeiten werden von Angreifern ausgenutzt, um ihre Ziele zu erreichen. Das Sammeln und Weiterverarbeiten von Informationen über Verwundbarkeiten ist dabei eine zentrale Anforderung an ein vorausschauendes Sicherheitsmanagement. Verwundbarkeiten entstehen durch schlechte Konfigurationen oder Fehler in Betriebssystemen, Netzwerkdiensten oder Applikationen. Um die eigene IT-Infrastruktur vor Angriffen zu schützen, werden z. B. Firewalls, Verschlüsselungs-, Content-Security-, Intrusion-/Prevention-Systeme eingesetzt. Dadurch kann aber höchstens das Ausnutzen der Verwundbarkeiten verhindert werden. Entfernt werden die Verwundbarkeiten nicht. Um die Bewertung vornehmen zu können, muss man die Verwundbarkeiten in ihrem Umfeld betrachten. Dabei sind die tatsächliche Infrastruktur, die Applikationen und Business-Prozesse zu berücksichtigen.[1]

Die obigen Ausführungen betreffen mehr das operative Risikomanagement. Bezüglich des strategischen Risikomanagements können in Anlehnung an das Konzept des strategischen Performance-Managements als Risiken für den IT-Security-Prozess die Prämissen- bzw. Selektionsrisiken der Planung (Irrtumsrisiken der Selektions- und Filterkriterien bei der Fokussierung auf die wichtigsten Prämissen der Security-Strategie) und zukünftige Security-Strategie-Umsetzungsgefahren analysiert werden.

Man kann interne und externe Planungsprämissen unterscheiden.[2] Diese können über miteinander verknüpfte beeinflussbare und nicht beeinflussbare Größen gebildet werden. Eine unbeeinflussbare Größe und damit externe Planungsprämisse betrifft z. B. die Marktentwicklung. Eine nicht beeinflussbare Größe ist z. B. auch die Entwicklung des rechtlichen Umfelds. Über rechtliche Risiken sind beeinflussbare Größen wie organisatorische, managementspezifische oder personelle Fragestellungen mit der Entwicklung des rechtlichen Umfelds verknüpft. Entsprechende Problemstellungen (z. B. Kompetenz, Know-how und potenzielles Verhalten des Personals) werden als interne Planungsprämissen bezeichnet.

Irrtumsrisiken der Selektions- und Filterkriterien bei der Fokussierung auf die wichtigsten Prämissen der Security-Strategie resultieren aus einer Fehleinschätzung, wie kritisch und

[1] vgl. Strobel, Stefan (2005)
[2] vgl. Eschenbach, Rolf (2003, S..97

sensitiv gewisse Sachwerte (vorhandenen Systeme, Netzwerke, Applikationen und Informationen) sind.

Security-Strategie-Umsetzungsgefahren bestehen potenziell bei mangelnder Flexibilität. Auch hier sind die beeinflussbaren Größen wie organisatorische, managementspezifische oder technische und personelle Fragestellungen von großer Bedeutung. Technische Fragestellungen betreffen die Beherrschbarkeit der für die Umsetzung relevanten Systeme.

5.1.2.2 Risikofrühwarnung, -früherkennung, -frühaufklärung

Im Vordergrund der Erfassung von Risiken steht deren Erkennung in einem möglichst frühen Stadium ihres Entstehens („Zukunft gerichtete Erkennung von Gefährdungspotenzialen“[1]). Identifiziert man Risiken so weit wie möglich vor ihrer Realisation, so schafft man dadurch einen – im Vergleich zur späteren Erkennung – größeren Handlungsspielraum zur Generierung von Handlungsalternativen.[2]

Diese Früherkennung kann z. B. auf Grundlage angenommener Kausalketten geschehen. Danach versucht man, potenzielle Risiken zu erkennen, welche Bedrohungen und Gefahren implizieren und mit ihrer Realisierung einen Schaden verursachen können.

Die Wahrnehmung von, als Frühindikator für Gefahren verstandene Risiken ist eng mit dem Bedürfnis verknüpft, für scheinbar unerklärliche Folgen, Ursachen ausfindig zu machen. Das Risiko wird bezüglich seiner Eintrittsmöglichkeit danach bewertet, mit welchem Grad an Sicherheit das singuläre Ereignis auf eine externe Ursache zurückgeführt werden kann.[3] Dies erfordert die Erfassung von Informationen über potenziell Risiko behaftete Entwicklungen im Umfeld des Unternehmens. Um rechtzeitig wichtige Informationen bezüglich Änderungen im Umfeld des Unternehmens zu erhalten, deren Wirkungen für die Weiterentwicklung des Unternehmens von großer Bedeutung sind, wurden in Theorie und Praxis Frühwarn-, Früherkennungs- und Frühaufklärungssysteme entwickelt. Diese sollen in Ergänzung bestehender Planungs- und Kontrollsysteme das Management mit den richtigen Informationen zum richtigen Zeitpunkt versorgen.[4]

Unter einem Frühwarnsystem wird ein Informationssystem verstanden, das einem Benutzer latente (verdeckt bereits vorhandene) Gefährdungen in Form von Reizen, Impulsen oder zeitlich vorlaufenden Informationen bereits vor deren Eintritt signalisiert. Als Grundlage gilt die Indikatorenhypothese, die besagt, dass Veränderungen nicht abrupt auftreten, sondern durch

[1] Wolf, Klaus (2003b), S.5
[2] Burger, Anton/Buchhart, Anton (2002):, S.67
[3] vgl. Hölscher, Reinhold (2002), S.83
[4] vgl. Gomez, Peter (2002), S.152

Signale angekündigt werden.[1] Ein Frühwarnsystem kann aber nicht nur latente Risiken frühzeitig erkennen, sondern auch Impulse zu deren Bewältigung (Steuerung) geben.[2] Im Gegensatz zur Frühwarnung zielt die Früherkennung auf die Erkennung latenter Bedrohungen/Risiken und Chancen ab. Die um den Chancenaspekt ergänzte informationelle Basis dient bei der Früherkennung als Grundlage einer Strategie- und Maßnahmenplanung. [ii] Im Fokus der sog. Frühaufklärung steht die Analyse des wirtschaftlichen, sozialen, politischen und technologischen Umfelds, und deren Einfluss auf die Erfolgspotenziale eines Unternehmens. Mit der Abkehr vom symptomatischen Vorgehen der operativen Frühwarnung und Früherkennung ist das Ziel verbunden, im Frühstadium strategischer Änderungen Handlungsbedarfe aufzuzeigen, um flexible Rektionsmöglichkeiten zu erzielen.[3]

Risikomanagement als systematisches Frühwarnsystem soll potenzielle Gefahren entdecken, bevor sie sich realisieren. Zu einem solchen Risikomanagement z. B. der IT-Infrastruktur wird ein permanenter Revisionsprozess vorgeschlagen, der aufgrund von Echtzeitdaten Soll-Ist-Überprüfungen vornimmt. Neben dieser automatisierten und permanenten Überwachung von Veränderungen im Netzwerk und ihre Validierung gegen Regeln sind realistische und ganzheitliche What-if-Analysen durchzuführen. Es ist szenarienbasiert darzustellen, wie sich eine bestimmte Änderung im Netzwerk auf alle anderen Datenflüsse und Performancegrößen wie Auslastungen und Antwortzeiten auswirkt. Um Risiken erst gar nicht entstehen zu lassen, konzentriert man sich also auf die Sicherstellung einer kontinuierlichen wie oben definierten Netzwerk-Integrität.[4] Man sieht in Veränderungen im Netzwerk also schon Anzeichen für mögliche Gefahren. Es ist zu untersuchen, welche Auswirkungen solche Veränderungen haben können, ob sie ein Risiko darstellen.

Moderne Frühwarnsysteme basieren auf neuronalen Netzwerken, deren Strukturen und Funktionen sich an den Nervenbahnen lebender Organismen orientieren. So sollen auch noch korrekte Ergebnisse geliefert werden können, wenn die für die Problemlösung notwendigen Informationen ungenau sind. Dies wird über die Lernfähigkeit und eine entsprechende Fehlertoleranz solcher neuronaler Strukturen ermöglicht.[5] Netzwerke sind anpassungsfähig und flexibel, Netzwerkstrukturen sind skalierbar und außerordentlich überlebensfähig. Im Prozess

[1] vgl. Romeike, Frank (2005), S.249
[2] vgl. Martin, Thomas A. (2002), S.118
[3] vgl. Wolf, Klaus (2003b), S.78,79
[4] vgl. Klapdor, Martin (2005)
[5] vgl. Romeike, Frank (2005), S.19

des Risikomanagements nehmen Sensoren Risiken auf und leiten sie an eine zentrale Stelle weiter.[1]

Als Frühwarninstrument kann dem Management auch richtig eingesetztes Benchmarking dienen: IT-Benchmarking unterstützt die langfristige Ausrichtung und Optimierung der IT-Strategie durch Vergleich von Kosten- und Leistungsstrukturen bezüglich der eigenen IT mit denen von Wettbewerbern. Neben den üblichen Preis- und Leistungsvergleichen mit Unternehmen vergleichbarer Größe, ähnlicher IT-Architektur, derselben Branche etc. können auch Mengenvergleiche auf Basis von Asset-Listen durchgeführt werden. Die Leistungsunterschiede werden durch Kennzahlen erfasst. Neben quantitativen Gründen für ein Benchmark gibt es auch qualitative Auslöser, z. B. Fragen hinsichtlich des richtigen Outsourcinggrades. Im Mittelpunkt stehen die SLAs (mit einem oder mehreren internen oder externen Dienstleistern vereinbarte Leistungsbeschreibungen). Regelmäßig genutzt offenbaren sich so frühzeitig Unstimmigkeiten in den Strukturen, die auf Optimierungspotenziale (sowohl der IT-Kosten und –Leistungen als auch der IT-Prozesse und –Strukturen) zur Verbesserung der Leistungsfähigkeit der IT hindeuten.[2]

In vielen Branchen wird zur Früherkennung von möglichen Fehlern in Prozessen und bei Produkten auch die Fehlermöglichkeits- und –einflussanalyse (FMEA) zur Qualitätssicherung sowie zur Prüfung der Anlagensicherheit im Umweltschutz im Rahmen von Sicherheitsanalysen nach der Störfall-Verordnung eingesetzt. Aber auch im Arbeitsschutzmanagement zur Vorbeugung von Unfällen wird die Verwendung dieser Methode vorgeschlagen. Eine derartige FMEA berücksichtigt neben dem Planungs-, Konstruktions- und Fertigungsprozess auch die Beziehungen zum gesamten geschäftlichen Umfeld.[3]

Wird zusätzlich noch der Prozessschritt der Risikosteuerung und Risikokontrolle (d. h. entsprechende Maßnahmen zur Realisierung der mit Risiken verbundenen Chancen bzw. der Abwehr/Minderung von Bedrohungen) berücksichtigt, so wird der Begriff Frühaufklärung verwendet.[4]

Sicherheit ist kein rein technisches Problem. Ohne begleitende organisatorische (z. B. Policies), betriebliche (z. B. Umsetzung von Technik in die Praxis des täglichen Betriebs) und

[1] vgl. Romeike, Frank (2004), S.147
[2] vgl. Seidl, Matthias (2006)
[3] vgl. Löbel, Jürgen (2005), S.91
[4] vgl. Romeike, Frank (2005), S.19

rechtliche (z. B. Datenschutz-) Maßnahmen kann keine umfassende Sicherheit erreicht werden.

Wenn es gelingen sollte, den Zustand IT-Sicherheit herzustellen, so kann dieser theoretisch nur durch ein dynamisches Nicht-Ereigniss verlassen werden. Um mit dynamischen Nicht-Ereignissen umzugehen und dafür zu sorgen, dass das Unerwartete nicht stattfindet, braucht man einen Fähigkeitsmix aus respektvoller Interaktion, Kommunikation, Vertrauen, direktem Wissen von der Technik, Aufmerksamkeit, Vertrautheit mit den gegenwärtigen Aufgaben und viel Erfahrung. Sicherheit wird durch ständigen Wandel erzeugt, Anpassungen an sich ständig ändernde Umfeldbedingungen halten sie aufrecht. Sicherheit in der betrieblichen Informationsverarbeitung ist ein kontinuierlicher Prozess, der ständig neuen internen und externen Entwicklungen und neu auftretenden Gefährdungspotenzialen angepasst werden muss. Sicherheit und Zuverlässigkeit bedürfen zu ihrer Aufrechterhaltung also kontinuierlicher Aufmerksamkeit und Anstrengung.[1] Zu dem, was diese Aufmerksamkeit und Anstrengung negativ beeinflussen könnte, gehören die Erwartungen, von denen sich die Menschen bei ihrer Arbeit leiten lassen: Erwartungen können zu „toten Winkeln“ in der Wahrnehmung führen: Man neigt dazu, nach bestätigenden Informationen zu suchen und alle Daten zu ignorieren, die nicht zu den Erwartungen passen.[2]

Zur steigenden Dynamik und Komplexität des Umfelds [3] tragen kürzere Produktlebenszyklen und sprunghafte Veränderungen in der Technologie bei. In einem solchen Umfeld wird die formale Planung und Kontrolle durch das größere Ausmaß möglicher zukünftiger Umweltzustände erschwert. Durch das Risikomanagement frühestmöglich identifizierte und beurteilte zukünftige risikobehaftete Entwicklungen müssen aber auch fortlaufend überwacht werden und, sobald ihr Eintritt gewisser wird, entsprechende Steuerungsprozesse auslösen, um die kontinuierliche Anpassung des Unternehmens an sich ständig verändernde Umfeldbedingungen sowie die Sicherung der unternehmerischen Existenz zu gewährleisten. Es müssen der Unternehmensführung Handlungsspielräume eröffnet werden, welche die langfristige Sicherung bestehender und den Aufbau neuer Erfolgspotenziale ermöglicht. Diese Zielsetzung ist kongruent mit derjenigen der Unternehmensführung, aber mit besonderer Fokussierung auf den Sicherheitsaspekt.[4]

[1] vgl. Weick, K. E. (2003), S.55
[2] vgl. Weick, K. E. (2003), S.43-54
[3] vgl. Horváth, Péter (2006), S.3
[4] vgl. Diederichs, Marc (2004), S.12,13

Handlungsspielräume in Abhängigkeit von möglichen Risiken zu unterstützen ist Aufgabe des strategisch-operativen Risiko-Controllings, welches auf einer adäquaten Risikoüberwachung, und Risikosteuerung basiert. Im IT-Bereich ist ein strategisches und ein operatives IT-Controlling bekannt. Durch Integration des klassischen IT-Security-Managements in das entwickelte Modell zum strategisch-operativen Risiko-Controlling entsteht ein so bezeichnetes strategisch-operatives IT-Security-Management. Der strategische Teil dieses strategisch-operativen IT-Security-Managements entspricht dem strategischen IT-Security-Controlling, und der operative Teil dieses strategisch-operativen IT-Security-Managements dem operativen IT-Security-Controlling.

5.1.2.3 Risikoüberwachung und Risikosteuerung

Das mit der laufenden Geschäftstätigkeit verbundene, sich ständig ändernde Risikopotenzial bedarf der ständigen Analyse und des Managements, um den Erfolg der Geschäftsprozesse und Geschäftsmodelle des Unternehmens nachhaltig zu sichern. Dazu dient vor allem die Risikokontrolle und -überwachung, die alle Risiken hinsichtlich ihres möglichen Eintritts und alle Risikomanagementmaßnahmen hinsichtlich ihrer Wirkungsweise untersuchen soll.

Will ein Unternehmen ein neues Geschäftsmodell (z. B. E-Business) einführen, so sind die Gefahren rechtlicher Gegebenheiten oder Risiken bei der Implementierung[1] zu überwachen und zu steuern. Es geht um die strategische und operative Absicherung, das Risikomanagement von neuen Geschäftsmöglichkeiten. Das entwickelte Modell zum strategisch-operativen Risiko-Controlling hat also neue Geschäftsmöglichkeiten (strategisch und operativ) abzusichern. Es sind die Risikofaktoren bei der Chancenwahrnehmung[2] zu analysieren. Dabei ist auch die Einhaltung sicherheitsrelevanter Aspekte zu gewährleisten.

Der Vorstand des Unternehmens, welcher die Risikostrategie festlegt, und für die Implementierung eines effektiven Risikomanagements verantwortlich ist, führen das Unternehmenscontrolling und/oder ein Risikomanager „das Risikomanagement als integralen Bestandteil des Planungs- und Controllingprozesses durch.“.[3]

[1] vgl. Kirchner, Michael (2002), S.91
[2] Kirchner, Michael (2002), S.93
[3] vgl. Hölscher, Reinhold (2002), S.95

Mit der Überwachung des gesamten Risikomanagement-Systems soll die „Wirksamkeit, Angemessenheit und Effizienz der ergriffenen Risikomanagementmaßnahmen einschließlich der entwickelten (Kontroll-)Strukturen überprüft werden.[1]

Abstrakt gesehen beschäftigt sich Risikomanagement mit Fragen nach der Risiko-orientierten Entwicklung und Fortführung von Strategien, Strukturen und Systemen. Im Kontext der Komplexität und des ständigen Wandels im Umfeld sind Strategien flexibel zu gestalten um sie sukzessive mit zunehmender Gewissheit über das Eintreffen vermuteter zukünftiger Entwicklung anzupassen.[2]

Allgemein können die Prinzipien des Managements des Unerwarteten,[3] d. h, wie ist zu verhindern, dass zunächst meist als unbedeutend erachtete unerwartete Ereignisse sich aufschaukeln und damit außer Kontrolle geraten, dafür einen konzeptionellen Ausgangspunkt bilden:

- Konzentration auf Fehler, alle Erfahrungen bei noch so kleinen Störungen sind zu analysieren, um daraus zu lernen; gründliche Auseinandersetzung mit Bedeutung und wirksamen Auflösungen von Diskrepanzen.
- Potenziellen Gefahren des Erfolgs, wie Selbstzufriedenheit, Nachlässigkeit bei den Sicherheitsstandards oder Abgleiten in Routine ist entgegenzuwirken; sowohl Misserfolge als auch Schwächen des Erfolgs sind als Anhaltspunkt für Vorsichtsmaßnahmen zu nutzen.
- Abneigung gegen vereinfachende Interpretationen: umfassendere und komplexere Wahrnehmungen, weniger endgültige Vorstellungen von Zusammenhängen, Vielfalt unterschiedlicher Perspektiven. Sensibilität für betriebliche Abläufe: Mängel in betrieblichen Abläufen (Lücken in den Abwehrmechanismen, Barrieren und Schutzvorrichtungen) aufdecken, allgemeinen Sicherheitszustand der Organisation regelmäßig überprüfen, ständige Aktualisierung der Definition von „Gefahr“, Verschweigen von Anzeichen für einen gestörten Betrieb verhindern.
- Streben nach Flexibilität: Fehler frühzeitig entdecken, sich von Irrtümern (die Teil einer ungewissen Welt sind) nicht lähmen lassen, sondern das System (wenn auch durch improvisierte Methoden) am Laufen halten, wahrgenommene Komplexität konstruktiv ohne starre Hierarchien nutzen und konstruktiv diskutieren, mehr Raum für Veränderungen.

[1] Hölscher, Reinhold (2002), S.1044
[2] vgl. Reichmann, Thomas (1993), S. 261
[3] vgl. Weick, K. E. (2003), S.10-36

Diese Prinzipien können im gesamten Risikomanagement-System, bestehend aus Risikofrüherkennungssystem und internem Überwachungssystem (welches wiederum aus Interner Revision, IKS und Risikocontrolling besteht), angewandt werden.

Dabei weisen Risikomanagementprozesse Pfadeigenschaften auf. Über welche Instrumente und Verfahren, über welches Wissen und welche Fähigkeiten die Systemakteure verfügen, hängt vom zurückliegenden Gang der Dinge ab, von damit verbundenen guten und schlechten Erfahrungen. [1] Ein durch Informationsschärfe justiertes Risikomanagement hält der Informationsunschärfe und Informationsdiffusion der Realität nicht Stand. Risikomanagement darf nicht nur als Baukasten zur Verbesserung von Reaktionsstrukturen verstanden werden, sondern muss auch Risiken, die mit dem Wahrscheinlichkeitskalkül nicht handhabbar sind, steuern können.[2] Risikomanagement muss so Nutzenpotenziale schaffen und die Nutzung der Ressource durchdenken[3] („Was ist machbar", „Was ist erforderlich"). Fragen wie „Was ist der Grund für Risiko", „Was ist Strategie bzw. Risiko, wenn der Gegner mitdenkt"[4] sollen so stets ihre situativ besten Antworten finden.

Das interne Überwachungssystem besteht aus Prozess-integrierten (organisatorischen Sicherungsmaßnahmen und Kontrollen) und Prozess-unabhängigen Überwachungsmaßnahmen, die vor allem von der Internen Revision durchgeführt werden.[5] Zum Aufgabenbereich des Kontrollsystems gehören neben dem Vergleich von Soll- mit Ist-Größen auch Prämissen- und Konsistenzkontrollen.[6] Die Elemente des internen Überwachungssystems sind wie die des Controllings einerseits eine Hilfsfunktion für die Risikofrüherkennung, besitzen aber auch eigene Aufgaben im Rahmen des Risikomanagement-Systems.

Betriebliche Probleme stehen bei allen Führungsfunktionen im Mittelpunkt. Controlling dient der Koordination innerhalb der betrieblichen Führungsfunktionen und zwischen ihnen. Es verbindet die Führungsteilfunktionen. Controlling ist damit eine Führungsfunktion, deren Aufgabe sich erst durch die Definition der anderen Führungsfunktionen erschließt. Zu den Teilfunktionen der Führung gehört die Festlegung allgemeiner Führungsprinzipien, die Zielbildung, die Planung und Kontrolle, die Organisation und Gestaltung der betrieblichen Informationssysteme. Letztere umfassen inhaltliche Aspekte (z. B. die Gestaltung des betrieb-

[1] vgl. Allenspach, Marco (2001), S.49
[2] vgl. Bieta, Volker (2004), S.0
[3] vgl. Bieta, Volker (2004), S.12
[4] vgl. Bieta, Volker (2004), S.11
[5] vgl. Schreiber, O.R. (2003), S.8
[6] vgl. Kimmig, Jens M. (2001), S.30

lichen Rechnungswesens) sowie informationstechnische Aspekte (z. B. den Aufbau von Datenbanken oder die Konfiguration von Rechnernetzen). Eine der typischen Teilaufgaben des Controllings ist es, mit geeigneten Messinstrumenten dem Management die Zielerreichung ihrer Handlungsalternativen aufzuzeigen.[1]

Das interne Überwachungssystem dient dem Erkennen von bereits aufgetretenen Risiken, die durch Missachtung von Gesetz und internen Vorgaben hervorgerufen worden sind und das Controlling der Identifizierung von Risiken in den Leistungsprozessen aufgrund aufgetretener Zielabweichungen.[2] Aufgabe des Controllings ist die Unterstützung der Unternehmensführung bei der zielgerichteten Planung und Steuerung, d. h. die ergebniszielorientierte Koordination von Planung, Kontrolle und Informationsversorgung. Zielorientierung bedeutet dabei eine Bündelung von Zielvereinbarung, Zielsteuerung und Zielerfüllung in einem sich selbst steuernden Regelkreis für eine langfristige Existenzsicherung des Unternehmens.[3] Die Phase der Risikosteuerung und -kontrolle zielt darauf ab, die Risikolage des Unternehmens positiv zu verändern. Dazu gehören Mechanismen und Maßnahmen zur Beeinflussung der Risikosituation. Ziele dieser Prozessphase sind die Vermeidung nicht akzeptabler Risiken sowie die Reduktion und der Transfer von nicht vermeidbaren Risiken auf ein akzeptables Niveau. Eine optimale Risikosteuerung und -kontrolle soll dabei auf die Steigerung des Unternehmenswertes ausgerichtet sein.[4]

Die Gesamtheit aller Aktivitäten zur Schaffung von Kosten-, Nutzen- und Risikotransparenz der IT, zur Erzielung einer nachhaltigen IT-Effizienz-/Produktivitätssteigerung bezogen auf die Unternehmensziele, wird als IT-Controlling bezeichnet. IT-Controlling ist aus dem Bedürfnis heraus entstanden, den „Erfolg“ des Einsatzes der Informations- und Kommunikationstechnik genauer zu überwachen, mit ihm finden „betriebswirtschaftliche Grundsätze Eingang in den IT-Bereich“. Dazu werden die betriebswirtschaftliche und die technische Welt konsequent zusammengeführt.[5] Das IT-Controlling plant, koordiniert und steuert die Informationstechnologie und ihre Aufgaben für die Optimierung der Geschäftsprozesse und der Aufbauorganisation (bezüglich Zielformulierung, -steuerung und -erreichung).[6] [7] Es vernetzt verschiedene Controlling-Sparten (Beschaffungs- und Logistikcontrolling, Fertigungscontrolling, Marketing- und Vertriebscontrolling), wenn der IT-Einsatz

[1] vgl. Trossmann, Ernst/Baumeister, Alexander/Werkmeister, Clemens (2003):, S.2-4
[2] vgl. Lentfer,Thies (2003), S.13
[3] vgl. Gadatsch, Andreas (2004), S.20,2 1
[4] vgl. Romeike, Frank (2004), S.235
[5] vgl. Tiemeyer, Ernst (2005), S.3,4
[6] vgl. Gadatsch, Andreas (2004), S.53
[7] vgl. Gadatsch, Andreas (2006), S.32

alle Bereiche des Unternehmens koordiniert.[1] Es umfasst Reporting und Bewertung des Einsatzes und Nutzens aller IT-Ressourcen und bezieht sich auf Anschaffung, Umsetzung und Betrieb im gesamten Lebenszyklus von Hard- und Software mit ihrer Zuordnung zu den Geschäftsprozessen des Unternehmens.

Unterschieden werden auch hier ein strategisches und ein operatives IT-Controlling. Das strategische IT-Controlling orientiert sich ohne Zeithorizont am Ziel der Effektivitätssteigerung (die richtigen Dinge tun). Als strategischer Baustein hat die IT die Erreichung der Unternehmensziele zu unterstützen. Ziel des operativen IT-Controllings ist die Effizienzsteigerung (die Dinge richtig tun) der vom strategischen IT-Controlling vorgegebenen Maßnahmen, innerhalb eines definierten Zeithorizonts, der konkreten Prozessunterstützung dienend.[2]

Strategisches Controlling stellt die „Synchronisierung der Unternehmensziele mit der Informationssystem-Strategie“ in den Mittelpunkt.[3] Das strategische IT-Controlling hat dazu den strategischen Führungsprozess zur Generierung, Umsetzung und Kontrolle der IT-Strategie mit Informationen zu versorgen und im Rahmen des strategischen Managements zu koordinieren. Entsprechend dieser Aufgabenbeschreibung werden die drei Teilbereiche „Unterstützung der IT-Strategieformulierung“, „Unterstützung der IT-Strategieumsetzung“ und „Strategische Kontrolle der IT-Strategie“ unterschieden. [4] : Bei der IT-Strategieformulierung geht es darum

- welche grundlegenden strategischen Optionen mit welcher IT-Unterstützung gewählt werden sollen
- wie die Effektivität (Wirtschaftlichkeit) der einzusetzenden Informationstechnologie zu bewerten ist
- Teilstrategien aus der gewählten IT-Gesamtstrategie abzuleiten.

Bei der Unterstützung der IT-Strategieumsetzung ist

- die IT-Strategie in konkrete Steuerungsgrößen zu transformieren.

Die strategische Kontrolle der IT-Strategie ist

- die laufende Überprüfung der Strategieprämissen und
- die Überprüfung des Strategierealisierungsgrades

[1] vgl. Gadatsch, Andreas (2004), S.54
[2] vgl. Gadatsch, Andreas (2006), S.39,40
[3] vgl. Tiemeyer, Ernst (2005), S.4
[4] vgl. Bursch, Daniel (2005), S.87-93

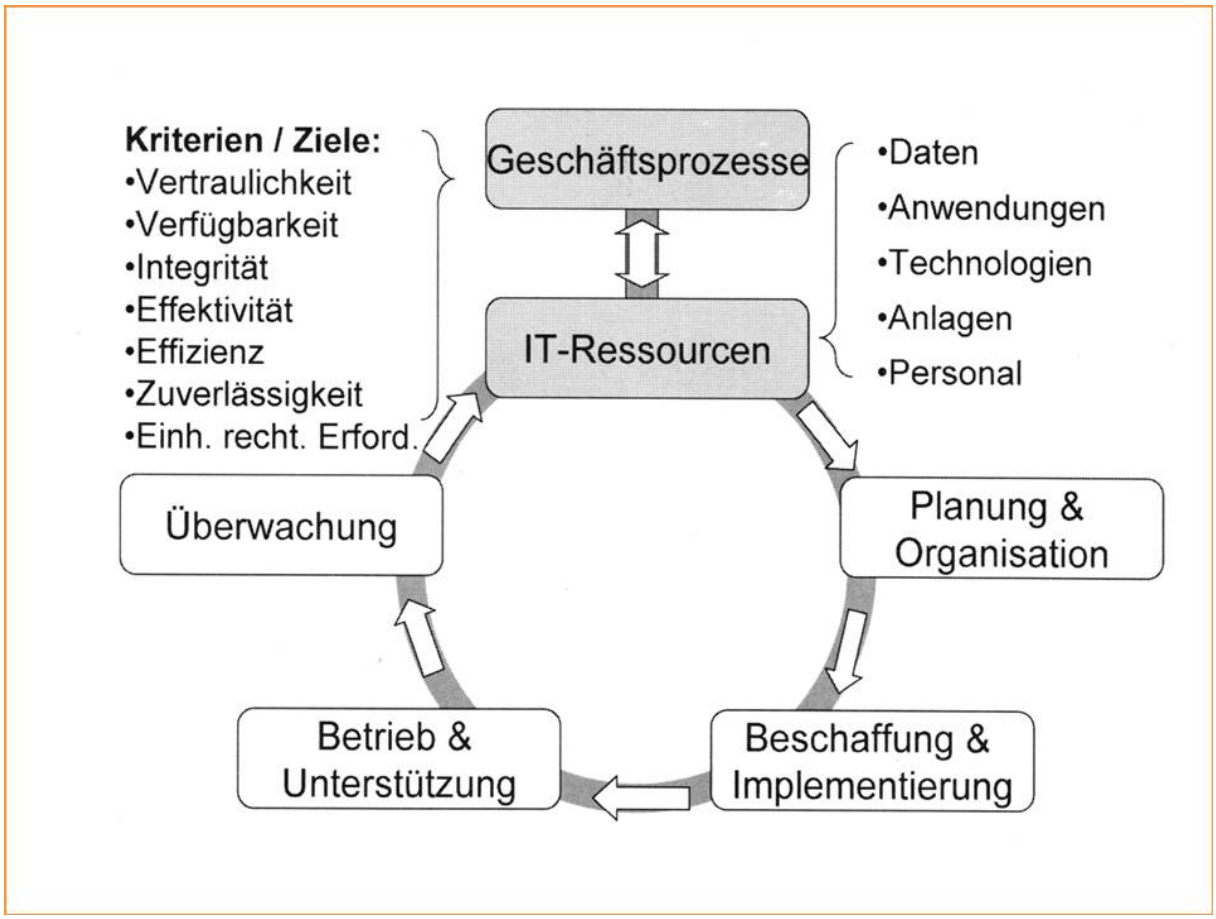
Das operative IT Controlling beschäftigt sich vor allem mit dem reibungslosen IT-Betrieb und der Weiterentwicklung und Wartung von Informationssystemen. Kernthemen und Zielorientierung sind „Steuerung von Produktivität und Kostensituation bei kurzfristigen Zielsetzungen“. Die Zielsteuerung koordiniert Controlling- dabei mit IT-Effizienzsteigerungs-Konzepten. Ausgehend von Kosten- und Leistungsdaten erfolgt die effiziente Steuerung der betrieblichen Prozesse.[1] Grundlage einer effizienten Steuerungsmethodik und -organisation ist das IT-Asset-Management (Verwaltung aller IT-Vermögensgegenstände des Unternehmens). Das IT-Asset-Management übernimmt die Inventarisierung und Verwaltung aller IT-Ressourcen im Unternehmen[2] (IT-Bestandsmanagement als Schlüssel für mehr Sicherheit, Komfort, Flexibilität, Erfolgsbeiträge durch Kosteneinsparung aber auch Ertrags- und Leistungswerte mit Blick auf mögliche IT-Risiken). Mit einem fundierten Bestandsmanagement sind Unternehmen in der Lage, die meist vorherrschende Heterogenität der Geräte, Betriebssysteme und der eingesetzten Software zu kontrollieren und zu steuern. Dies ist Voraussetzung für höhere Produktivität, Servicelevels und Sicherheit der Betriebsprozesse.[3] In Bezug auf ITIL bietet sich eine Kombination von IT-Asset-Management im Rahmen des IT-Service-Managements und BPM-Systemen an. BPM-Systeme ermöglichen den Transfer des über die eigenen Abläufe entstandenen Wissens in elektronische Prozesse. BPM-Systeme machen dieses Wissen zentral zur Auswertung verfügbar und zur Optimierung nutzbar.[4]

Um seine angestrebten Geschäftsziele erreichen zu können, sollte ein Unternehmen seine Geschäftsprozesse optimieren. Eine zentrale Aufgabe dabei ist, bestimmte Anforderungen an die in den Geschäftsprozessen verarbeiteten Informationen zu stellen. Eine Anleitung dazu stellt der Standard CObIT (Control Objectives for Information and Related Technology) bereit. Es handelt sich um eine Methode zur Entwicklung eines Kontrollumfelds zur Begrenzung von IT-Risiken. Die Einhaltung dieser Anforderungen soll sicherstellen, dass die eingesetzte Informationstechnologie die Geschäftsziele abdeckt, die Ressourcen verantwortungsvoll eingesetzt werden und die Risiken angemessen überwacht werden. Dazu definiert CObIT für jeden IT-Prozess sowohl die Geschäftsziele, die durch diesen Prozess unterstützt werden sollen, als auch die Kontrollziele für diesen. Er empfiehlt bei der optimalen Ausrichtung der IT auf die Unternehmensziele sowie dem Umgang mit IT-Risiken Kontrollziele in den Kategorien Qualität (Effektivität, Effizienz), Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit)

[1] vgl. Tiemeyer, Ernst (2005), S.3,4,5
[2] vgl. Gadatsch, Andreas (2004), S.60
[3] vgl. Krüger, Torsten/Graf, Richard (2005), S.39
[4] vgl. Besemann, Martin (2005), S.33

und Ordnungsmäßigkeit (Einhaltung rechtlicher Erfordernisse (Compliance), Zuverlässigkeit). Als IT-Ressourcen definiert CObIT Daten, Anwendungen, Technologien, Anlagen und Personal.

Das Framework besteht aus 4 sog. „Domains“ (Planung & Organisation, Beschaffung & Implementierung, Betrieb & Unterstützung, Überwachung), denen kritische IT-Prozesse und Aktivitäten zugeordnet sind.[1]



(Quelle: Heisel, Frank (2005), S.20)

Abb. 17 Das CObIT-Framework

CObIT eignet sich insbesondere zur Umsetzung der IT Governance, d. h. die optimale Unterordnung und den Einsatz der IT zur Unterstützung der Geschäftsanforderungen. Die Kriterien von CObIT werden von Wirtschaftsprüfern im Rahmen der Jahresabschlussprüfung eingesetzt. Aufgrund der Prozess- und Kontroll-orientierten Sichtweise kommt CObIT bei vielen Sarbanes-Oxley-Act-Projekten zum Einsatz. Spezielle Werkzeuge wie die IT Infrastructure Library, ISO 17799, GSHB (Grundschutzhandbuch) können auf ihrem Spezialgebiet weiter in die Tiefe gehen. Eine mögliche Vorgehensweise wäre daher im Rahmen eines umfassenden Assessments (z. B. im Bereich IT-Security), mittels CObIT breitflächig eine Schwachstellen-

[1] vgl. Heisel, Frank (2005), S.20

analyse zu beginnen und bei „Problemzonen“ unterstützend weitere Werkzeuge heranzuziehen. Die Unterstützung der Geschäftsprozesse geschieht durch die IT-Ressourcen Daten, Anwendungssysteme, Technologie, Anlagen, Personal. Die Optimierung der Geschäftsprozesse soll über ein geeignetes Management dieser Ressourcen erfolgen.[1]

Zielgruppen von CObIT sind[2] neben Nutzern (zur besseren Abschätzung der Zuverlässigkeit und Kontrolle von intern oder extern erbrachten Dienstleistungen), IT-Verantwortlichen (zur Unterstützung bei ihrer Arbeit), dem Management (zur Unterstützung beim Abwägen zwischen Risiken und den Investitionen für Kontrollmaßnahmen) auch Prüfer (zur sachlichen Begründung von Prüfungsaussagen und bei der Beratung im Rahmen des Aufbaus und des Betriebs internen Kontrollen). CObIT wird von vielen Wirtschaftsprüfungsorganisationen und Beratungsunternehmen eingesetzt und im Rahmen der Jahresabschlussprüfung zur Prüfung der IT-Systemumgebung verwendet.

Zur unternehmensweiten Steuerung IT-basierter Geschäftsprozesse mittels einer homogenen Lösung dient das Enterprise Job Scheduling (EJS). Alle Anwendungen werden so, unabhängig von der IT-Infrastruktur, proprietären Schnittstellen, unterschiedlichen Datenmodellen und Softwarearchitekturen effizient gesteuert und überwacht. Unternehmensweite, abteilungsübergreifende Prozesse können ohne aufwendige Integrationsprojekte abgebildet werden. Dies setzt eine vollständige Unterstützung durch die IT-Infrastruktur z. B. bezüglich Skalierbarkeit, Hochverfügbarkeit, Nachvollziehbarkeit (u. a. eine Anforderung des Sarbanes-Oxley-Act)) voraus. EJS muss sich zudem dynamisch an wechselnde Systemumgebungen anpassen können. Die zentrale, nachvollziehbare Steuerung soll für den zuverlässigen Ablauf aller IT-basierten Geschäftsprozesse sorgen, und über auftretende Fehler unmittelbar informieren. Mittels Laufzeitkontrolle und automatischer Jobreport-Analyse sollen auch logische Fehler sofort erkannt werden.

Wenn die Geschäftsprozesse einer Organisation auf einer gut funktionierenden Informationsversorgung basieren, wird die Organisation zunehmend von den IT-Dienstleistungen abhängig, um ihre Geschäftsziele zu erreichen. Als Plattform für die verschiedenen IT-Controlling-Konzepte und -Tools hat sich zur Strukturierung aller IT-Betriebsprozesse als Best-Practise-Ansatz das ITIL-Prozessmodell etabliert. Es handelt sich um ein Referenzmodell zur Ausgestaltung, Implementierung und Management von IT-Service-Prozessen. Es

[1] vgl. Wallmüller, Ernest (2004), S.45,46
[2] vgl. Schröder, Georg F. (2006), S.95,96

schafft die Grundlage für Qualitätsmanagement in der IT mit Prozess- und Service-orientierung.[1] Es dokumentiert die für den Betrieb von IT-Systemen durch einen internen oder externen Dienstleister erforderlichen standardisierten und nachvollziehbaren Abläufe. Es dient als Rahmenwerk und Orientierungshilfe zur Ausgestaltung eigener IT-Prozesse und skizziert somit die Schnittstelle zum gesamten IT-Betrieb. Das Regelwerk ist ein Leitfaden der Inhalte, Prozesse und Ziele innerhalb der IT-Organisation beschreibt. Die konkrete Umsetzung und Ausgestaltung der Prozesse liegt im Ermessensspielraum jeder IT-Organisation selbst. Die individuellen Ausprägungen einer IT-Organisation lassen sich entlang des Leitfadens entwickeln und mit konkreten Inhalten füllen.[2] Es wird beschrieben, welche Aspekte bei der IT-Prozessoptimierung zu beachten und individuell durch den Dienstanbieter anzupassen sind.[3]

ITIL macht Vorgaben für den gesteuerten Betrieb der IT-Infrastruktur.

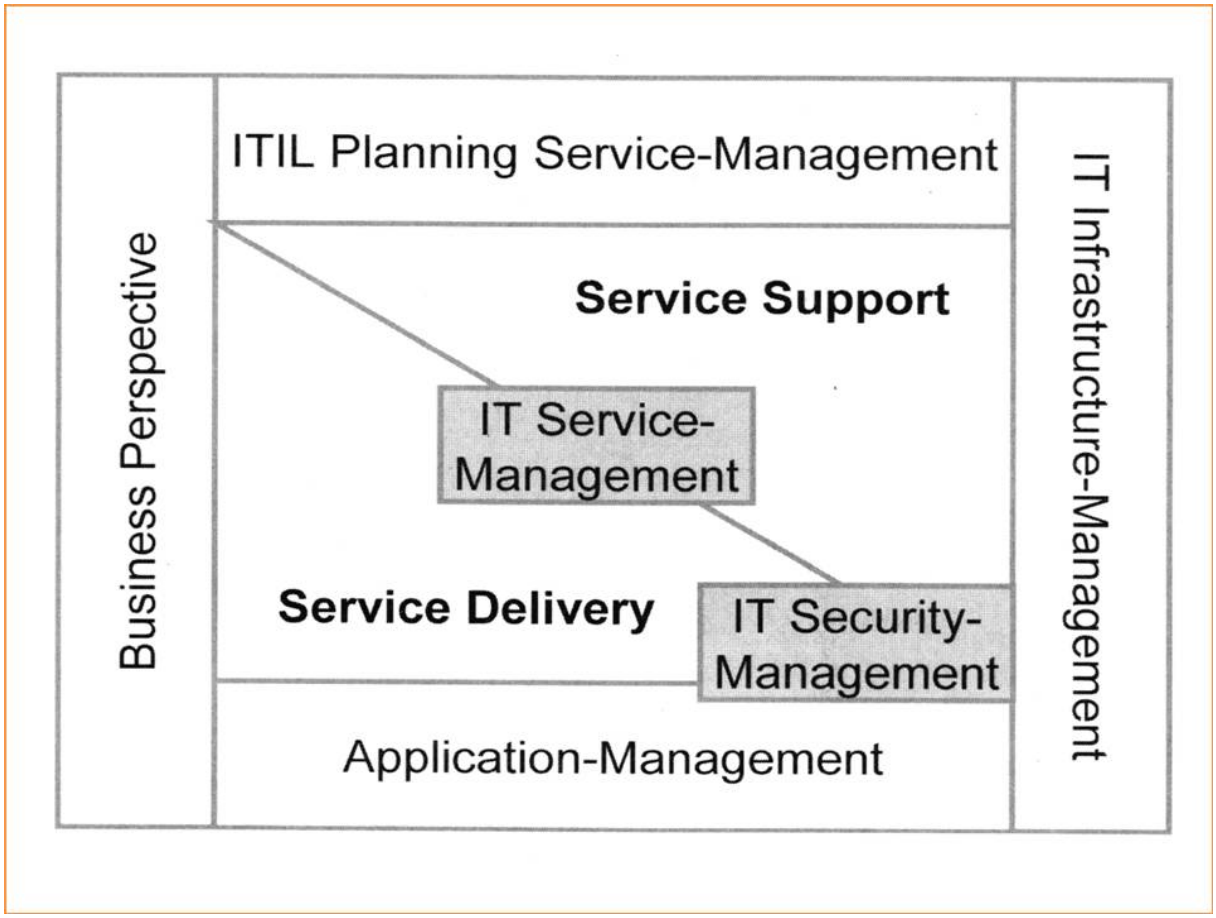
Grundsätzlich unterscheidet man zwischen aktiven und passiven Maßnahmen zur Risikosteuerung. Aktive Maßnahmen (ursachenbezogene Maßnahmen) gestalten und beeinflussen die Risikostrukturen und -verhältnisse. Passive Maßnahmen (wirkungsbezogene Maßnahmen) reduzieren nur die (finanziellen) Auswirkungen auf das Unternehmen nach einem möglichen Risikoeintritt, etwa durch Haftungsverlagerung oder Risikotransfer.[4] Der Risikoträger versucht, durch geeignete Maßnahmen Risikovorsorge zu betreiben mit dem Ziel, die Auswirkungen des Risikoeintritts zu vermeiden oder zu vermindern. Das klassische Mittel zur finanziellen Vorsorge für bereits vorhandene oder zukünftig drohende Schäden sind Rücklagenbildungen, z. B. in Form von Rückstellungen gemäß § 249 HGB. Eine besondere und innovative Form der Reservenbildung ist das Funding. Die Reserven werden extern gebildet, während das Unternehmen eine Risikoprämie als Aufwand absetzen kann.[5]

Wo es um Risikosteuerung geht, ist im Zusammenhang mit der Thematik dieser Arbeit eine aktive Steuerung gefragt. Gleichzeitig wird das Ziel verfolgt, die Auswirkungen des Risikoeintritts zu vermeiden oder zu vermindern.

In ITIL werden die Abhängigkeiten aller Einzelaktivitäten sowie die Abstimmungstätigkeiten in den übergeordneten Zusammenhang eines einheitlichen Prozessmodells gesetzt. ITIL bildet so eine Orientierungs- und Strukturierungshilfe zum Aufbau und zur Verwaltung komplexer IT-Infrastrukturen. ITIL betrachtet die IT intern und extern gleichermaßen als Dienstleistung

[1] vgl. Bernhard, Martin G. (2005, S.96
[2] vgl. Elsässer, Wolfgang (2005), S.9
[3] vgl. Gadatsch, Andreas (2006), S.276-82
[4] vgl. Romeike, Frank (2004), S.160
[5] vgl. Romeike, Frank (2004), S.240,241

mit dem Ziel, die IT-Organisation Service-, Prozess- und Kunden orientiert auszurichten. Damit rückt eine dienstleistungs- und Geschäftsprozess-orientierte Sichtweise in den Vordergrund. Kunden und Anwender erwarten eine zuverlässige und permanent zur Verfügung stehende Informationstechnologie. Deshalb müssen alle angebotenen Services durchgängig über alle Systeme hinweg überwacht werden.[1]



(Quelle: Heisel, Frank (2005),S.19)

Abb. 18 Grundkomponenten von ITIL

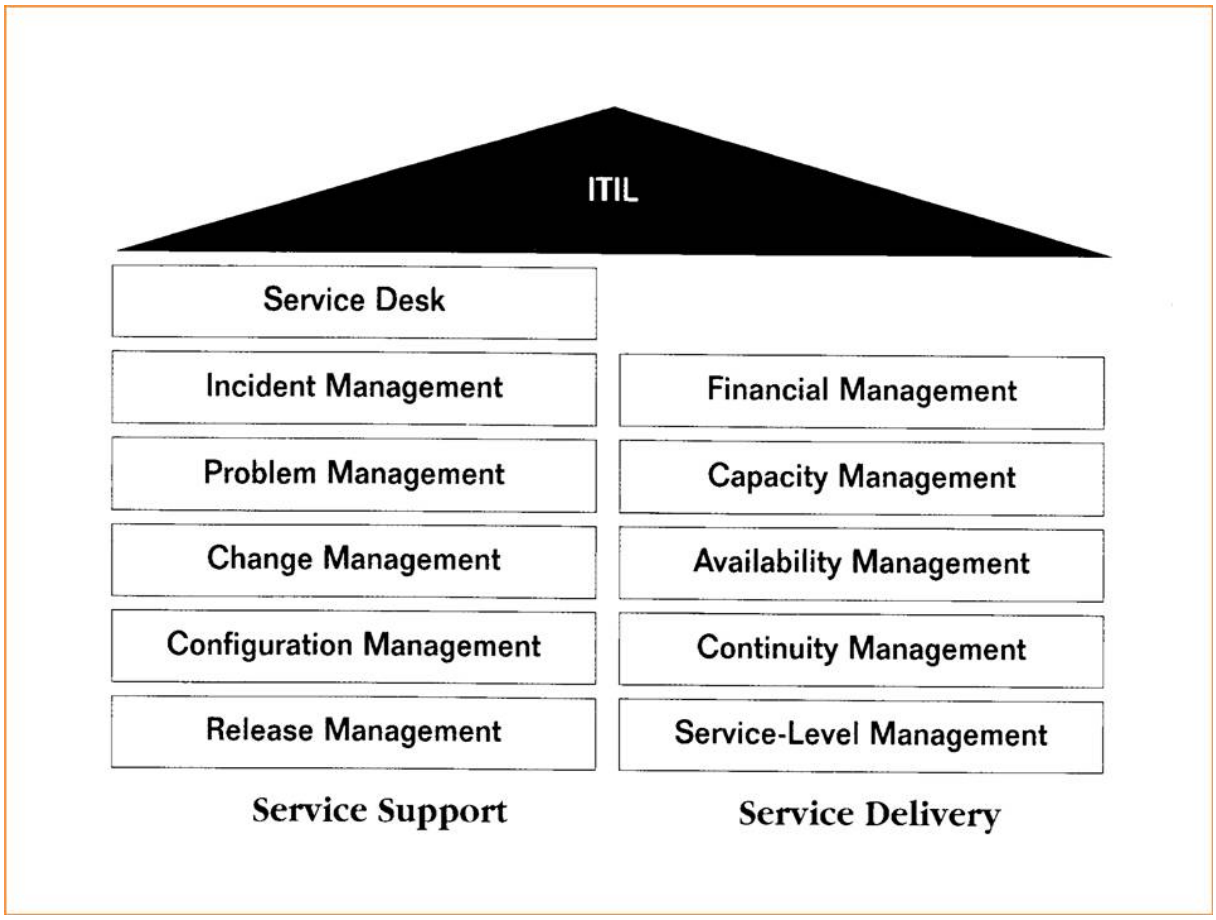
ITIL besteht aus 5 Grundkomponenten/Sichten des IT-Managements/Planungsebenen: der Geschäftssicht (Business Perspective), der Servicemanagement-Planung, dem IT-Service-Management, dem Applikationsmanagement sowie dem Infrastrukturmanagement. Die Business Perspective behandelt strategische Aspekte der IT-Services, z. B. die Sicherstellung der Dienstleistungen in diversen Ausnahme- und Notsituationen. Servicemanagement-Planung enthält z. B. Konzepte zur Bestimmung des Status quo der IT-Landschaft (Istaufnahme), Zieldefinitionen und Meilensteine für das ITIL-Projekt. Das Applikationsmanagement befasst sich mit dem gesamten Lebenszyklus von Anwendungen und Dienstleistungen sowie z. B. der Sicherheit von Software und der Stabilität von Anwendungs-

[1] vgl. Elsässer, Wolfgang (2005), S.16

systemen für die Endnutzer. Das Infrastrukturmanagement hat Planung, Aufbau und Organisation der gesamten IT-Infrastruktur zum Inhalt.[1] Dabei wird nicht die konkrete Umsetzung beschrieben, sondern der Rahmen, die Anforderungen und die gewünschten Ergebnisse definiert. Die Ausformulierung der operativen IT-Serviceprozesse muss in Abstimmung mit den branchen- und unternehmensspezifischen Prozessen erfolgen.[2]

Das Prozessmodell bildet auch die Basis, Verbindungen zwischen den Sicherheitsanforderungen der Geschäftsprozesse mit denen der IT-Prozesse zu erkennen. Eine Restrukturierung der IT-Prozesse soll den Bereich der Informationssicherheit stärker in den der IT-Prozesse integrieren.

IT-Service-Management soll die störungsfreie Ausführung der implementierten Dienste im laufenden Betrieb observieren und im Störungsfall adäquate Maßnahmen bereitstellen bzw. (z. B. durch Load Balancing) automatisiert ausführen.[3]



(Quelle: Kob, Timo/Schumann, Detlef (2005), S.32)

Abb. 19 Bestandteile ITIL

[1] vgl. Elsässer, Wolfgang (2005, S.40,41
[2] vgl. Heisel, Frank (2005), S.19
[3] vgl. Bieberstein, Norbert (2006), S.24

Das IT-Service-Management wird in elf Bestandteile gegliedert (die als Disziplinen eingeführt und in die IT-Organisation übernommen werden sollen), die in die Bereiche Service Support (Unterstützung) und Service Delivery (Bereitstellung) aufgeteilt sind:[1]

Das Service-Support-Set beinhaltet die Prozesse für den Support der IT-Umgebung. Diese Prozesse betreffen den operationalen Teil der IT-Aufgaben und den praktischen Betrieb:

Das Release-Management betrachtet alle Aspekte umfangreicher oder kritischer Hard- und Softwareeinführungen. Das Configuration-Managment zeigt das logische Abbild aller IT-Komponenten und ihrer Beziehungen auf, beschäftigt sich mit der Konfiguration, Wartung, Entwicklung und Probleminformation aller Komponenten.[2]

Innerhalb einer an ITIL orientierten Service-Organisation hat das Configuration-Managment die Aufgabe, die frist- und anforderungsgerechte Erfüllung der Service-Anforderungen der Kunden zu gewährleisten und eine effiziente Steuerung der IT-Ressourcen sicherzustellen. Dies soll durch geeignete Planungs- und Überwachungsmethoden garantiert werden. Alle Anwendungen eines Servers müssen miteinander verträglich sein, auf gleichen Betriebssystemen oder Midlelware-Versionen aufsetzen, und so voneinander isoliert sein, dass die Sicherheit und Vertraulichkeit der Daten immer gewährleistet ist. Insbesondere rückt auch der Faktor Wirtschaftlichkeit immer mehr in den Fokus wettbewerbsorientierter IT-Dienstleister. Zur Optimierung der Server-Kapazitäten wird für Programme und Dienste eine virtuelle Ausführungsumgebung geschaffen, die von der physikalischen Umgebung (dem Rechner mit allen Hardware-Schnittstellen) entkoppelt ist. In diesem Sinne stellt z. B. die Java Virtual Maschine eine sog. Virtualisierungsschicht dar, die innerhalb einer Betriebssystemumgebung liegt. Der einzelne Server ist nicht mehr Planungsobjekt, betrachtet, beplant und verwaltet nur noch einen übergeordneten Ressourcenpool.[3]

Eine zentrale Ausprägung des Configuration Managements gemäß ITIL ist die CMDB (Configuration Management Database). Sie bildet Prozesse, Services, Rollen und die eigentlichen Configuration Items (Hardware, Software und andere Elemente der IT-Infrastruktur) ab. Ergänzt man dieses Beziehungsnetz um die Anforderungen der IT-Sicherheit, hat man ein universelles Werkzeug auch für das Securitymanagement. Die Nutzung der CMDB bietet aber auch die Möglichkeit einer Tool-gestützten Notfallplanung und bringt Vorteile für den IT-Betrieb.[4]

[1] vgl. Kob, Timo/Schumann, Detlef (2005)
[2] vgl. Elsässer, Wolfgang (2005), S.31-33
[3] vgl. Wulff, Joachim (2006)
[4] vgl. Kob, Timo/Schumann, Detlef (2005):, S.33

Change Management ist die Entwicklung und Umsetzung geeigneter Strategien, um das Unternehmen den zu erwartenden Veränderungen im Unternehmensumfeld anzupassen. Das Problem Management dient der präventiven Vermeidung von Störungen. Das Incident Management beschäftigt sich mit dem Umgang mit kritischen Ereignissen. In Bezug auf Sicherheitsereignisse (Security Incidents) ist genau festzulegen, wie auf bestimmte Ereignisse reagiert werden soll. Um z. B. Intrusion Detection-Systeme erfolgreich einzusetzen, ist die rein technologische Betrachtungsweise bei weitem nicht ausreichend. In Abhängigkeit von Quelle, Ziel und Art des Angriffs sind angemessene Reaktionen festzulegen.[1]

Das Service Delivery Set beinhaltet Prozesse zur strategischen Unterstützung des IT-Managements. Der Prozess zur Erfolgsmessung des sich auf die Informationssicherheit konzentrierenden Securitymanagements nach ITIL, anhand der Service-Level-Kennzahlen, ist das Service-Level-Management. Es betrifft die Verhandlungsprozesse zwischen IT-Organisation und Fachabteilungen. Das Continuity Management trifft Maßnahmen, um bei Ausnahmesituationen die IT-Leistungen schnellstmöglich wiederherzustellen. Das Availability Management soll die permanente Leistungsfähigkeit der IT-Infrastruktur und die Verfügbarkeit von Diensten und IT-Ressourcen gewährleisten. Hierzu gehört auch die Definition von Sicherheitskonzepten (Security Policies). Das Capacity Management betrifft die Kapazitätsplanung für derzeitige und zukünftige Ressourcen-Erfordernisse und die wirtschaftliche Bereitstellung der IT-Infrastruktur. Das Financial Management (Cost Management) stellt eine Kosten/Nutzen-Rechnung für IT-Komponenten und Ressourcen bzgl. Anschaffung und laufendem Betrieb auf und stellt eine verursachungsgerechte Abrechnung der erbrachten Leistungen und entstandenen Kosten sicher.[2]

Neben diesen zehn Management-Disziplinen des IT-Service-Managements (ITSM) gibt es noch die vom ITSM weitgehend unabhängige Prozessgruppe des Operations-Managements bzw. IT-Infrastructure-Managements, das den Betrieb und die Abwicklung der IT-Aufgaben betrifft. Dazu gehören die Bereitstellung aller notwendigen Verfahren, allgemeine Administrationsaufgaben, das Monitoring und die Netzwerkanalyse.[3]

Im Zusammenhang mit Qualitätskonzepten und Qualitätssicherung bietet ITIL Unterstützung, um die notwendigen Qualitätsprozesse zu realisieren und zu implementieren. ITIL ist kein

[1] vgl. Horster, Patrick (2002b), S.282-292
[2] vgl. Elsässer, Wolfgang (2005), S.31-33
[3] vgl. Elsässer, Wolfgang (2005), S.31,33

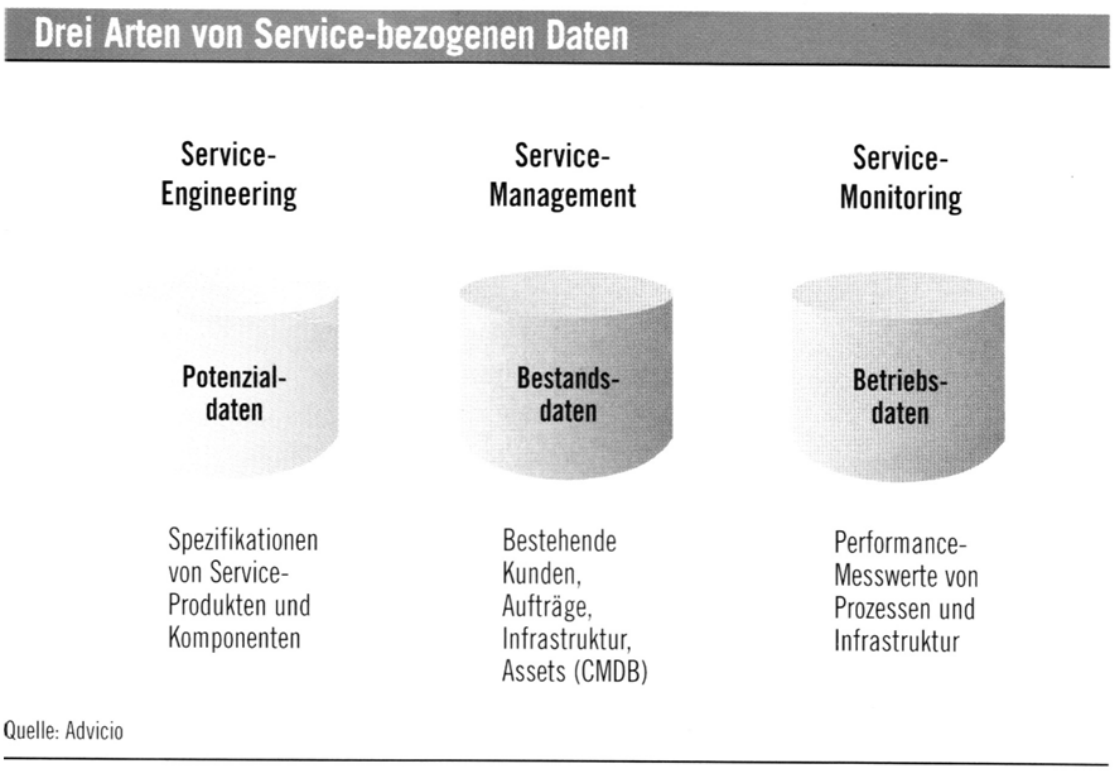
Ersatz für bewährte Normen wie ISO 9000. Das Rahmenwerk bietet aber abgestimmte Prozesse, welche die Qualitätssicherungsaspekte der gesamten IT unterstützen können.[1]

Im Rahmen des IT-Managements muss die Vielzahl zusammenhängender Informationen verwaltet werden, die in unterschiedlichen Prozessen gewonnen werden.[2] ITIL hat sich als Standard zum Management der gesamten Unternehmens-IT entwickelt.[3] ITIL ist ein gemeinsamer Rahmen für sämtliche Aktivitäten der IT-Organisation im Zusammenhang mit Prozessen zur Erbringung von IT-Services unabhängig von deren konkretem organisatorischen Aufbau: Er ist eine Sammlung von Best Practices um schneller auf veränderte Anforderungen an den IT-Betrieb reagieren zu können (Integration der Geschäftsanforderungen der internen oder externen Kunden, bestehende Prozesse optimieren und besser aufeinander abstimmen)[4] :Ziel von ITIL ist es, die im Unternehmen vorhandenen Strukturen für Service und Support zu optimieren sowie die erbrachten Leistungen zu messen und darzustellen. Es soll eine Grundlage für das Servicemanagement der IT geliefert werden. Ein effektives und effizientes Servicemanagement ist dabei ohne eine adäquate IT-Sicherheit nicht möglich.[5]

Durch Verwendung von ITIL-Komponenten ist es möglich, eine Anzahl von Maßzahlen zur Überwachung und Messung des Servicemanagements zu entwickeln. Zwecks Umsetzung von ITIL zur Kontrolle und Steuerung der Prozesse in einer IT-Service-Management(ITSM)-Umgebung wird als Ausgangspunkt eine zentrale Configuration Management Database (CMDB) vorgeschlagen, in der alle IT-Ressourcen und deren Beziehungen zueinander hinterlegt sind. Beziehungen der Hardware- und Software-Ressourcen in der IT-Infrastruktur zueinander und zu Informationen aus den administrativen Prozessen (etwa Störungsmeldungen) werden ebenfalls in der CMDB hinterlegt. Aus dieser Datenbasis beziehen alle Prozesse Informationen zur Unterstützung ihrer Funktionen.[6]

Bestandsdaten werden in CMDB- oder Asset-Management-Sytemen, und Bewegungsdaten in Performance Management-, Fault Management- und Trouble-Ticket-Systemen verwaltet und gepflegt.

[1] vgl. Elsässer, Wolfgang (2005, S.12
[2] vgl. Gerick, Thomas (2004)
[3] vgl. Ludwig, Bernd (2004)
[4] vgl. Dollinger Bernd F./ Schmidt Rainer (2004)
[5] vgl. Vossbein, Reinhard (2005a)
[6] vgl. Santifaller, Michael (2005)



(Quelle: Grawe, Tonio (2005a), S.23)

Abb. 20 Arten von Service-bezogenen Daten

Als Ansatz für ein Securitymanagement auf Unternehmensebene von zentraler Stelle aus wird eine Kombination von Funktionen zur Device Security und Systemmanagementlösungen vorgeschlagen.[1] Clients müssen auf Richtlinien-Konformität/Einhaltung einer vorgegebenen Sollkonfiguration überprüft werden, bevor sie ans Netz gehen. In der Sicherheitsrichtlinie wird auch festgelegt, welche Anwendungen auf dem Gerät laufen dürfen.

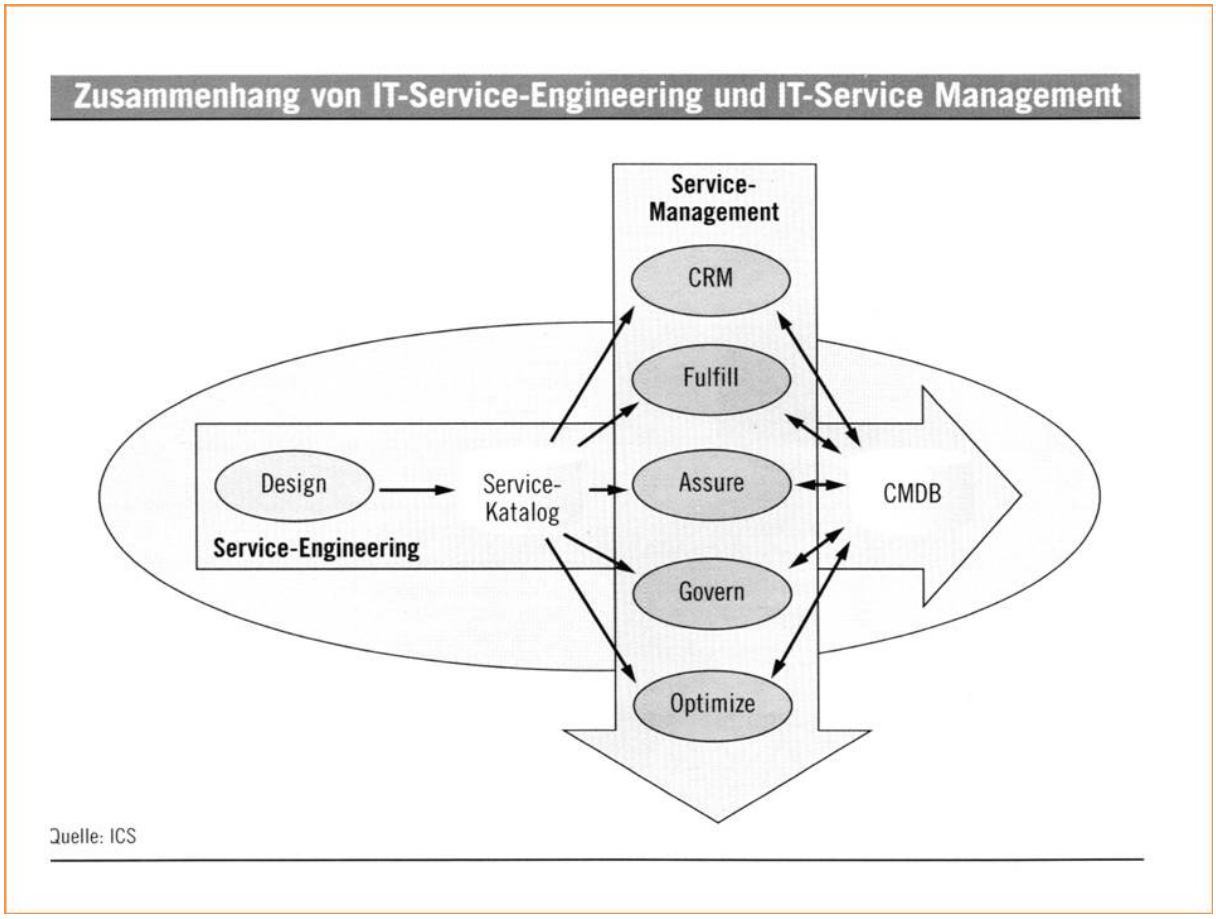
Dieser Ansatz könnte ebenfalls auf Basis einer CMDB realisiert werden.

Das IT-Service-Engineering, d. h., die systematische Entwicklung von IT-Dienstleistungen wird zusehends zu einem kritischen Erfolgsfaktor für IT-Dienstleister. Standardisierte IT-Dienstleistungen, Service-Produkte werden primär durch Beschreibungen spezifiziert, welche Services mit welchen Ressourcen von wem erbracht werden.

Die Beschreibungen, welche Dienstleistungen durch den Einsatz welcher Ressourcen und durch welche Prozesse erbracht werden können, werden als Potenzialdaten bezeichnet. Sie

[1] vgl- Lüke, Detlef (2005)

sind quasi die Baupläne für die Erbringung der Dienstleistung. Beim Abschluss von Service-Level Agreements (SLA) mit Kunden werden die Dienstleistungen beschrieben und die Dienstgüte festgelegt. Die Service-Produkte stellen für den IT-Dienstleister dynamische Geschäftsobjekte dar, wobei alle Phasen des Service-Lebenszyklus geplant werden müssen. Dabei ist zu berücksichtigen, dass standardisierte Dienstleistungen innerhalb definierter Grenzen an spezielle Kundenwünsche anpassbar sein müssen, dazu werden viele Dienstleistungen konfigurierbar gestaltet oder Varianten in der Service-Architektur vorgesehen. Bei Änderungen bestehender IT-Services kann das Change Management gemäß ITIL herangezogen werden. Ein wesentlicher Erfolgsfaktor für die Entwicklung kundenorientierter Dienstleistungen ist des Weiteren die kontinuierliche Erweiterung, Erneuerung oder Anpassung des Service-Portfolios.[1]



(Quelle: Grawe, Tonio (2005a), S.24)

Abb. 21 Aufgaben im IT-Service-Management

Ein übergreifender ITIL-Prozess ist das Securitymanagement: Der ITIL-Ansatz ermöglicht eine individuelle Integration des Securitymanagements mit dem IT-Management. IT-Sicherheit wird bereits im Service Continuity Management angeschnitten und über die

[1] vgl. Grawe, Tonio (2005a)

britische Norm BS 7799 detailliert spezifiziert. Securitymanagement nach ITIL wird definiert als der Prozess zum Management eines vorgegebenen Niveaus der Sicherheit bezüglich Informationen und IT-Services. Dieser Prozess hat Schnittpunkte/inhaltliche Überlappungen mit den BS 7799 „Domains“ Security Policy, Organizational Security, Personal Security, Physical and Environmental Security, Access Control and Compliance.

Bei der Implementierung von IT-Service-Management-Prozessen ist das Securitymanagement so einzubeziehen, dass sich alle Sicherheitsmaßnahmen auf klar definierte Prozesse und Serviceanforderungen beziehen. Jedes Kapitel des ITIL Service Support Set sieht Sicherheitsaspekte als unverzichtbaren Bestandteil an. Für den IT-Sicherheitsbeauftragten bietet die Ankopplung an das Prozess-orientierte Thema ITIL die Chance einer erhöhten Management-Attention und Akzeptanz.[1]

Daneben gibt es noch andere ITIL-Prozesse, die Sicherheitsaspekte behandeln. Das Securitymanagement definiert Anforderungen für diese anderen Prozesse. Z. B. Availability Management, Business Continuity Management und Service-Level Management.[2]

Der Security-Management-Prozess gemäß ITIL betrifft Implementierungspläne mit Maßnahmen, die aus der Informationssicherheitspolitik abgeleitet wurden sowie mit Maßnahmen aufgrund der Risikoanalyse und spezifischen Business-Sicherheitsanforderungen. Es geht um die im IT-Service-Level Agreement identifizierten Security-Anforderungen und nicht um Fragestellungen im Zusammenhang mit der Security Policy.

Im Security Management Prozess nach ITIL werden also keine Risikoanalysen und -bewertungen durchgeführt. Der Security Management Prozess ist als Methode im Zusammenhang mit anderen Methoden und Standards (z. B. BS 7799, Grundschutzhandbuch, CObIT) zu verstehen und anzuwenden.[3] Es geht in den Implementierungsplänen zwar um Maßnahmen aufgrund der Risikoanalyse, die Risikoanalyse wird aber nicht explizit beschrieben.

Dies ist in dem Standard ISO/IEC 20000/BS 15000 enthalten, die die eindeutige Möglichkeit, die Qualität des IT-Service-Managements nach ITIL zu „messen“, somit vor allem in der Risikoanalyse und -bewertung sehen.

Über die Betrachtung von durch die IT-Security beeinflussbaren Nutzenpotenzialen der IT kann die ex-ante Bewertung der IT-Security konkretisiert werden. Die hinreichende Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security (im Kontext des

[1] vgl. Kob, Timo/Schumann, Detlef (2005):
[2] vgl. Bernhard, Martin G. (2005):, S.100,101
[3] vgl. Bernhard, Martin G. (2005):, S.101

technisch-organisatorischen Umfelds des Unternehmens) wurde mit der Optimierung der durch die IT-Security beeinflussbaren Nutzenpotenziale/der Effizienz der IT in Verbindung gebracht. Diese Optimierung kann in der Form geschehen, die Maximierung, die Nutzenpotenziale der IT durch geeignete Eskalations- und Risikobewältigungsstrategien sowie ein geeignetes Business Continuity Planning (Notfallplanung/Incident-Management) organisatorisch abzusichern. Diese zielen auf die Unterstützung/Herstellung der Handlungsbefähigung ab.

5.1.2.3.1 Eskalations- und Risikobewältigungsstrategien

Eskalationsstrategien beschreiben das Vorgehen beim Auftreten bestimmter kritischer Ereignisse und sollen die Auswirkungen eines Sicherheitsvorfalls begrenzen. Das im Rahmen von Basel II von den Banken einzuführende Risikomanagement-System muss Maßnahmen enthalten, die ergriffen werden, wenn Risiken auftreten. Zudem muss es mit einer sog. Eskalationsleiter unterlegt sein, die beschreibt, wer zu welchem Zeitpunkt welche Entscheidungsgewalt hat.[1]

Informationssicherheits-Vorfälle sind Ereignisse, die Schaden bezüglich der Vertraulichkeit, Integrität und/oder Verfügbarkeit von Informationen oder der Informationsverarbeitung verursachen können. Tritt ein Schaden ein, wird dieser mit Hilfe von festgelegten Prozessen gemeldet, aufgenommen und mittels definierter Workflows an die betroffenen Ansprechpartner zur Bewertung weitergeleitet. Alle relevanten Fachabteilungen des Unternehmens werden sofort informiert und im Notfall werden Experten kontaktiert. Zudem besteht die Möglichkeit, dokumentierte Schadensfälle als E-Learning-Kurs zur Verfügung zu stellen.

Interne Sicherheit, gefährdet durch interne und externe Risiken, bedeutet die Sicherstellung der Zugriffsmöglichkeiten auf vertrauliche, genaue und vollständige Daten. Externe Sicherheit bedeutet Informationssicherheit als Produktionsfaktor für Waren und Dienstleistungen, d. h. einen sicheren Informationsfluss in allen Richtungen (zwischen verschiedenen Unternehmen, Unternehmen und Kunden, Lieferanten und anderen Partnern).[2]

Strategien zur Erhöhung der Sicherheit bzw. Gewährleistung eines definierten Sicherheitsniveaus basieren auf der Beseitigung bzw. der Veränderung der Risikoursachen einerseits und die Vorsorge für den Fall des Schadenseintritts andererseits. Die Risikobewertung soll Entscheidungsgrundlagen hinsichtlich Risikobewältigungsmaßnahmen schaffen. Risikobewältigungsstrategien versuchen, den Risikofaktor zu eliminieren (Risikovermeidung) oder

[1] vgl. Töpfer, Armin (2003), S.25
[2] vgl. Bernhard, Martin G. (2005):, S.104

effektive Risikoreaktionen festzulegen bzw. Risikoauswirkungen zu verringern (Risikovorsorge).

Werden Produkte oder wirtschaftliche Aktivitäten aufgegeben mit dem Ziel, die damit verbundenen Risiken zu vermeiden, so spricht man von Risikovermeidung. Auch die Anpassung der Prozessabläufe (beispielsweise im Produktionsprozess) kann zur Vermeidung von Risiken beitragen.

Werden Risiken durch die Ausgliederung von Unternehmensfunktionen, durch regionale oder objektbezogene Streuung bzw. durch technische oder organisatorische Maßnahmen (z. B. umfassendes Brandschutzkonzept) reduziert, so spricht man von Risikoverminderung.

Risiken können auf andere Wirtschaftssubjekte externalisiert werden durch: Haftungsvereinbarungen und Gewährleistungsregelungen in Allgemeinen Geschäftsbedingungen. Durch Outsourcing von Unternehmensfunktionen (beispielsweise Facility-/Gebäude-Management, EDV-Funktionen, Factoring/Forderungseinzug, Logistik, Leasingverträge für Produktionsmaschinen) können Risiken – sofern sie voneinander unabhängig sind – regional, objektbezogen oder personenbezogen gestreut werden. Wird beispielsweise die Produktion von Speicherchips auf drei regional voneinander getrennte Produktionseinheiten verteilt, so wird das Risiko einer Betriebsunterbrechung oder eines Totalausfalls durch Brand reduziert.

Bei der Risikofinanzierung geht es um die Frage, inwieweit Risiken externalisiert werden (beispielsweise gegen die Zahlung einer Versicherungsprämie) bzw. welche Risiken vom Unternehmen selbst getragen werden.

Die Sichten Verlässlichkeit, Beherrschbarkeit und Handlungsbefähigung sind im Allgemeinen komplementär. Eine größere Handlungsbefähigung trotz Unsicherheit führt zu einer größeren Akzeptanz der Risiken. Die Sichten Verlässlichkeit und Beherrschbarkeit des technisch-organisatorischen Kontexts für die IT-Security sind daher (im Rahmen der Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen) in den Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume abzubilden, um eine größere Akzeptanz der Risiken zu ermöglichen. Eine "Einstellung" des Kontextes für die IT-Security, sodass erkannte Risiken akzeptabler gemacht werden können, ist also folgendermaßen zu ermöglichen: Die Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in den Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume muss zu einer größeren Handlungsbefähigung führen. Dies ist durch entsprechend ausgestaltete Prä-

missenkontrolle, strategische Durchführungskontrolle und strategische Überwachung (über den diese Transformation definiert wurde) zu ermöglichen.

Auf Seite des technisch-organisatorischen Kontexts für die IT-Security soll dies dann zu einer IT-Infrastruktur führen, die den Anforderungen auf Basis von vorhandenen Normen und Bewertungskriterien genügt und eine möglichst hohe System- und Datenverfügbarkeit sowie den Schutz der Informationen gewährleistet.

Zur Behebung von Sicherheitsrisiken der IT-Infrastruktur werden Präventivmaßnahmen zum physischen Schutz von Installationen durchgeführt. Dieser Anpassungsprozess an die Umgebung (in Form des Risikoumfelds der IT-Infrastruktur) muss die Bedingung erfüllen, dass die Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in den Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume zu einer größeren Handlungsbefähigung führt. Diese Bedingung muss z. B. auch im Rahmen eines auf Risikoakzeptanz abzielenden Change Managements gemäß ITIL erfüllt werden:

Das Change Management stellt Methoden und Verfahren für Veränderungen vor allem der IT-Infrastruktur bereit. Das Security Management hat hier die Aufgabe, die Sicherheitsrelevanz der Änderungen festzustellen. Aber auch umgekehrt stellt die IT-Security Anforderungen an ein Unternehmensweites Change Management.

5.1.2.3.2 Business Continuity Planning (Notfallplanung/Incident Management)

Aufgrund weltweit steigender Bedrohungen durch Naturkatastrophen und politisch motivierte Anschläge ist das Business Continuity Planning/Management zu einem bedeutenden Thema für das Management der Unternehmen geworden. Business Continuity Planning ist darauf ausgerichtet, nach einem Schadensfall die Funktionsfähigkeit eines Unternehmens/einer Organisation wieder herzustellen. Ziel ist die volle Wiederherstellung der Funktionsfähigkeit nach einem Unfall/Schaden/einer Störung in möglichst kurzer Zeit.[1] Um die Möglichkeiten der technischen Notfallvorsorge auszuschöpfen, ist das Business Continuity Planning durch eine im Rahmen der Business Continuity Prozesse stehenden Business Continuity Organisation einzurahmen. Diese sollte vorgeben, wer was wann auf welchem Weg zu tun hat. Jeder Unternehmensbereich soll einen Business Continuity Manager stellen, der für seinen Verantwortungsbereich in einer Notfallsituation die Entscheidungsgewalt hat. Entscheidungen, die andere Unternehmensbereiche beeinflussen, Dissens zwischen den Unternehmensbereichen muss über schnelle Eskalationsstrategien gelöst werden. Für die ver-

[1] vgl. Parthier, Ulrich (2005a)

schiedenen Rollen, von den Business Continuity Managern bis hin zu den Administratoren sind innerhalb von sog. Business Continuity Prozessen die Kommunikations-, Informations- und Entscheidungswege klar zu konzipieren.[1]

Verbindlich gefordert wird eine „schriftliche Notfallplanung“ sowie „Vorsorge für mögliche Fehler in der angewandten Software und für unvorhergesehene Personalausfälle“ etwa in den Mindestanforderungen für das Kreditgeschäft der Kreditinstitute (MaK). Diese wurden im Rahmen der Umsetzung europäischer Anforderungen resultierend aus Basel II durch die MaRisk zusammen mit den Mindestanforderungen an das Betreiben von Handelsgeschäften der Kreditinstitute (MaH) und den Mindestanforderungen an die Ausgestaltung der Internen Revision (MaIR) der Kreditinstitute in einem modularen Regelwerk auf Basis des § 25a Abs. 1 KWG zusammengefasst. Die Notfallpläne sind – wie auch die DV-Systeme und DV-technischen Verfahren – regelmäßig zu prüfen und gegebenenfalls anzupassen.

Im Business Continuity Management/Planning werden die Anforderungen zur Bewältigung eines Notfalls von den Geschäftsprozessverantwortlichen definiert, sind also von der Kritikalität der Geschäftsprozesse abhängig. Der Bereich Business Continuity Management in der Business Perspektive von ITIL beschäftigt sich mit Geschäftsprozessen, die im Katastrophenfall die Betriebsbereitschaft wieder herstellen bzw. aufrechterhalten sollen. Business Continuity Planning bezieht sich auf den Geschäftsbetrieb insgesamt, die Notfallplanung dagegen mehr auf einzelne Objekte. So eine Notfallplanung muss die Einhaltung folgender Zielsetzungen gewährleisten: [2]

- Schutz von Menschen vor Gefahren,
- Schutz der entscheidenden Prozess-Ressourcen;
- Ermöglichung der gewünschten Prozess-Ergebnisse selbst im Fall einer Störung, und
- Garantie der schnellen Wiederaufnahme einzelner Aktivitäten nach einem Schaden..

Zu berücksichtigen ist dabei, dass der Schaden das ihn auslösende System insgesamt verändern kann, d. h., dass Rückwirkungen solcher Schadensverläufe auf ihre eigenen Ausgangsbedingungen angenommen werden. Dies ist durch komplexe Technologien begründet, deren Nutzenfunktion mit unvorhersehbaren Schadensfunktionen verbunden ist[3] (z. B. Atomkraft oder auch sich aufschaukelnde Schäden bei Kausalketten in der IT). Schaden ist im Allgemeinen das ungünstigste Ergebnis einer getroffenen Entscheidung.

[1] vgl. Miscbur, Oliver (2006)
[2] vgl. Wieczorek, Martin (2003), S.16
[3] vgl. Japp, Klaus P. (2000), S.8

Die Notfallplanung sollte sich an den Prozess der Risikoanalyse anlehnen sowie Verantwortlichkeiten und konkrete Handlungsanweisungen festlegen. Sie ergänzt die Verfahrensbeschreibungen für den Regelbetrieb und die Maßnahmen zur Aufrechterhaltung des Systembetriebs um Vorgaben zur Handhabung von Schadensvorfällen mit dem Ziel, die Schadensauswirkungen zu minimieren und die schnellstmögliche Wiederaufnahme des Regelbetriebs zu ermöglichen.[1]

Die Vorfall-/Notfallbehandlung ist umso wirksamer, je früher der Vorfall entdeckt wird. Dazu ist neben technischen Maßnahmen wesentlich, dass die Anwender auf ungewöhnliches Systemverhalten und ungewöhnliche Systemzustände achten. Außerdem muss vorausschauend agiert werden und z. B. auf extern erkannte Schwachstellen vorsorgend reagiert werden. Auf technischer Seite müssen die Systeme zur Verhinderung und Entdeckung von Vorfällen auf Eindring- und Manipulationsversuche überwacht werden. Zur Behandlung des Vorfalls selber (Minimierung der Auswirkungen) müssen geeignete und ausreichend Ressourcen bereitgestellt werden.[2]

Wenn das Management mögliche Risikoauswirkungen vorab mit Szenariotechniken durchspielt und für verschiedene Situationen einen Notfallplan entwickelt, kann es schneller, besonnener und wirkungsvoller auf solche unvorhersehbaren Ereignisse reagieren.[3]

Dabei ist vor allem das Verhältnis zwischen genauer Festlegung der Verfahren des Notfallmanagements und der Business-Coninuity-Sicherung einerseits und notwendiger Handlungsfreiheit im Notfall andererseits nur schwer richtig zu gestalten. Der IT-Revisor hat die Verfahren des Notfallmanagements und der Business-Continuity-Sicherung, ausgehend von der vorhandenen Dokumentation, auf ihre Praktikabilität, Effizienz und organisatorische Lösungskompetenz hin zu prüfen. [4] Als Notfallmanagement und Business-Continuity-Sicherung sind Notfallpläne wesentliche Bestandteile operativer IT-Systeme.

Die frühzeitige Erkennung und Behebung von Krisensituationen im klassischen betriebswirtschaftlichen Sinn (z. B. in Projekten) wird als Turnaround-Management bezeichnet. Es grenzt sich dabei vom Krisenmanagement ab, was etwa beim Eintreten einer Liquiditätskrise notwendig wird.[5]

[1] vgl. Kamlah, Bernd (2004a), S.10
[2] vgl. Weissmann, Olivet (2005)
[3] vgl. Merbecks, Andreas (2004), S.107
[4] vgl. Vossbein, Reinhard (2005b)
[5] vgl. Harbick, Dierk (2005)

Business Continuity Planning/Management verallgemeinert die Notfallplanung dahin gehend, dass die Anforderungen an die Bewältigung eines Notfalls von der Kritikalität der Geschäftsprozesse abhängig gemacht werden. Daraus ist abzuleiten, [1]

- innerhalb welcher Zeitspanne nach einem Vorfall die betroffene Anwendung bzw. das betroffene IT-System wieder verfügbar sein muss und
- welcher Daten-/Integritätsverlust tolerierbar ist bzw. wie hoch die damit verbundenen Kosten sein dürfen.

Die größte Herausforderung bei der Erarbeitung eines Notfallkonzeptes ist also eine Datensicherungs- und Ausweichstrategie zu finden, die die geforderte Verfügbarkeit mit minimalem Kostenaufwand garantiert. Technische Notfallmanagement(Incident Management) -Lösungen basieren meist einfach darauf, zusätzliche interne oder externe IT-Ressourcen bereitzustellen, auf die im Notfall zurückgegriffen werden können. Für ein integriertes Notfallmanagement ist jedoch das Zusammenspiel von Technik, Notfallverfahren und Organisation ausschlaggebend.[2]

Was vorbeugend zu tun ist, wenn Maßnahmen der Risikopolitik versagen, sich Störfälle, Unternehmenskrisen oder gar Katastrophen ereignen, bedarf weiterer Untersuchungen. Klar ist zunächst, dass auch das Krisenmanagement die bewährten Methoden der betriebswirtschaftlichen Organisation übernehmen muss, um insbesondere die hohen Kosten ihrer Dienstleistungsbereitschaft zu rechtfertigen und zu optimieren. [3] Zur Schaffung eines adäquaten Grades an Robustheit gegenüber Risiken, Gefahren und Krisen wird z. B. ein strategisches Kontinuitätsmanagement (SKM) vorgeschlagen. Dabei wird „Sicherheit“ als nur eine, aber signifikante Klasse von Risiken im Rahmen „elektronischer Geschäftsmodelle“ betrachtet. Die Robustheit wird einerseits durch Auswahl geeigneter Präventivmaßnahmen, zudem jedoch auch durch die Fähigkeit zur „reaktiven Krisenbewältigung“ gewährleistet. Dabei wird berücksichtigt, dass vor allem im Rahmen elektronischer Geschäftsmodelle, die einem raschen unvorhersehbaren Wandel unterliegen, trotz umfassender Vorkehrungen krisenhafte Ereignisse auftreten. Typische Folgen einer sicherheitsbezogenen Krise sind Unterbrechungen, Modifikationen an elektronischen Geschäftsprozessen, indirekte Schäden wie Reputationsschäden usw. Beeinträchtigungen der IT-Umgebung durch Brand oder Stromausfall werden nicht als Problem der IT-Sicherheit im engeren Sinne angesehen, da die Verantwortung für die gebäudeseitige Absicherung nicht bei der IT-Abteilung liegt. Wichtig für die Wirksamkeit eines strategischen Kontinuitätsmanagements ist, dass sich offensichtliche und verdeckte Risiken nicht durch Zuweisung unter einzelne Gebiete wie „IT-Sicherheit“

[1] vgl. Mischur, Oliver/Bostelmann, Uwe (2005)
[2] vgl. Kullmann, Peter (2005)
[3] Vgl. Mayer, Volker (2003):

oder „Datensicherung“ isolieren lassen. Zu untersuchen sind die Abhängigkeit des Kerngeschäfts von den IT-Prozessen und die Anfälligkeit des Unternehmens gegenüber jeglichen Einflussfaktoren, die das Geschäftsmodell stören könnten (business impact assessment). Als entscheidend für den Grad der Absicherung elektronischer Geschäftsprozesse wird der „zu erwartende Folgeschaden, der im Zuge eines Ausfalls des Kerngeschäfts zu bewältigen“ ist, benannt. Insbesondere für elektronische Geschäftsmodelle und die zugehörigen Technologien – da sich diese gewöhnlich in einem starken Wandel befinden – ist „zur Dynamisierung und Optimierung“ ein SKM-Zyklus erforderlich, in welchen durch Tests, Revision und nachfolgende Wartung der vorgesehenen Maßnahmenkataloge eine stetige Verbesserung der Robustheit sichergestellt wird. Gegenüber dem präventiven IT-Sicherheits- und allgemeinen Risikomanagement, die vorbeugend eingesetzt werden, um bestandsgefährdende Risiken zu begrenzen, soll der „reaktive“ Teil des SKM-Ansatzes eine Fortführung der Geschäftstätigkeit nach Eintreten eines krisenhaften Ereignisses bzw. Sicherheitsvorfalls gewährleisten.[1]

Auch Ausfälle und Störungen der Informations- und Kommunikationsinfrastruktur können – ohne entsprechende Absicherungen – zu einem Ausfall der Informationsverarbeitung führen. Dies gilt entsprechend für den Ausfall von Mitarbeitern, die über Spezialwissen verfügen und keinen gleich kompetenten Vertreter haben. Derartige Ausfälle schränken die Handlungsfähigkeit des Unternehmens/der Organisationseinheit mehr oder weniger stark ein. Um den Auswirkungen eines Notfalls oder einer Katastrophe entgegenzuwirken, müssen Maßnahmen präventiver Art getroffen werden, die Ausfälle z. B. aufgrund menschlichen Fehlverhaltens von vornherein vermeiden. Außerdem sollen Stellen vermieden werden, bei deren Ausfall es keine Ausweich-/Ersatzmöglichkeit gibt. Prinzipiell sollte jedes Element des Gesamtsystems redundant vorhanden sein. So hat das Kontinuitätsmanagement sicherzustellen, dass eine angemessene Handlungsfähigkeit des Unternehmens erhalten bleibt.[2]

Im Folgenden geht es um die Überwachung/Steuerung des IT-Security-Managements mithilfe des Modells zum strategisch-operativen Risiko-Controlling. Damit soll die Effektivität und Effizienz des IT-Security-Managements, welche gleichzeitig die strategisch-operative Beweglichkeit/Handlungsbefähigung des Unternehmens unterstützen soll, gewährleistet werden.

[1] vgl. Horster, Patrick (2002b), S.16-29
[2] vgl. Müller, Klaus-Rainer (2003), S..103-106

5.1.3 Einrichtung und Etablierung eines IT-Security-Managementsystems

Das Risikomanagement betrachtet neben diversen Geschäftsrisiken natürlich auch Risiken aus dem Umgang mit Informationen. Dazu gehören Verletzungen der Vertraulichkeit oder Integrität von Informationen sowie deren Nicht-Verfügbarkeit. Ein Informationssicherheits-Managementsystem (ISMS) stellt eine Möglichkeit zur Ausgestaltung eines solchen Managements von Risiken aus dem Umgang mit Informationen dar.

Der internationale Sicherheitsmanagement-Standard ISO/IEC 17799 (Information technology – Code of practice for information security management) und (basierend auf den BS 7799-2) der internationale Standard für Informationssicherheits-Managementsysteme ISO/IEC 27001 (Information security management systems – Requirements) verfolgt mit der Einführung eines systematischen Managements der Informationssicherheit in der Organisation den Ansatz eines kontinuierlichen Verbesserungsprozesses. Ein nach dieser Norm aufgebautes Informationssicherheits-Managementsystem soll eine Grundlage zur Identifikation und Beherrschung spezifischer IT-Risiken sowie zur Sicherstellung der benötigten Zuverlässigkeit von IT&TK-Systemen bieten. Dieser Ansatz wird in Richtung eines Managements der IT-Security verallgemeinert:

Ein Managementsystem umfasst alle Regelungen, die für die Steuerung und Lenkung der Zielerreichung der Institution sorgen sollen; es ist ein Führungs- und Organisationssystem zur optimalen Führung im Rahmen der Unternehmenspolitik und der für einen bestimmten Bereich festgelegten Unternehmensziele. Es kann als Regelkreis interpretiert werden: Die Einhaltung vor Vorgaben wird mit entsprechenden Maßnahmenprogrammen angestrebt, und die Erreichung der Ziele ist ständig zu überprüfen. Diese Managementsysteme orientieren sich nicht an der Aufbauorganisation, sondern an den wichtigsten Prozessen im Unternehmen.[1] In „hoch entwickelten“ Unternehmen werden manchmal die Bereiche Anlagensicherheit, Produktsicherheit, Transportsicherheit und Notfallmanagement in das Managementsystem für Qualität, Umwelt- und Arbeitsschutz integriert. Ziel ist es, verschiedene Managementsysteme zu einem Gesamt- oder Integrierten Managementsystem (IMS) auszugestalten. Die wesentlichen Punkte bei einem IMS sind dabei die Bewertung der Wirksamkeit (dauerhafte Effizienzverbesserung durch optimale Ressourcennutzung (Personal, Technik und Organisation)) durch die Unternehmensleitung und kontinuierliche Verbesserungsprozesse.[2]

Das ISMS ist der Teil des Managementsystems, der sich mit Informationssicherheit beschäftigt. Das ISMS legt dazu fest, mit welchen Instrumenten und Methoden das Management die auf die Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar

[1] vgl. Löbel, Jürgen (2005), S.33-35
[2] vgl. Löbel, Jürgen (2005), S.5-7

lenkt (plant, einsetzt, durchführt, überwacht und verbessert.[1] Als Information Security Management System wird jener Teil des übergreifenden Managementsystems bezeichnet, das die Organisationsstruktur, Regelungen, Abläufe und Ressourcen zur Entwicklung, Umsetzung, Bewertung und Aufrechterhaltung der Informationssicherheitspolitik beinhaltet und dokumentiert.[2]

Die Standards ISO/IEC 17799 und ISO/IEC 27001 definieren Methoden und Anforderungen an ein leistungsfähiges Managementsystem für Informationssicherheit. Informationssicherheit ist der Schutz von Informationen oder Informationsressourcen vor unautorisierter oder ungewollter Zerstörung, Modifizierung, Offenlegung oder Benutzung. IT-Sicherheit beschreibt in diesem Zusammenhang den Schutz der durch die Informationstechnik verarbeiteten Informationen, wobei einzelne Bestandteile der IT-Sicherheit (z. B. physikalischer Schutz von Datenverarbeitungsanlagen) nicht zur Informationssicherheit gehören. Informationen können sowohl auf Papier, in Rechnern, oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich primär mit dem Schutz elektronisch gespeicherter Informationen und derer Verarbeitung. Der Begriff Informationssicherheit umfasst die IT-Sicherheit.[3] Die Herstellung und Aufrechterhaltung einer umfassenden Informationssicherheit in einer Organisation wird als globaler Prozess gesehen.

Die Standards beschreiben neben Sicherungsmaßnahmen dazu den Aufbau eines Informationssicherheits-Managementsystems mit den Schwerpunkten Security Policy, Risikoanalyse, Risikomanagement, Kontrollmechanismen und Schutzmaßnahmen. „Übersetzt“ wurde der ISO 27001 in den BSI Standard 100-1:[4] Er definiert allgemeine Anforderungen an ein Informationssicherheits-Managementsystem (ISMS), ist vollständig kompatibel zum ISO Standard 27001 und berücksichtigt des Weiteren die Empfehlungen der ISO Standards 13335 und 17799.[5]

Um die Ziele des ISMS zu erreichen, sind Managementinstrumente zur Planung, Realisierung, Betrieb, Überwachung und kontinuierlichen Verbesserung erforderlich. Dazu ist der Informationssicherheits(IS)prozess eines der wichtigsten Kernelemente eines ISMS.

Der ISO 27001 ähnelt in der Methodik der Vorgehensweise anderer Qualitätsnormen wie den ISO 9001 (Qualitätsmanagementsysteme- Anforderungen) und ISO 14001 (Anforderungen an ein Umweltmanagementsystem) und setzt auf dem Plan-Do-Check-Act Modell mit dem Zyklus Risikoanalyse und Festlegung von Maßnahmen, Implementierung, Überwachung,

[1] BSI (2006), S.24
[2] vgl. Rudholzer, Gerhard (2005), S.32
[3] vgl. BSI (2006),S.20
[4] BSI (2006), S.15-52
[5] vgl. BSI (2006), S.12

Bewertung und Verbesserung auf.[1] Man verlässt damit das lineare Ursache-Wirkungs-Denken und geht zu einem integrierten Denken und Handeln in rückgekoppelten Prozessen über.[2] Der PDCA-Zyklus des ISO 27001 enthält zunächst die Darstellung der Aktivitäten für die Planung eines ISMS (Phase Plan), in der der Anwendungsbereich festgelegt, spezifische Risiken erhoben und Maßnahmen zur Risikobehandlung ausgewählt werden. Als Ergebnisse liegen nach der Planungsphase die Schutzbedarfsanalyse (Inventur und Bewertung von Schutzobjekten), die Risikoanalyse (Identifizierung und Analyse von Risiken), die Risikobewertung (quantitativ oder qualitativ) und Maßnahmenkataloge zur Risikobewältigung vor. In der Phase Do ist das ISMS umzusetzen (Realisierung des Maßnahmenkatalogs, was entsprechende Anpassungen von Technik, Organisation und Prozessen auslöst), in der Phase Check auf Einhaltung der Anforderungen zu überwachen/zu prüfen (Ermittlung der Wirksamkeit der Maßnahmen durch Neubewertung der verbliebenen Risiken und Erarbeitung von Alternativen zur Risikobehandlung) und in der Phase Act durch kontinuierliche Verbesserung aufrechtzuerhalten (Umsetzung der Alternativen zur Risikobehandlung und Anpassung von internen Richtlinien und Standards).

Als Ergebnis eines PDCA-Zyklus liegt neben einer Bewertung der durch Maßnahmen behandelten Risiken ein ggf. optimiertes Richtlinienwerk vor. Der ISO 27001 macht Vorgaben für diese Phasen und somit für ein System aufeinander abgestimmter Aktivitäten. Die im Rahmen des PDCA-Zyklus durchzuführenden Schritte sollen dem Unternehmen ermöglichen, die eigenen Risiken zu ermitteln und zu steuern. Der ISO 17799 liefert für dieses System die konkretisierten Schutzziele und plattformunabhängigen Maßnahmen. Darüber hinausgehende Beschreibungen systemspezifischer Schutzmaßnahmen finden sich in detaillierteren Maßnahmenkatalogen wie dem Grundschutzhandbuch des BSI.

Die Informations-Security-Norm ISO 17799 will erprobte Bewertungsmethoden und Sicherheitsmaßnahmen liefern, die den Aufbau eines strategischen ISMS ermöglichen. Der ISO/IEC 17799:2005 unterteilt sich dazu in die Kapitel Security Policy, Organizing Information Security, Asset Management, Human Ressources Security, Physical & Environmental Security, Communications & Operations Management, Access Control, Information Systems Acquisition Development & Maintenance, Information Security Incident Handling, Business Continuity Management und Compliance. In den einzelnen Kapiteln gliedert er sich in Maßnahmenziele und Maßnahmen, mit denen diese Ziele erreicht werden sollen. Jede Maßnahme wird in drei Teile Control, Implementation Guidance und Other Information unterteilt.

[1] vgl. Hirch, Axel/Rahmel, Jürgen (2005)
[2] vgl. Gomez, Peter (2002), S.127

Das Strategische beim ISMS bezieht sich auf die Kernpunkte der Sicherheitspolitik (legt die Sicherheitsziele und damit das angestrebte ganzheitliche Sicherheitsniveau fest) wie Risikoevaluierung und -minimierung. Die Sicherheitspolitik umfasst die strategische Ausrichtung und die Unterstützung der Geschäftsführung bei der Informationssicherheit. Diese ist mit der Unternehmensstrategie abzustimmen. Diese strategischen Aspekte sollen um die, dem in dieser Arbeit entwickelten Modell zugrunde liegenden Konzepte mit dem Ziel der Gestaltung einer automatisierten permanenten Kontrolle/Überwachung der Formulierung und Umsetzung des Sicherheitskonzepts (auf einer Schwachstellenanalyse basierende SOLL-Darstellung des Sicherheitszustandes, welche Basis für das Sicherheitsmanagement ist), erweitert werden:

Ist das Sicherheitskonzept erstellt, muss dessen Umsetzung gesteuert, sowie ständig kontrolliert werden, ob es noch der aktuellen Situation gerecht wird.[1] Dies kann mithilfe der von dem als „management control“ (Controlling im Sinne der umfassenden koordinationsorientierten Konzeption) bezeichneten Controlling geforderten Systeme zur Unterstützung der Strategieformulierung und -umsetzung bezüglich der IT-Security-Managements geschehen. Strategieformulierung betrifft dann die Formulierung, und Strategieumsetzung die Umsetzung des Sicherheitskonzepts. Dazu können Prozesse bzw. Systeme integriert werden, die die für den IT-Security-Prozess definierten Risikokomponenten Planungsrisiko, Umsetzungsrisiken, und Überwachungsrisiko analysieren, bewerten und steuern.

Der IT-Security-Prozess ist der Regelkreis von der Planung zur Umsetzung und Überwachung der Sicherheitsstrategie. Die ungewissen konkreten Zielvorgaben/Zielsetzungen des IT-Security-Prozesses werden ersetzt durch die Zielsetzung Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit (bei der Durchsetzung/Umsetzung/ Implementierung der Unternehmensstrategie/IT-Security-Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses, bzw. Abstimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander). Das Risiko für den IT-Security-Prozess setzt sich aus drei Komponenten zusammen: Planungs-, Umsetzungs- und Überwachungsrisiko bezüglich der Security-Strategie.

Der gesamte IT-Sicherheitsprozess wird im Sinne des PDCA-Zyklus in die Phasen Planung (Plan), Umsetzung der Planung/Durchführung des Vorhabens (Do), Erfolgskontrolle/Überwachung der Zielerreichung (Check) und Beseitigung von erkannten Mängeln und Schwächen/Optimierung und Verbesserung (Act) eingeteilt.

[1] vgl. Bursch, Daniel (2005), S.117

Die Phase Plan des zugehörigen IT-Security-Managements betrifft u. a. die auch zukünftige Gültigkeit der der Planung zugrunde liegenden Prämissen. Das Risiko, dass die auch zukünftige Gültigkeit der der Planung zugrunde liegenden Prämissen nicht korrekt überprüft/überwacht wird, sei als Überwachungsrisiko definiert.

Die Umsetzung der Planung/Durchführung des Vorhabens (Phase Do) betrifft das Management und das Controlling von Umsetzungsrisiken. Die Umsetzungsrisiken werden im Rahmen des Controllings vom technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen in den Kontext der Handlungsbefähigung/strategisch-operativen Beweglichkeit abgebildet. Dies ist auch der Anknüpfungspunkt für die ex-ante Bewertung (der Umsetzung) der IT-Security/des IT-Security-Prozesses.

Die Überwachung schließlich betrifft Fehleinschätzungen der Kritikalität/Sensitivität der Sachwerte und Prozesse und wie relevant die Konformität mit externen und internen Ordnungsmäßigkeitsvorgaben ist (Planungsrisiken).

Das IT-Security-Managementsystem kann in ein strategisches und in ein operatives System konzeptioniert werden. Das strategische IT-Security-Managementsystem führt das operative IT-Security-Managementsystem, steuert den vom IT-Security-Managementsystem insgesamt implementierten IT-Security-Prozess. Ergebnisse des strategischen IT-Security-Managementsystems fließen in das operative IT-Security-Managementsystem ein.

Zwei wichtige Werkzeuge der Prozesssteuerung sind das Risikomanagement und das Prozesscontrolling. Das Risikomanagement baut eine Analyse der Risiken ein, die im Prozess und vor allem nach Prozessende zu überwachen und zu ergänzen sind. Prozesscontrolling in Form eines Umsetzungscontrollings steuert und lenkt die Umsetzung des Prozesses auf der Maßnahmenseite, treibt die Umsetzung an.[1]

Analog werden zur Steuerung des IT-Security-Prozesses vom IT-Security-Management die Werkzeuge IT-Security-Risikomanagement und IT-Security-Prozesscontrolling verwendet. Das IT-Security-Managementsystem kann sich dabei an dem in dieser Arbeit entwickelten IT-Security-Framework auf Basis des strategisch-operativen Risiko-Controllings orientieren, welches die Strategieebene mit der Ebene der IT-Security/IT-Sicherheit verbindet. Dieses Framework verbindet diese beiden Ebenen in Form der Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in die auf das System bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume. Das

[1] vgl. Stöger, Roman (2005), S.183,186

Informationssicherheits-Managementsystem wird damit um die drei Komponenten (strategische und operative) Prämissenkontrolle, (strategische und operative) Durchführungskontrolle und (strategische und operative) Überwachung erweitert, welche operativ die Umsetzung des IT-Security-Prozesses auf der Maßnahmenseite steuern und lenken. Dies zielt ab auf die Unterstützung der strategisch-operativen Beweglichkeit und die Optimierung der durch die IT-Security beeinflussbare Effektivität und Nutzenpotenziale/Effizienz der IT.

Diese IT-Security soll die Strategie konforme und IT-Nutzenpotenzial absichernde Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume so weit möglich gewährleisten. Die Strategie-Konformität und Absicherung der IT-Nutzenpotenziale soll dadurch unterstützt werden, dass adäquate Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security in das strategische und operative Performance Managements integriert werden.

Das strategische Performance Management (mit strategischer Prämissenkontrolle, strategischer Durchführungskontrolle und strategischer Überwachung) und das operative Performance Management (mit operativer Prämissenkontrolle, operativer Durchführungskontrolle und operativer Überwachung) können, in dem entwickelten Modell zum strategisch-operativen Risiko-Controlling, als PDCA.Zyklus dargestellt werden.

Der strategische Teil des strategisch-operativen IT-Security-Managements soll auf die Optimierung der Effektivität des IT-Security-Managements, und der operative Teil des strategisch-operativen IT-Security-Managements auf die Optimierung der Effizienz des IT-Security-Managements ausgerichtet werden.

Das strategisch-operative IT-Security-Management(system) wird mithilfe der Komponenten (strategische und operative) Prämissenkontrolle, (strategische und operative) Durchführungskontrolle und (strategische und operative) Überwachung eines entsprechenden Performance-Managements als dem klassischen IT-Security-Managementprozess übergeordneter (und diesen integrierenden) Baustein konzipiert.

Der strategische Teil des strategisch-operativen IT-Security-Managements startet mit der Phase Plan auf Ebene der strategischen Sichtweise, eigene Handlungsmöglichkeiten/Flexibilität/Handlungsbefähigung: und kommt nach der Phase Act auf diese Ebene zurück.

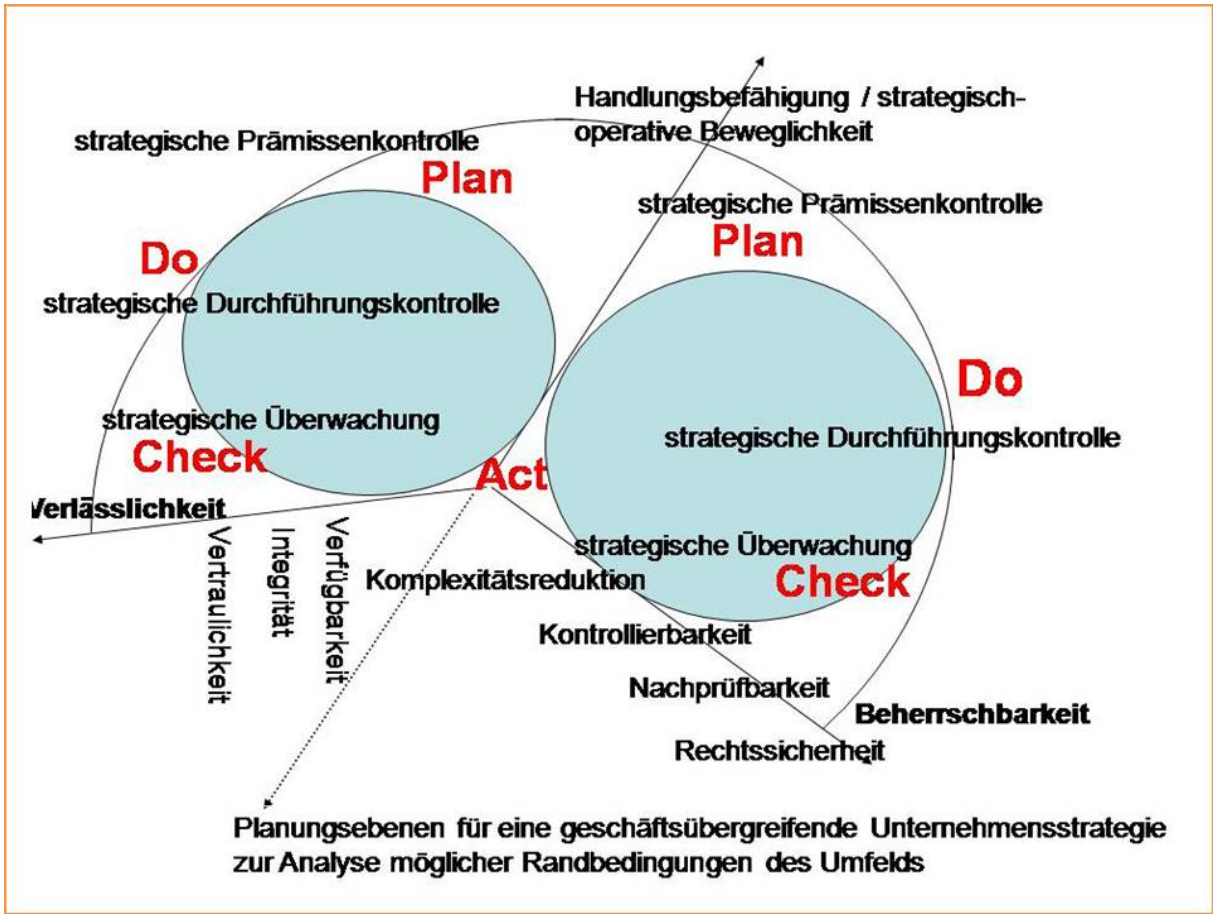


Abb. 22 Strategischer Teil des strategisch-operativen IT-Security-Managements

Über die Komponenten strategische Prämissenkontrolle, strategische Durchführungskontrolle und strategische Überwachung werden direkte Risiken im Kontext Handlungsbefähigung/strategisch-operative Beweglichkeit (z. B. aufgrund mangelnder Flexibilität des Managements) in den Kontext der IT-Sicherheit der für die Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit relevanten Systeme bzw. zu implementierenden Maßnahmen abgebildet.

Der operative Teil des strategisch-operativen IT-Security-Managements startet mit der Phase Plan auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen und kommt nach der Phase Act auf diese Ebene zurück.

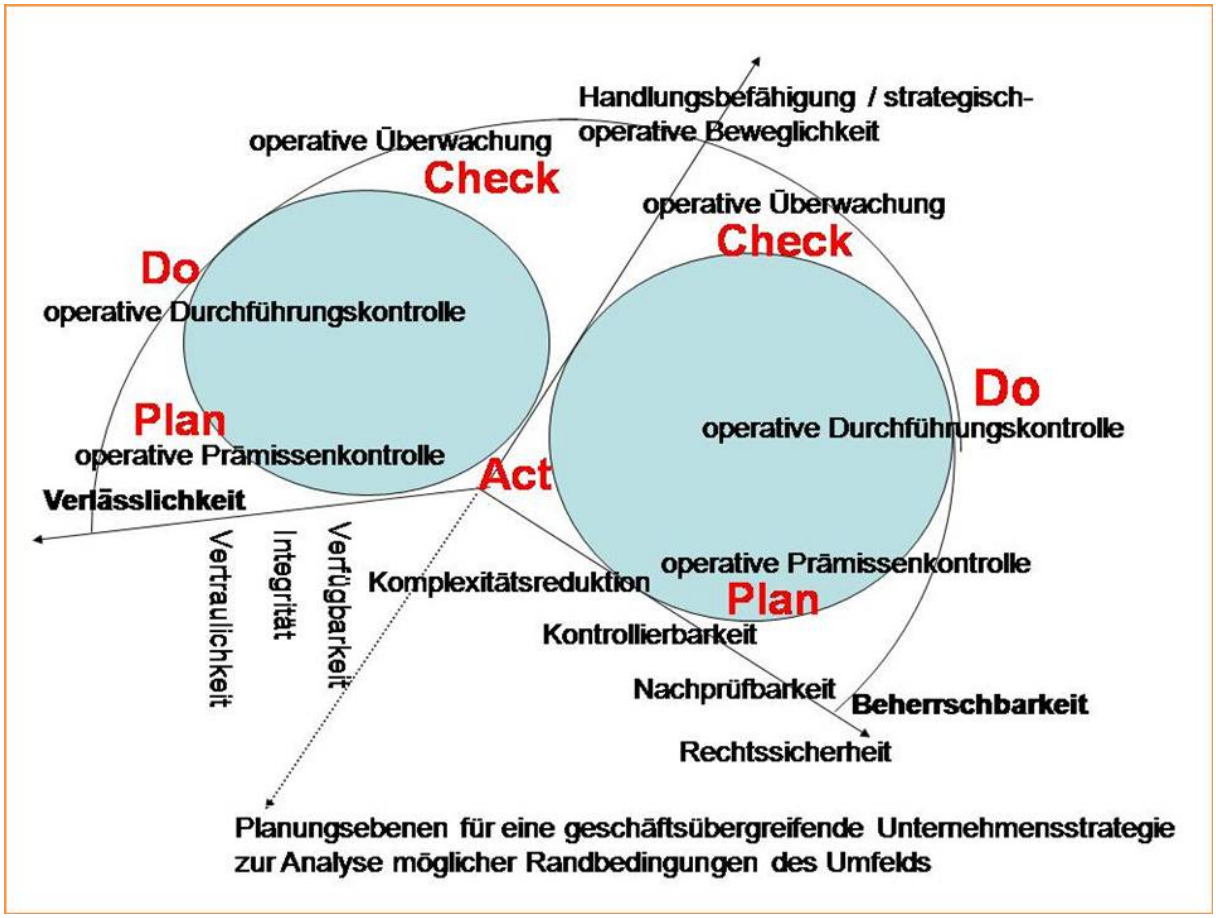


Abb. 23 *Operativer Teil des strategisch-operativen IT-Security-Managements*

Über die Komponenten operative Prämissenkontrolle, operative Durchführungskontrolle und operative Überwachung werden Risiken im Kontext der IT-Sicherheit der für die Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit relevanten Systeme bzw. zu implementierenden Maßnahmen in den Kontext Handlungsbefähigung/strategisch-operative Beweglichkeit abgebildet.

Das strategisch-operative Risiko-Controlling (mit der Abbildung des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in die auf das System bezogene Kontextseite der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse) entwickelt sich so zum Rahmen für den gesamten IT-Security-Management-Prozess zur Ausrichtung auf das Erreichen und die Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit (bei der Umsetzung der IT-Security-Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses, bzw. Abstimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander).

Dazu sind die Komponenten des strategischen Performance Managements (strategische Prämissenkontrolle, strategische Durchführungskontrolle und strategische Überwachung) und die

des operativen Performance Managements (operative Prämissenkontrolle, operative Durchführungskontrolle und operative Überwachung) im – auf die strategisch-operative Beweglichkeit/Handlungsbefähigung abzielenden – Modell des strategisch-operativen Risiko-Controllings entsprechend zu gestalten:

Die (strategische und operative) Prämissenkontrolle hat die, auch zukünftige Gültigkeit der Prämissen der Planung zu bestimmen. Prämissen der Planung sind die Annahmen, wie relevant die Konformität mit Ordnungsmäßigkeitsvorgaben ist, und beziehen sich auf die Relevanz und Anwendbarkeit der festgelegten Methoden, Standards, Tools und Best Practices zur Erreichung des Ziels der Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit (bei der Umsetzung der IT-Security-Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses, bzw. Abstimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander), sowie die Kritikalität/Sensitivität entsprechender Sachwerte und Prozesse.

Die (strategische und operative) Durchführungskontrolle betrifft die Umsetzung der Planung/Durchführung des Vorhabens (Do), d. h. die Durchsetzung/Implementierung der Handlungsbefähigung/strategisch-operativen Beweglichkeit (bei der Umsetzung der IT-Security-Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses, bzw. Abstimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander). Dazu sind Risiken für die Umsetzung der Planung und die Erreichung des Ziels der Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit aufzudecken: Risiken im Kontext Handlungsbefähigung/strategisch-operative Beweglichkeit (z. B. aufgrund mangelnder Flexibilität des Managements) sind von der strategischen Durchführungskontrolle aufzudecken. Für diese Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit sind aber auch bestimmte Systeme bzw. zu implementierende Maßnahmen relevant. Risiken bezüglich dieser Systeme bzw. zu implementierenden Maßnahmen werden in den Kontext der Handlungsbefähigung/strategisch-operativen Beweglichkeit abgebildet. Dazu hat die operative Durchführungskontrolle im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen mögliche Risiken für die notwendige Verlässlichkeit und Beherrschbarkeit der für die Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit (bei der Umsetzung der IT-Security-Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses, bzw. Abstimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander). relevanten Systeme bzw. zu implementierenden Maßnahmen aufzudecken.

Die (strategische und operative) Überwachung betrifft die Erfolgskontrolle/Überwachung der Zielerreichung (Check), d. h. die Überwachung der Durchsetzung/Implementierung der Hand-

lungsbefähigung/strategisch-operativen Beweglichkeit (bei der Umsetzung der IT-Security-Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses, bzw. Abstimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander). Zur Gewährleistung dieser Handlungsbefähigung/strategisch-operativen Beweglichkeit sind bestimmte Sachwerte und Prozesse kritisch sowie Methoden, Standards, Tools und Best Practices als relevant und anwendbar zu bestimmen. Die (strategische und operative) Überwachung hat zu gewährleisten, dass Fehleinschätzung, wie kritisch und sensitiv die Sachwerte und Prozesse sind – orientiert am strategischen Ziel der Handlungsbefähigung – sowie der Relevanz und Anwendbarkeit der festgelegten Methoden, Standards, Tools und Best Practices aufgedeckt werden. Denn aufgrund dieser Nichtaufdeckung der Fehleinschätzungen der Kritikalität/Sensitivität werden kein Anpassungsbedarf der implementierten Maßnahmen zum Erreichen und zur Gewährleistung dieser Handlungsbefähigung/strategisch-operativen Beweglichkeit evaluiert und somit auch die implementierten Maßnahmen nicht angepasst.

Mit der Evaluierung des Anpassungsbedarfs der implementierten Maßnahmen zum Erreichen und zur Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit und der Anpassung der implementierten Maßnahmen erfolgt die Beseitigung von erkannten Mängeln und Schwächen/Optimierung und Verbesserung (Act). Dies erfolgt sinnvollerweise an den Systemen, dessen Verlässlichkeit und Beherrschbarkeit unmittelbar die Handlungsbefähigung/strategisch-operativen Beweglichkeit beeinflusst.

Im Folgenden wird zunächst betrachtet, welche Kosten/Nutzen-Vorteile ein (eventuell wie beschrieben erweitertes) IT-Security-Management bringt, und ob und wann entsprechende Engagements (z. B. als IT-Risk-Assessment) angemessen sind.

5.2 Nutzen/Kosten und Angemessenheits-Betrachtungen bezüglich Security-Engagements

Ziel der Optimierung des Verhältnisses Nutzen/Kosten ist entweder bei gleichem Nutzen die Kosten zu reduzieren oder bei gleich bleibenden Kosten den Nutzen zu erhöhen.

Um den Einsatz von Technologien zu evaluieren, die Kosten alternativer Möglichkeiten zu vergleichen, benutzen Unternehmen zur Abwägung von Investitionsentscheidungen das Total Cost of Ownership (TCO) -Verfahren.

Dabei werden alle Kosten, die über einen bestimmten Zeitraum anfallen (Investitions-, Betriebs- und sonstige Kosten) insgesamt und der jährliche Durchschnitt ausgewiesen.

Festgestellt werden die Gesamtkosten des Besitzes und des Betriebs von Hard- und Software. Zu den sonstigen Kosten gehören Kosten der Anpassung und Integration von Rechnern und Programmen und die Kosten, die die Rechner indirekt auslösen.[1]

Dieses Verfahren betrachtet aber nur die Kosten und in keiner Weise den wirtschaftlichen Nutzen, der durch die Investition generiert wird. Um den Wert einer Investition zu ermitteln, werden finanzmathematische Verfahren wie die Kapitalwertmethode angewandt. Die wesentlichen Ergebniskennzahlen dabei sind Return on Investment und Amortisationsdauer.

Um über den Nutzen der Gerätschaften und Business-Programme etwas aussagen zu können, können die Abläufe im Unternehmen analysiert werden. Eine Abweichung der tatsächlichen Abläufe von den idealisierten Abläufen wird als Störfaktor mit Kosten hinterlegt. Damit ist man in der Lage, eine Verbesserung der Produktivität als Nutzenzufluss/Kostenersparnis, etwa in einem schnellen Return on Investment einer angeschafften Software festzustellen.[2] So erweitert die Gartner-Group das TCO-Modell durch ihr TBO (Total Benefit of Ownership)-Konzept. Einzubeziehende Benefits für PDAs (Personal Digital Assistent) sind z. B. [3]

- geringere Fehlerquote bei der Datenerfassung,
- beschleunigte mobile Prozesse,
- höhere Erreichbarkeit der Mitarbeiter und
- Mitarbeiterzufriedenheit.

Auch die in die IT-Sicherheit getätigten Investitionen und zum Aufrechterhalten des gewünschten Sicherheitsniveaus erforderlichen Aufwendungen müssen wirtschaftlichen Erwägungen genügen. Die Bewertung der Wirtschaftlichkeit von Sicherheitsinvestitionen erfordert, sich damit zu beschäftigen, [4]

- welche Auswirkungen auf den IT-Einsatz neue Technologien haben,
- welchen Risiken die schützenswerten Objekte – Daten, Software, Hardware – ausgesetzt sein könnten und
- wie im Schadensfall den Folgen für die Kontinuität der Leistungserbringung in den Wertschöpfungsprozessen vorgesorgt wird.

Wirtschaftlichkeit der IT-Sicherheit verlangt, das erforderliche Sicherheitsniveau mit minimalen Kosten herzustellen. Voraussetzung hierfür ist – z. B. in Anlehnung an das Grundschutzhandbuch des BSI – einen Mindeststandard für die eingesetzten IT-Komponenten, -

[1] vgl. Deininger, Olaf (2005)
[2] vgl. Deininger, Olaf (2005)
[3] vgl. Gadatsch, Andreas (2004), S.94
[4] vgl. Kruth, Wilhelm (2004), S.6

Systeme und –Anwendungen zu definieren, und die so vorgegebenen Sicherheitsanforderungen mit angemessenen Sicherheitsmaßnahmen abzudecken. Bei sensitiven Anwendungen, bei denen dieser Mindeststandard nicht ausreicht, sind zusätzliche Risikoanalysen durchzuführen.[1]

Angemessen heißt, vernünftige Investitionsentscheidungen bei der Anwendung von Gegenmaßnahmen für gefundene Verwundbarkeiten zu treffen. Dazu kann etwa der materielle oder immaterielle Wert der zu schützenden Systeme oder die Wichtigkeit/Kritikalität der entsprechenden Prozesse herangezogen werden. Eine „gesunde“ Sicherheitspolitik bestehend aus sinnvollen Gegenmaßnahmen, Verhaltensregeln und Prozeduren sind vernünftige, meist kostenwirksame Mittel, um die Risiken einer Verwundbarkeitslandschaft zu reduzieren.[2]

Ein angemessenes IT-Sicherheitsniveau ist in erster Linie abhängig vom IT-Sicherheitsmanagement und erst in zweiter Linie von einzelnen technischen Maßnahmen.[3] Als Ergebnis von Sicherheitsmaßnahmen soll eine Risikominimierung erreicht werden. Dennoch sind Schäden nicht auszuschließen. Daher ist die Effektivität von Informationssicherheit üblicherweise nicht messbar. Eine klassische Amortisation von Investitionen in Informationssicherheit (Amortisationsdauer = ursprünglicher Kapitaleinsatz/ (Gewinn bzw. Kostenersparnis pro Jahr + jährliche Abschreibung)) lässt sich nur herleiten, wenn eine Kostenersparnis nachgewiesen werden kann.

Im Allgemeinen hat eine Wirtschaftlichkeitsberechnung einerseits zu beschreiben, wo die Schwachstellen des derzeitigen Prozesses liegen und andererseits, wie zu deren Beseitigung positive Wirkungen alternativer Maßnahmen genutzt werden können. Die Wirtschaftlichkeit einer Maßnahme lässt sich dabei bestimmen als dessen Effekt auf Kosten und Qualität (gemessen am Anteil zur Nutzenerbringung) des Geschäftsprozesses bezogen auf die Kosten der Maßnahme. [4] Die Wirtschaftlichkeit der Business Intelligence (BI) umfasst auch die Priorisierung von Investitionsentscheidungen, die Bewertung des Ist-Zustands und die Ableitung eines Verbesserungspotenzials.[5]

Ein Return on Security Investment (RoSI) wird definiert als Differenz aus dem Nutzen, der durch die IT-Sicherheitsmaßnahmen erzielt wird und den Kosten für Implementierung und Betrieb der notwendigen IT-Sicherheitsmaßnahmen. Im von der University of Idoha entwickelten Rechenmodell wird als Nutzen die erwartete Ersparnis durch Reduzierung der

[1] vgl. Herweg, Ralf (2001)
[2] vgl. Schneier, Bruce (2000), S.277-278
[3] BSI (2006), S.17
[4] vgl. Zarnekow, Rüdiger (2005), S.2,5
[5] vgl. Funk-Kadir, Thomas (2006)

Schadensbeseitigungskosten betrachtet.[1] Es scheint jedoch unmöglich, eine „erwartete Ersparnis durch Reduzierung der Schadensbeseitigungskosten“ sinnvoll anzusetzen, wenn man Schadensereignissen im Bereich der IT-Sicherheit keinen Erwartungswert zuordnen kann. Zudem investiert man ja in Implementierung und Betrieb der notwendigen IT-Sicherheitsmaßnahmen, um das Schadenspotenzial auf Null zu reduzieren. Wenn man davon ausgeht, dass ein gewisses Sicherheitsniveau vorhanden ist, und man investiert in verbesserte Sicherheitsmaßnahmen, so ist nur mit ungerechtfertigtem Aufwand entscheidbar, ob ein verhindertes Schadensereignis (selbst wenn man Nicht-Ereignisse betrachten könnte) den vorher bereits vorhandenen oder den verbesserten Sicherheitsmaßnahmen zuzuordnen ist.

Sinnvollere Erwägungen bei Kosten-Nutzen-Analysen umfassen die Gegenüberstellung mit den Zielen der Geschäftsprozesse bei verschiedenen Geschäftsmöglichkeiten.[2]

Der Nutzen der IT liegt darin, die Prozesse/Anwendungen des Unternehmens effizienter zu gestalten, etwa durch Konsolidierung von dezentralen Anwendungen mit überlappenden Anforderungen auf eine zentrale Plattform (z. B. Portal). Es ist jedoch schwer monetär darzustellen, wenn eine Anwendung „schneller“, „besser“ oder „effizienter“ ausgeführt wird, und daraus ertragswirksame Potenziale abzuleiten.[3] Im Bereich der Informationstechnologie (und damit auch der IT-Security) liegt die Herausforderung darin, Nutzenfaktoren, welche sich aus der Unterstützung von Geschäftsprozessen ergeben, z. B. in Segmenten wie Mitarbeiterproduktivität oder Ertragssteigerung durch höhere Kundenzufriedenheit zu identifizieren und zu bewerten.[4]

Höchste Kundenzufriedenheit und Kundenorientierung sind nur zu erreichen, indem die Rahmenbedingungen dafür im eigenen Unternehmen und im Binnenverhältnis der Partner ständig überprüft und optimiert werden. Um diesen permanenten Wandel zu meistern, übernimmt in Projekten zur Neustrukturierung oder Neuausrichtung einer Organisation ein professionelles Change Management die Aufgabe, einen möglichst rational und emotional reibungslosen Ablauf aller notwendigen Prozessschritte sicher zu stellen. Nur so gelingen erfolgreiche Geschäftsmodelle, die unterstützende Geschäftsprozesse zeitnah implementieren, jederzeit kostenadäquate Leistungen bereitstellen, und sich somit dem Wettbewerbs- und Kostendruck ihrer Kunden anpassen.[5] Um die sich daraus auch ergebenden wechselnden Anforderungen an Rechenleistung und IT-Infrastruktur jeweils aktuell anzupassen, stellen zu-

[1] vgl. Gadatsch, Andreas (2003), Kap.6.6.6
[2] vgl. Wieczorek, Martin (2003), S.29,30
[3] vgl. Funk-Kadir, Thomas (2006)
[4] vgl. Pobbig, Heiko (2005)
[5] vgl. Mallow, Birgit (2005)

nehmend externe Unternehmen IT- und TK-Kapazitäten zur Verfügung. Ehemals an die Hardware und IT-Infrastruktur gebundene Fixkosten werden so zu variablen Kosten für das Unternehmen, das dieses sog. Outtasking in Anspruch nimmt.[1]

Die IT-Sicherheit kann die Kundenzufriedenheit diesbezüglich also insbesondere über die Absicherung des „professionellen“ Change Managements fördern. Change Management werde dabei wie in ITIL gesehen als die Entwicklung und Umsetzung geeigneter Strategien, um das Unternehmen den zu erwartenden Veränderungen im Unternehmensumfeld anzupassen. Die IT-Sicherheit hat die Sicherheit der vom Change Management bereitgestellten Methoden und Verfahren für Veränderungen vor allem der IT-Infrastruktur zu gewährleisten. Das operative Security Management hat die Aufgabe, die Sicherheitsrelevanz der Änderungen festzustellen.

Zur Behebung von Sicherheitsrisiken der IT-Infrastruktur werden Präventivmaßnahmen zum physischen Schutz von Installationen durchgeführt. Dies kann als Anpassungsprozess an die Umgebung (in Form des Risikoumfelds der IT-Infrastruktur) gesehen werden. Im Rahmen eines u. a. auf Risikoakzeptanz abzielenden Change Managements muss dieser (im in Kap. 5.1.1.4 entwickelten Modell) die Bedingung erfüllen, dass die Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in die auf das System bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume zu einer größeren Handlungsbefähigung führt. Insbesondere muss das in ein solches Change Management eingebettete strategisch-operative IT-Security-Management die für den IT-Security-Prozess definierten Risikokomponenten Prämissenrisiko, Umsetzungsrisiken, Überwachungsrisiko analysieren, entsprechend bewerten und steuern.

Revision und Controlling der IT-Security werden so gesehen, dass Analyse, Bewertung und Steuerung von Prämissenrisiko, Umsetzungsrisiken, Überwachungsrisiko so zu ermöglichen sind, dass das Ziel der Unterstützung strategisch-operativer Handlungsspielräume bei der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse erreicht werden kann. Betrachtet wird dabei die Bedeutung von Risiken der IT-Security für die Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse. Diese organisatorische Abwicklung der Geschäftsprozesse hat die Unterstützung strategisch-operativer Handlungsspielräume bezüglich der mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens zum Ziel. Eine mangelnde IT-Sicherheit

[1] vgl. Lutz, Harald (2005)

kann die ordnungsgemäße organisatorische Abwicklung der Geschäftsprozesse beeinträchtigen. Dies wird insbesondere dann der Fall sein, wenn fehlende Sicherheitseigenschaften Optionen in den IT-Projekten, mit denen die Geschäftsprozesse und Geschäftsmodelle des Unternehmens umgesetzt und optimiert werden sollen, negativ beeinflussen. Zur Unterstützung/Herstellung der Handlungsbefähigung ist dafür zu sorgen, dass Optionen in den IT-Projekten nicht negativ beeinflusst (oder sogar nicht mehr wählbar) werden. Das abstrakteste IT-Security-Projekt ist die korrekte Bestimmung der Anwendbarkeit und die konsequente Umsetzung bestehender Methoden, Standards, Tools und Best Practices der IT-Sicherheit. Die IT-Security hat zu gewährleisten, dass keine fehlenden Sicherheitseigenschaften Optionen/Alternativen bei der Umsetzung bestehender Methoden, Standards, Tools und Best Practices negativ beeinflussen.

Das IT-Security-Management hat die in Optionen ausgedrückte Handlungsbefähigung bei der Umsetzung von IT-Projekten abzusichern. Dies kann dadurch erfolgen, den IT-Security-Prozess/das IT-Security-Management auf die Absicherung der Priorisierung und Umsetzung von IT-Projekten auszurichten, und die Risikokomponenten Prämissenrisiko, Umsetzungsrisiken, Überwachungsrisiko zu analysieren, entsprechend zu bewerten und zu steuern. Die Effizienz eines solchen IT-Security-Managements liegt darin, inwieweit die Absicherung der Priorisierung und Umsetzung von IT-Projekten gelingt. Die Absicherung der Priorisierung und Umsetzung von IT-Projekten sei gleichzeitig als der ex-ante Nutzen eines solchen IT-Security-Managements definiert.

6 ex-post und ex-ante Bewertung der IT-Security

Bewerten (bezüglich angestrebter Ziele) kann als Vergleichen und Beurteilen von Anforderungshöhen und Erfüllungsgraden definiert werden. Risikobewertung wird als „Verarbeitung von Daten zu aussagekräftigen Informationen“ (der Risikolage des Unternehmens) definiert.[1] Zielbezug wäre hier z. B. die angestrebte Effektivität und Effizienz des Risikomanagements. Zur Quantifizierung eines möglichen, aus einem Risikoeintritt resultierenden Schadens werden etwa der maximal mögliche Schaden und der erwartete Höchstschaden (der im Gegensatz zum maximal möglichen Schaden das Funktionieren risikopolitischer Maßnahmen berücksichtigt) berechnet.[2] Das Bewerten wird auf der Basis von Anforderungen vorgenommen, die die Organisationsstrukturen und die technischen Einrichtungen erfüllen müssen.

Der Wertbegriff kann als Normwert in dem Sinne definiert werden, dass hierunter „alle Wertinformationen verstanden werden, die aufgrund von Normen aus dem zu bewertenden Objekt abgeleitet werden können und die an einen sich für diesen Ausschnitt der Realität interessierenden Adressaten gerichtet sind“.[3] Die Ausprägung der Variable Wert richtet sich nach den Ausprägungen anderer charakteristischer Merkmale des zu bewertenden Sachverhalts. Zum Ermitteln des Wertes muss der Beitrag des zu bewertenden Objekts zum Erreichen beschreibbarer und fixierbarer Dimensionen bekannt sein. Die Basis für das Bewerten bildet das Ermitteln der Ausprägungen dieser vereinbarten Dimensionen.[4]

Im Bereich der IT-Sicherheit sind aber Maße wie „maximal möglicher Schaden“ oder „erwarteter Höchstschaden“ nicht unproblematisch. Hier ist eine objektive Quantifizierung nicht möglich, das Risiko wird subjektiv bewertet (existenzbedrohend, schwerwiegend, mittel, gering, unbedeutend).

Um Sicherheitsaussagen für ein IT-/IV-Gesamtsystem treffen zu können, sind neben den IT-Sicherheitsmaßnahmen die IT-Installationen unter besonderer Berücksichtigung der in der Regel anzutreffenden Heterogenität, Komplexität und insbesondere Dynamik solcher IT-/IV-Systeme zu überprüfen. Zudem sind Abhängigkeiten und gegenseitige Beeinflussung vor allem in vernetzten und verteilten Systemen (als Zusammenschaltung von Einzelkomponenten) zu untersuchen. Das Gesamtsystem kann dann nicht mehr ohne weiteres als Verbindung von Teilnetzen unterschiedlicher Zuständigkeitsbereiche betrachtet werden.

[1] vgl. Romeike, Frank (2004):, S.287
[2] vgl. Romeike, Frank (2004):, S.290
[3] Hölscher, Reinhold (2002), S.259
[4] vgl. Pietsch, Thomas (2003), S.19

Ein Bewertungsmodell soll unabhängig vom Bewerter zu gleichen, zumindest zu ähnlichen Ergebnissen kommen. Es soll objektiv, praktisch anwendbar und nachvollziehbar sein. Bewertungsverfahren basieren auf einem strukturierten Ansatz oder einem strategischen Ansatz. Beim strukturierten Ansatz sollen sie so aufgebaut sein, dass sie die Wirkungen von Maßnahmen strukturiert zusammentragen, dokumentieren und somit beurteilbar machen.

Ein Konzept, das objektiv, praktisch anwendbar und nachvollziehbar mehrere Zielkriterien in eine Entscheidung einbezieht und zu einer Punktzahl verdichtet, sind Scoringmodelle. In diesem mehrdimensionalen Bewertungsverfahren werden die einzelnen Bewertungskriterien mit Punktbewertungen und Gewichtungen versehen und anschließend zu einem Gesamtwert aggregiert. Dazu sind Skalen für Messdimensionen sowie Messgrößen festzulegen. Damit die Beurteilungen der einzelnen Kriterien unabhängig vom Beurteiler werden, sollen Mindestanforderungen in Form von Szenariobeschreibungen hinterlegt werden. Im Rahmen der Beurteilung spielen zudem Ausschlusskriterien eine wichtige Rolle. Zur Berücksichtigung solcher Ausschlusskriterien wird die Festlegung eines Katalogs von Knock-Out Kriterien vorgeschlagen, der die Herabstufung auf eine bestimmte Bewertungskategorie bestimmt.[1]

Beim strategischen Ansatz sollen Bewertungsverfahren Beurteilungshinweise für den Beitrag einer Maßnahme zur Erreichung der strategischen Zielsetzung des Unternehmens geben können.[2] So sollte ein optimales Instrument zur Messung der IT-Effizienz eine mehrdimensionale Messung sein, die Abhängigkeiten zur strategischen Ebene berücksichtigt.[3]

Dies wird auf die Unterstützung strategisch-operativer Handlungsspielräume bei der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse ausgerichtet. Die Verbindung zur Ebene der IT-Security ist die Abbildung des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in diesen Kontext. Als Maßnahmen sind IT-Security-Projekte zu betrachten, welche zur Umsetzung bzw. Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens notwendig sind.

Zudem wird eine ex-post (Vergangenheit orientierte) und ex-ante (Zukunft gerichtete) Bewertung unterschieden. In Zusammenhang mit dem IT-Security-Management soll im weiteren Verlauf auf eine auf dem strategischen Ansatz basierende ex-ante Bewertung fokussiert werden.

[1] vgl. Reichling, Peter (2003), S.211-213
[2] vgl. Pietsch, Thomas (2003), S.51
[3] vgl. Jekel, Nicole (2006), S.25

6.1 Messbarkeit von Sicherheit/Bewertungsobjekt, Bewertungsmethode

Um die Sicherheit in einem Unternehmen zu kontrollieren, muss die Sicherheit zunächst messbar gemacht werden. Dies kann z. B. mit der Aufnahme von Erfüllungsgraden geschehen, multipliziert mit einem der Kritikalität/Wichtigkeit angemessenen Gewichtungsfaktor.[1]

Insbesondere beinhaltet das IT-Service-Management [2] die Forderung, Leistungen messbar und bewertbar zu machen, denn was sich nicht messen lässt, kann nicht (oder kaum) verbessert werden.

Auch der ISO 27001 stellt Anforderungen bezüglich der Messbarkeit von Sicherheit. Diese Anforderungen haben die Messbarkeit der Effizienz von Maßnahmen zum Ziel: In den Anforderungen zur Implementierung und Operation des ISMS (Informationssicherheits-Managementsystem) wird gefordert, dass Maße zur Bestimmung der Effizienz implementierter Maßnahmen definiert und benutzt werden. Auch im SOX (Sarbanes-Oxley-Act) hat die Messbarkeit eine hohe Bedeutung. So müssen die eingesetzten Kontrollverfahren nachweisbare Resultate liefern. Insbesondere ist ein effizientes Risikomanagement entsprechend auszugestalten.[3]

Risiken wird eine Messbarkeit zugestanden, wenn ein Vergangenheitsbezug gegeben ist. Annahmen über künftige Risiken werden als Schätzung bezeichnet.[4] Basis zur Quantifizierung von Risiken sind die ursachenbezogene Komponente (bezieht sich auf die Möglichkeit des Eintritts eines Ereignisses) und die wirkungsbezogene Komponente (bezieht sich auf die Möglichkeit der Zielverfehlung). Als Folge der Beschäftigung mit der Messung von Risiken kann es sich dabei als sinnvoll erweisen, bestimmte Unternehmensaktivitäten mit Hilfe von Realoptionsmodellen zu bewerten. Dabei werden mit Risikokennzahlen und Risiko adjustierten Ergebniskennzahlen oder Performancemassen Handlungsalternativen bewertet.[5] Als Ziel der Quantifizierung operationeller Risiken ist zudem die Verbesserung interner organisatorischer Abläufe zu nennen.[6]

[1] vgl. Bursch, Daniel (2005), S.117,118
[2] vgl. Sommer, Jochen (2004)
[3] vgl. Coester, Ursula/Hein, Matthias (2005):, S.92
[4] vgl. Ibers, Tobias (2005), S.113
[5] vgl. Merbecks, Andreas (2004), S.104-106
[6] vgl. Romeike, Frank (2005), S.258

Eine triviale Möglichkeit der Messbarkeit von Leistungen ist die Auslagerung der Verantwortlichkeit: Werden für die Security-Infrastruktur sog. Managed Services mit entsprechenden SLAs (Service Level Agreements) vereinbart, so wird die Leistung messbar und bewertbar.[1] SLAs sollten dabei nicht nur die Qualität der Ressourcen (z. B. Verfügbarkeit von Netzen und Servern), sondern auch die Qualität aus Sicht des Anwenders (z. B. Dauer von Geschäftstransaktionen, Laufzeiten von E-Mails oder Reparaturzeiten bei Fehlern) beschreiben.[2]

Im Rahmen der Erhebung der sicherheitsrelevanten Betriebsanforderungen bei der Informationssystem-Schutzbedarfsanalyse werden als messbare Sicherheitsziele im Hinblick auf die Verfügbarkeit z. B. die Betriebszeit, die maximal tolerierbare Ausfalldauer, die Häufigkeit von Ausfällen und die minimale Zeit zwischen zwei Ausfällen definiert.[3]

Schicht	Beschreibung
Übergreifende Aspekte	Enthält Sicherheitsaspekte, die für sämtliche oder große Teile des IT-Verbundes gleichermaßen gelten und zugehörige Regeln. Wichtige Bausteine sind das IT-Sicherheitsmanagement, Personal oder das Notfallvorsorge-Konzept.
Infrastruktur	Diese Schicht umfasst Sicherheitsaspekte zu baulichen und technischen Gegebenheiten. Sie führt Aspekte der Infrastruktursicherheit zusammen für Räume, Gebäude, Haustechnik etc.
IT-Systeme	Bezieht sich auf einzelne oder vernetzte Systeme eines IT-Verbundes. Diese Schicht bündelt Sicherheitsmaßnahmen für einzelne Komponenten.
Netze	Diese Schicht enthält Sicherheitsmaßnahmen und Bausteine, die sich nicht auf einzelne Systemkomponenten, sondern auf entsprechende Netzkomponenten und Verbindungen beziehen.
Anwendungen	Diese Schicht umfasst ausschließlich die Sicherheitsmaßnahmen für einzelne Anwendungen, die im IT-Verbund genutzt werden.

(Quelle: Humpert, Frederik (2005), S.9)

Abb. 24 Schichten im Grundschutzmodell

Im Allgemeinen erfordert Sicherheit die konsequente Umsetzung bestehender Methoden, Standards, Tools und Best Practices. So soll Sicherheit z. B. auch über den Grundschutz messbar und überprüfbar gemacht werden. Um dies IT-Objekt- oder IT-Anwendungs-

[1] vgl. Sehlhorst, Michael (2004)
[2] vgl. Zarnekow, Rüdiger (2005), S.8
[3] vgl. Müller, Klaus-Rainer (2003) , S.49

übergreifend zu machen, wird im IT-Grundschutz ein Schichtenmodell gebildet. Dieses Modell soll alle relevanten und notwendigen Punkte für eine vernünftige Beschreibung des eigenen IT-Umfelds enthalten. Diese Schichten sollen eine modellhafte Sicht auf den gesamten IT-Verbund, also die Gesamtheit der IT-Objekte ermöglichen. Dazu können auf den einzelnen Schichten Maßnahmen gebündelt, strukturiert und unter gleiche Oberelemente gefasst werden. Die Schichten im Grundschutzmodell sind „Übergeordnete Aspekte", „Infrastruktur", „IT-Systeme", „Netze" und „Anwendungen":[1]

Sämtliche obige Bewertungskriterien dienen im Prinzip nur dem strukturierten Zusammentragen und Dokumentieren der Wirkungen von Maßnahmen und somit mehr der ex-post Bewertung. Im Folgenden geht es im Sinne einer strategischen ex-ante Bewertung um Beurteilungshinweise für den Beitrag einer Maßnahme zur Erreichung der strategischen Zielsetzung des Unternehmens. Bewertungsobjekt ist dann der Erreichungsgrad unternehmerischer Zielsetzung. Die Beurteilungshinweise liefert das Ermitteln der Ausprägungen des Erreichens der Zieldimensionen des IT-Security-Prozesses.

Die Quantifizierung von operationalen Risiken ist dabei kein selbstständiges Ziel. Das übergeordnete Ziel ist die Verbesserung des Managements operationeller Risiken.[2] In diesem Sinne geht es um das Management der Auswirkungen von Risiken der IT-Security auf die Erreichung der strategischen Zielsetzung des Unternehmens.

6.1.1 Erreichungsgrad unternehmerischer Zielsetzung

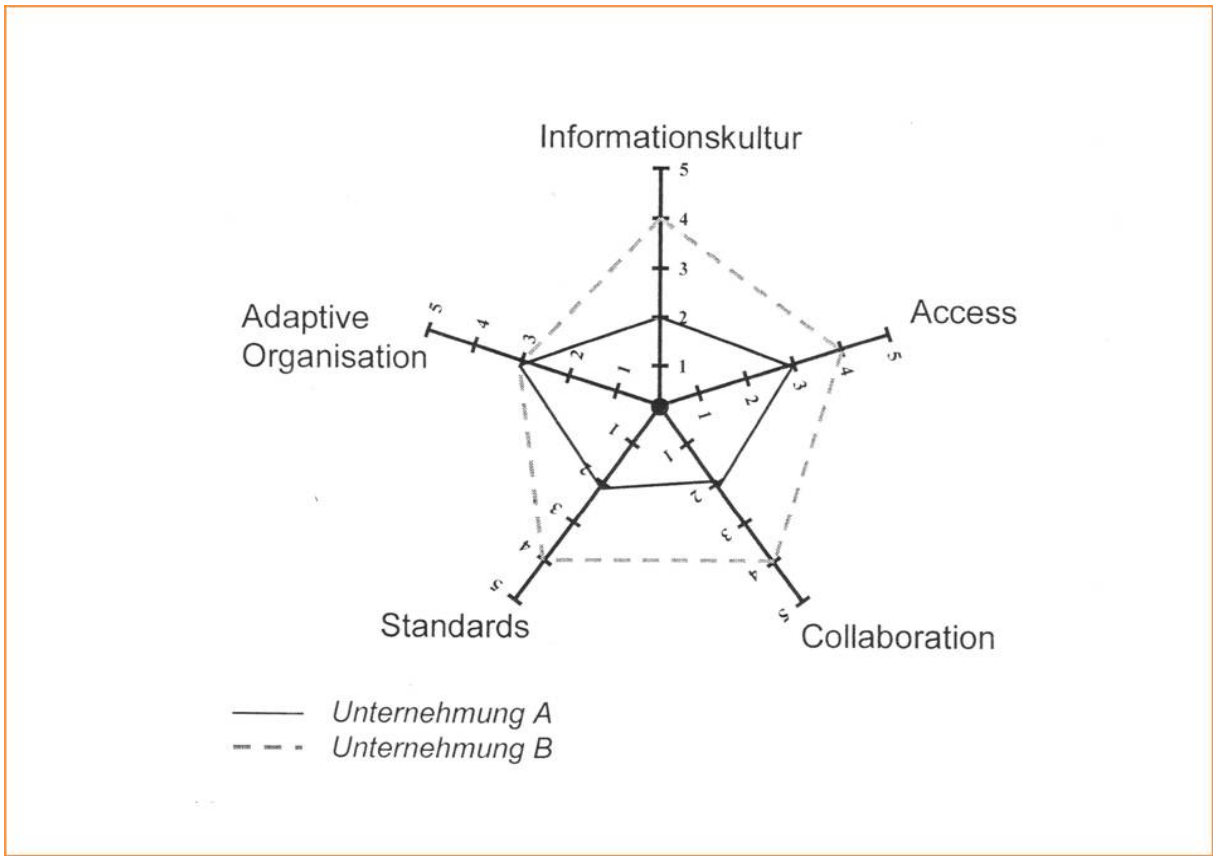
Im Hinblick auf Kostenbewertung und Kostenmanagement von IT-Sicherheitsmaßnahmen sollen IT-Security-Kennzahlensysteme für mehr Transparenz und Handlungssicherheit sorgen. Mit diesen könnten Organisationen ihr Sicherheitsniveau analysieren, transparent machen, bewerten und daraus Handlungsbedarf ableiten.[3]

IT-Risiken lassen sich nicht ohne weiteres antizipieren, eine Datenbasis zur Ableitung kritischer Kennzahlen ist a priori nicht vorhanden. Im Zusammenhang mit der Revision und dem Controlling der IT-Security stehen zukunftsbezogene Nutzenaspekte der IT-Security im Mittelpunkt. Die Optimierung des durch die IT-Security beeinflussbaren Nutzenpotenzials der IT geschieht in der Form, diese Nutzenpotenziale zu maximieren und abzusichern. Letzteres zielt auf die Unterstützung/Herstellung der Handlungsbefähigung ab. Die ex-ante Bewertung

[1] vgl. Humpert, Frederik (2005), S.9
[2] vgl. Romeike, Frank (2005), S.256
[3] vgl. Henze, Detlev/Parthier, Ulrich.(2005)

der IT-Security läuft also auf die Beurteilung der Unterstützung/Herstellung der Handlungsbefähigung zur Absicherung von Nutzenpotenzialen der IT hinaus.

Unternehmen können im Allgemeinen durch eine einfache Analyse von Erfolgsfaktoren eine Bewertung vornehmen. So können Unternehmen oder Abteilungen mithilfe einer einfachen Ist-Analyse z. B. ihre E-Readiness bewerten:[1]



(Quelle: Dietrich, Lothar (2004), S.306)

Abb. 25 Dimensionen zur Bewertung der E-Readiness

Diese Dimensionen sind bezüglich der Untersuchungsgegenstände mit den Planungsebenen für eine Geschäftsfeld übergreifende Unternehmensstrategie verknüpft. Allerdings werden die in diesen Dimensionen im Prinzip zu betrachtenden konkreten Zielvorgaben des IT-Security-Prozesses aufgrund der Ungewissheit der zukünftigen Entwicklungen im Umfeld des Unternehmens und daraus resultierender Ungewissheit über diese Zielvorgaben ersetzt durch die angestrebte strategisch-operative Beweglichkeit/Handlungsbefähigung bei der Umsetzung der Unternehmensstrategie und Abstimmung der Unternehmensziele und der Geschäftsprozesse (auch des IT-Security-Prozesses) aufeinander im Kontext der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse. Der auf der jeweiligen Planungsebene

[1] vgl. Dietrich, Lothar (2004), S.306

zu analysierende (Erfolgs)Faktor ist dann bezüglich der Zielsetzung der Unterstützung der Handlungsbefähigung/strategisch-operativen Beweglichkeit das auf der jeweiligen Ebene relevante Flexibilitätspotenzial (ausgedrückt in Realoptionen).

Bei der Dimension (offene) Informationskultur (und Nutzen bringende Inhalte) geht es um Informationsvorsprünge, d. h., das Streben nach vollkommener Information und „das Management der Informationen über die gesamte Wertschöpfungskette zu beherrschen", Technologie ist der „Enabler" einer solchen Informationskultur. Im Zusammenhang mit dem Management der Informationen über die gesamte Wertschöpfungskette und der Abstimmung der Unternehmensziele und der Geschäftsprozesse aufeinander geht es um die IT-Ressourcen zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse. Diese Dimension kann also mit der Ressourcenebene verknüpft werden.

Beim (massenhaften und einfachen) Access geht es im Zusammenhang mit E-Business um den steigenden Nutzen eines Produkts oder Systems mit seiner zunehmenden Verbreitung (Netzwerkeffekt). So gibt es neben dem Asset Information das Asset Access. Dies ist ein Gegenstand der sozio-technischen Ebene.

Collaboration bedeutet die Kooperation mit Lieferanten oder Kunden, die für bestimmte Teilprozesse bessere Kernkompetenzen haben und als Spezialisten die komplementären Leistungen erbringen. Collaboration ist besonders in Netzwerken ein Erfolgsfaktor. Gerade Webtechnologien ermöglichen effizient die virtuelle Integration und Vernetzung von Unternehmen und die Umsetzung knotenübergreifender Prozessmodelle. Für diese Zusammenarbeit fungieren die E-Technologien als „Enabler". Dies ist ein Gegenstand der Organisationsebene.

Auch die Standardisierung der eigenen Stammdaten, Systeme und Prozesse ist ein Erfolgsfaktor. Sie erleichtert die Entscheidungsfindung und das Management der Infrastruktur. Für Ansatzpunkte zur Erzielung von Wettbewerbsvorteilen ist die Standardisierung der Netzwerke ein wichtiges Gestaltungsprinzip für interne und unternehmensübergreifende Informationsnetzwerke mit effizienten Informationsflüssen. Hier steht die Homogenisierung der vorhandenen Systeme und Technologien im Mittelpunkt. Die Standardisierung betrifft auch die Anforderungen der Partner im (collaborative) Netzwerk; im Extremfall wird der Access zum Netzwerk verwehrt. Die Standardisierung ist u. a. Voraussetzung für den Einsatz innovativer Informationstechnologien (die von einer entsprechenden IT-Security abhängen) für die Unterstützung/Ermöglichung/Sicherung bestehender und neuer Geschäftsprozesse/Geschäftsmodelle, die strategisch-operative Beweglichkeit und Unterstützung/Herstellung der Handlungsbefähigung um Wettbewerbsvorteile und auf den Vorgaben der Unternehmensstrategie basierende Wachstumsmöglichkeiten zu erschließen. Dies wird auf der Geschäftsebene betrachtet.

Bei der Adaptiven Organisation geht es um schnelle Anpassungsfähigkeit; die Integration und Desintegration von Unternehmensteilen müssen IT-gestützt innerhalb kürzester Zeit abwickelbar sein. Hier gestatten Internetsysteme, Organisationsformen virtuell und nicht zwingend auch physisch anzupassen. Dies wird auf der Unternehmensebene betrachtet.

Anhaltspunkte zur Abschätzung der Gefährdung der Unterstützung/Herstellung der Handlungsbefähigung zur Absicherung von Nutzenpotenzialen der IT aufgrund mangelnder IT-Security sind die Risiken für einen adäquaten IT-Security-Prozess. Diese Risiken sind neben den Prämissen- bzw. Selektionsrisiken der Planung (Irrtumsrisiken der Selektions- und Filterkriterien bei der Fokussierung auf die wichtigsten Prämissen der Security-Strategie), zukünftige Security-Strategie-Umsetzungsgefahren. Als sinnvolles Kriterium für Sicherheit bleibt die Bewertung der korrekten Bestimmung der Anwendbarkeit und der konsequenten Umsetzung bestehender Methoden, Standards, Tools und Best Practices. (d. h., wie die Richtlinien und die dazu verwendeten Technologien implementiert und umgesetzt werden).

Diese Methoden, Standards, Tools und Best Practices müssen als relevant und anwendbar bestimmt werden. Eine für den strategischen Ansatz brauchbare Ausgangsbasis für die Bewertung ist die Nützlichkeit eines Mittels zum Erreichen eines Ziels.[1] Ziel in diesem Zusammenhang ist die Unterstützung strategisch-operativer Handlungsspielräume (bezüglich der mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens) bei der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse. Es wäre dann die diesbezügliche Nützlichkeit dieser Methoden, Standards, Tools und Best Practices zu untersuchen.

Das auf das Management der IT-Security übertragene Konzept des strategischen Performance Managements (zum generellen Management zur Operationalisierung der Unternehmensstrategien und –ziele und deren Überführung in ein permanentes Führungssystem) ist die Ausgangsbasis für ein Konzept zum Management zur Operationalisierung der IT-Security-Strategie und deren Überführung z. B. in ein Informationssicherheits-Managementsystem. Die Bewertung der IT-Security würde dann auf die Bewertung der Wirksamkeit (dauerhafte Effizienzverbesserung z. B. durch optimale Ressourcennutzung (Personal, Technik und Organisation) eines solchen Informationssicherheits-Managementsystems hinauslaufen. Es ist zu beurteilen, inwieweit das Informationssicherheits-Managementsystem gewährleistet, dass das Eintreten von Risiken der IT-Security das Erreichen der Unternehmensziele nicht gefährdet. Ausgegangen wird dabei von der betriebswirtschaftlichen Sicht von Risiko als Aus-

[1] vgl. Pietsch, Thomas (2003), S.17

maß, in dem das Erreichen geschäftlicher Ziele oder Strategien durch Ereignisse oder Handlungen/Unterlassungen von innerhalb oder außerhalb des Unternehmens gefährdet ist. Diese Gefährdung bedeutet, dass das Risiko nicht akzeptiert werden kann. Zum Erreichen anpassbarer strategischer Unternehmensziele ist die Unterstützung strategisch-operativer Handlungsspielräume bei der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse eine Voraussetzung. Die Beurteilung wird durch Analyse der Bedeutung der im Zusammenhang mit der Unterstützung strategisch-operativer Handlungsspielräume bei der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse relevanten Risiken der IT-Security möglich. Dies entspricht der Projektion des Kriteriums „gefährlich“/von Risiko allgemein in den Kontext „Handlungsbefähigung trotz Unsicherheit“. Die ex-ante Bewertung der IT-Security bedeutet also eine Analyse der IT-Security relevanten Risiken für die Zielerreichung. Diese Risiken werden im Modell der Abbildung des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in den Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume vom technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen in den Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse projiziert:

Analysiert werden als Risiken für den IT-Security-Prozess die Prämissen- bzw. Selektionsrisiken der Planung (Irrtumsrisiken der Selektions- und Filterkriterien bei der Fokussierung auf die wichtigsten Prämissen der Security-Strategie) und zukünftige Security-Strategie-Umsetzungsgefahren. Aus der Regelkreis-Charakteristik des IT-Security-Prozesses ergab sich, dass sich dieses Risiko aus drei Komponenten zusammensetzt: Planungs-, Umsetzungs- und Überwachungsrisiko bezüglich der Security-Strategie.

Die Planungsrisiken ergeben sich aus Fehleinschätzungen der Kritikalität/Sensitivität der Sachwerte und Prozesse sowie aus Unsicherheiten und Fehleinschätzungen bezüglich der Wirksamkeit z. B. von Maßnahmen. Umsetzungsrisiken resultieren aus unzureichender Handlungsbefähigung bei der Umsetzung der IT-Security-Strategie. Überwachungsrisiken resultieren daraus, dass Fehleinschätzung, wie kritisch und sensitiv die Sachwerte und Prozesse sind – orientiert an der angestrebten Handlungsbefähigung/strategisch-operativen Beweglichkeit – nicht aufgedeckt werden.

6.1.2 Ermitteln der Ausprägungen des Erreichens der Zieldimensionen des IT-Security-Prozesses

IT-Systeme unterstützen die Geschäftsprozesse des Unternehmens und sind Investitionsgüter von strategischer Bedeutung. IT-Sicherheit ist eine wichtige Voraussetzung für den effektiven

und effizienten Einsatz von IT-Systemen. Ein IT-System verliert immer dann an Wert, wenn es einen Geschäftsprozess nicht mehr optimal unterstützt.[1] Die Bewertung der IT-Security im Rahmen des strategischen Ansatzes beurteilt, inwieweit von der IT-Security der für die Unterstützung von Geschäftsprozessen/Enabling von Geschäftsmöglichkeiten eingesetzten IT die Erreichung der entsprechenden Zielsetzungen abhängt.

Organisationen ermitteln ihr Sicherheitsniveau z. B. mittels eines IT-Security-Kennzahlensystems. Es wird sowohl das Sicherheitsgefälle innerhalb der Organisation als auch die Bereiche der Informationssicherheit aufgezeigt, in denen eine Steigerung des Niveaus erfolgen kann. Um eine einheitliche, vergleichbare Definition, Bestimmung und Bewertung zu erhalten, ist entscheidend, dass es auf anerkannten internationalen Normen und Verfahren basiert. Das Kennzahlensystem ist sinnvollerweise in Themenkomplexe zu gliedern, die sich an dieser Norm orientieren.[2]

Die Anforderungen bezüglich der Messbarkeit von Sicherheit haben die Messbarkeit der Effizienz von Maßnahmen zum Ziel: Diese Effizienz bezieht sich bei der auf dem strategischen Ansatz basierenden ex-ante Bewertung auf die Unterstützung strategisch-operativer Handlungsspielräume bei der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse im Zusammenhang mit Nutzenpotenzialen der IT. Es wird also beurteilt, inwieweit die IT-Security der IT-Systeme, welche der Unterstützung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens dienen, zum Erreichen der Zielsetzung Unterstützung der Handlungsbefähigung/strategisch-operativen Beweglichkeit (bei der Umsetzung der Unternehmensstrategie und Abstimmung der Unternehmensziele und der Geschäftsprozesse aufeinander) beitragen. Die Ausgestaltung der IT-Security geschieht über den IT-Security-Prozess. Die Beurteilung der Effizienz basiert auf der Analyse der für den IT-Security-Prozess relevanten Risiken.

In Anlehnung an das Konzept des strategischen Performance Managements wurden als Risiken für den IT-Security-Prozess die Prämissen- bzw. Selektionsrisiken der Planung (Irrtumsrisiken der Selektions- und Filterkriterien bei der Fokussierung auf die wichtigsten Prämissen der Security-Strategie) und zukünftige Security-Strategie-Umsetzungsgefahren betrachtet.

[1] vgl. Hess, Andreas (2004)
[2] vgl. Kirchhoff, Tobias (2005)

Der IT-Security-Prozess enthält eine Planungskomponente bezüglich der IT-Security-Strategie. Wird Security als strategisches Unternehmensziel und die IT-Security-Strategie als geschäftsübergreifende Unternehmensstrategie gesehen, so können die ungewissen zukünftigen Anforderungen an die IT-Sicherheit/IT-Security als Grund für die Unbestimmtheit der Zielvorgabe und Zielerreichung des IT-Security-Prozesses auf den Planungsebenen für eine geschäftsübergreifende Unternehmensstrategie untersucht werden. Diese ergeben sich aus der durch die Kriterien der Sichten Verlässlichkeit (beurteilt nach den Kriterien Verfügbarkeit, Integrität und Vertraulichkeit) und Beherrschbarkeit (beurteilt nach den Kriterien Nachprüfbarkeit und Rechtssicherheit) beeinflussten mangelnden Handlungsbefähigung/Flexibilität/ strategisch-operativen Beweglichkeit bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander. Dies beschränkt die Beurteilung auf die IT-Systeme, welche von der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander betroffen sind. Die auf die Zukunft bezogene Bewertung der IT-Security untersucht dann, inwieweit die IT-Security der betreffenden IT-Systeme zur Erreichung der entsprechenden Handlungsbefähigung/Flexibilität/strategisch-operativen Beweglichkeit auf den Ebenen der Unternehmensplanung beitragen. Angenommen wird dabei, dass die Erreichung der Unternehmensziele/strategisch-operativen Zielsetzungen des Unternehmens eine entsprechende Handlungsbefähigung/Flexibilität/strategisch-operative Beweglichkeit voraussetzt. Die Bewertungsdimensionen der Erreichung der Unternehmensziele/strategisch-operativen Zielsetzungen des Unternehmens sind in diesem Zusammenhang dann die der entsprechenden Handlungsbefähigung/Flexibilität/strategisch-operativen Beweglichkeit.

Beurteilungshinweise für den Beitrag von Security-Maßnahmen zur Erreichung der strategischen Zielsetzungen ergeben sich über eine Analyse der, in dem im Verlauf dieser Arbeit entwickelten Modells zum strategisch-operativen Risiko-Controlling definierten drei Risikokomponenten (Planungs-, Umsetzungs- und Überwachungsrisiko).

6.2 Anwendbarkeit existierender Bewertungsstandards

Die Ziele, die in der IT verfolgt werden, sind neben der Ausrichtung auf die Geschäftsziele und bestmögliche Unterstützung der Geschäftsprozesse die Verbesserung der Servicequalität, die Reduzierung der Servicekosten, die Erhöhung der Liefergeschwindigkeit sowie die Ver-

ringerung von IT-Risiken. Zur gemeinsamen Umsetzung dieser Ziele stehen als Hilfsmittel die Rahmenwerke und Standards CObIT, ITIL und BS 7799/ISO 17799 zur Verfügung.[1]

In der heutigen Economy sind die Geschäftsumfelder primär von Ideen getrieben. Die Fähigkeit, Wissen generieren und nutzen zu können stellt eine größere Wertkomponente dar als die Fähigkeit zur Entwicklung physischer Assets.[2] Nicht Kontinuität, lineare Entwicklungen, und Informationssymmetrien sondern Überraschungen, nicht-lineare Entwicklungen und Informationsasymmetrien sind die Treiber für Fortschritt, die Wertpotenziale schaffen. Investitionen in den Aufbau immateriellen Vermögens erhöhen das Potenzial des Unternehmens zur Erwirtschaftung zukünftiger Zahlungsüberschüsse.[3] Vielen Unternehmen fehlt jedoch Verständnis und Gefühl für ihre immateriellen Werte. Da ein Verlust dieser Werte nicht zwangsläufig buchhalterische Auswirkungen hat, scheint der damit verbundene Schaden nicht vorhanden zu sein. Vor diesem Hintergrund wäre zu überlegen, ob die IT-Security als immaterieller Vermögensgegenstand bewertet werden kann.

6.2.1 Management-Ebene

Der ISO/IEC 17799 wie auch das Grundschutzhandbuch (GSHB (Übergeordnete Maßnahmen)) betrachten das Management der IT-Sicherheit. Die Norm BS 7799-2/ISO 27001, die das Informationssicherheitsmanagementsystem für ein gezieltes Management von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen/Daten spezialisiert, wird als Grundlage für die Bewertung des Informationssicherheitsmanagementsystems angesehen. Die ISO/IEC 27001 enthalten mit dem Plan-Do-Check-Act-System zudem einen Qualitätszirkel, der die dauerhafte Qualität der Arbeitsergebnisse der Überprüfung des Managements sicherstellen soll.

Mit dem Standard SSE-CMM (System Security Engineering – Capability Maturity Model)/ISO 21827 lässt sich aufzeigen, wie sich die Qualität des Sicherheitsmanagements signifikant steigern lässt. Dieser Standard wurde aus dem in der Softwareentwicklung verbreiteten allgemeinen Reifegradmodell CMMI entwickelt. CMMI ist ein Prozessmodell, das die Vorgehensweise beschreibt, um die Prozesse zur Entwicklung von Produkten und Dienstleistungen im IT-Bereich zu definieren, zu überprüfen, zu optimieren und langfristig zu etablieren. Die CMMI-Prinzipien umfassen geplantes Vorgehen, Transparenz, „gelebte“ Prozesse und eine kontinuierliche Verbesserung der Vorgehensweisen: CMMI gibt aber nicht

[1] vgl. ASTRUM IT (2005)
[2] vgl. Bieta, Volker (2004), S.3
[3] vgl. Stoi, Roman (2003), S.176

den Einsatz bestimmter Methoden, Vorgehensmodelle, Technologien oder Tools vor. CMMI hat sich jedoch geöffnet und seinen Fokus von Softwareentwicklung auf Entwicklungsprojekte allgemein (um Hardwareentwicklung) erweitert.[1] SSE-CMM wendet Prozessevaluierungsmethoden auf den Bereich der IT-Sicherheit an, um die schwer evaluierbaren „weichen" Aspekte des Securitymanagements (z. B. Dienstleistungssteuerung) im Sinne eines Benchmarks bewertbar zu machen. Es ist so ein Modell zur Einschätzung des Reifegrads von Sicherheitsprozessen, ohne diese dabei selbst vorzugeben. In Kombination mit den BS 7799/ISO 17799 und dem IT-Grundschutzhandbuch bietet SSE-CMM aber eine Basis zum Aufbau eines Securitymanagements. Der Prozessansatz in SSE-CMM macht zudem die Anbindung an übergeordnete IT-Frameworks wie ITIL oder CObIT möglich.[2]

Mit den angesprochenen Standards ist jedoch eine Bewertung wie in 6.1 angestrebt letztlich nicht möglich.

6.2.2 Monetäre/bilanzielle Ebene

Es geht hier um die Frage, ob die IT-Security als immaterieller Vermögensgegenstand bilanziell angesetzt werden kann, was eine monetäre Bewertung erfordern würde.

Der vom Deutschen Standardisierungsrat verabschiedete Rechnungslegungsstandard (DRS) Nr. 12[3] definiert Immaterielle Vermögenswerte als identifizierbare, in der Verfügungsmacht des Unternehmens stehende, nicht monetäre Vermögenswerte ohne physische Substanz, welche für die Herstellung von Produkten oder das Erbringen von Dienstleistungen, die entgeltliche Überlassung an Dritte oder für die eigene Nutzung verwendet werden können.

Dem DRS 12 kommt gemäß § 342 Abs. 2 HGB aufgrund der Veröffentlichung im Bundesanzeiger vom 22.10.2002 durch das Bundesministerium für Justiz die Vermutung eines Grundsatzes ordnungsgemäßer Buchführung zu. Er regelt die Behandlung immaterieller Vermögenswerte des Anlagevermögens im Konzernabschluss: Zur Erreichung einer Konvergenz mit IAS und US-GAAP orientiert sich DRS 12 so am Konzept des wahrscheinlichen künftigen Nutzenzuflusses: Ein entgeltlich erworbener immaterieller Vermögenswert des Anlagevermögens ist bilanziell anzusetzen, wenn es wahrscheinlich ist, dass dem Unternehmen der künftige wirtschaftliche Nutzen, der diesem Vermögenswert zugeordnet werden kann,

[1] vgl. Neeb-Bruckner, Barbara (2007)
[2] vgl. Kob, Timo (2005)
[3] BMJ (2002)

zufließt und er zuverlässig bewertbar ist. Nicht entgeltlich erworbene immaterielle Vermögenswerte dürfen nicht angesetzt werden.

Nach dieser Regelung könnte ein bilanzieller Ansatz der IT-Security als immaterieller Vermögensgegenstand zur Diskussion gestellt werden: Ein künftiger Nutzenzufluss ist bei einem strategischen IT-Security-Management gerade das angestrebte Ziel. Aber eine zuverlässige Bewertbarkeit kann diesem Nutzenzufluss nicht zugestanden werden.

Eine andere Frage wäre, ob man Aufwendungen für IT-Security-Maßnahmen als nachträgliche Anschaffungs- oder Herstellungskosten nach § 255 Abs. 1 Satz 1 HGB, um einen Vermögensgegenstand in einen betriebsbereiten Zustand zu versetzen, ansehen kann. Bezüglich der Anschaffungskosten entgeltlich erworbener Software sagt die IDW-Stellungnahme zur Rechnungslegung „Bilanzierung von Software beim Anwender“ (RS HFA 11) hierzu, dass bei Individualsoftware und unternehmensspezifisch modifizierter Standardsoftware Betriebsbereitschaft dann vorliegt, wenn die „unternehmensspezifischen Anforderungen an die Leistungsfähigkeit der Software“ erfüllt werden. Aufwendungen, um die Software in einen betriebsbereiten Zustand zu versetzen, zählen laut RS HFA 11 zu den Anschaffungskosten, sofern diese Aufwendungen der Anschaffung direkt zuzurechnen sind. Als unmittelbar mit der Anschaffung im Zusammenhang stehende Ausgaben werden Aufwendungen für das Customizing genannt.[1]

Customizing bedeutet Implementierung, Anpassung und Änderung von Produkten/Systemen, um das System an die individuellen Bedürfnisse und Anforderungen des Unternehmens und Ihrer Benutzer anzupassen, oder individuelle Optimierung besonderer unternehmenskritischer Geschäftsprozesse. Dies kann in Projekten z. B. nach dem internationalen IT Infrastructure Library Standard durchgeführt werden. Diese Anpassungen werden normalerweise nicht durch die einzelnen Standard-Softwarekomponenten abgebildet und müssen im Laufe des Gesamtprojektes zusätzlich erstellt werden. Dabei handelt es sich z. B. um kundenspezifische Modifikationen in den Menüstrukturen, User-Berechtigungen, Masken und Reports. So müssen auch umfangreiche Customizing-Einstellungen hinterlegt werden, z. B. Standard- und Vorschlagswerte auf vielen Ebenen, die dann wahlweise pro Framework, pro Unternehmen oder systemweit gelten. Für Benutzer müssen vielfältige individuelle Einstellungen systemweit und ebenso für jede OLTP-Datenbank einzeln, auf mehreren Ebenen möglich sein. Zeit und Administrationskosten können dabei gespart werden, wenn die auf höherer

[1] vgl. IDW (2004): RS HFA 11, TZ 28-31

Ebene hinterlegten Einstellungen konsequent auf die tieferen Ebenen übernommen werden und hierbei auch Einstellungen überschreiben können.

Aufsetzend auf einer Klassifizierung von Software in Firmware, Systemsoftware und Anwendungssoftware wird im IDW RS HFA 11 zudem eine Aktivierung von Firmware als unselbstständiger Teil der Hardware zusammen mit dieser im Anlagevermögen bejaht. Das bedeutet also, dass z. B. ein „IT-Security-Firmware-Modul“ zusammen mit dem entsprechenden IT-System aktivierbar wäre. System- oder Anwendungssoftware soll aufgrund ihrer selbstständigen Verwertbarkeit dagegen losgelöst von der Hardware als immaterielle Vermögensgegenstände behandelt werden. Ausgenommen davon wird Anwendungssoftware auf Datenträgern zur „Wiedergabe von allgemein zugänglichen Inhalten“ (z. B. Telefon- oder Kursbücher in elektronischer Form), wenn dabei „für ihre Verwendung weder aus dem Inhalt der Software resultierende besondere wirtschaftliche Vorteile (z. B. Nutzung von Kundenkarteien und Verlagsarchiven) noch die Fähigkeit der Software zur Steuerung von Abläufen im Vordergrund stehen“. Solche Anwendungssoftware ist dann als materieller Vermögensgegenstand auszuweisen.[1]

Ein IT-Security-Managementsystem wird im Allgemeinen aber kein reines Softwaresystem sein. Von daher ist der RS HFA 11 nicht weiterführend.

Im deutschen Rechnungslegungssystem stehen der Gläubigerschutz und das Vorsichtsprinzip im Vordergrund. Die EU hat sich für die IAS als einheitliche Rechnungslegungsnorm entschieden. Von allen EU-Unternehmen, die einen Geregelten Markt in Anspruch nehmen, wird seit dem Jahr 2005 die Aufstellung von Konzernabschlüssen nach den Vorschriften der IAS gefordert. Abschlüsse nach IAS sollen für einen weiten Adressatenkreis entscheidungsrelevante Informationen über die Vermögens-, Finanz- und Ertragslage sowie die Zahlungsströme des bilanzierenden Unternehmens und deren Veränderungen liefern. Die Interessen der Investoren stehen im Vordergrund.

Der International Accounting Standard No. 38 (Intangible Assets) betrifft die bilanzielle Aktivierung selbsterstellter und erworbener immaterieller Vermögenswerte. Zunächst ist zu prüfen, ob ein Vermögenswert (Asset) vorliegt. Assets sind Ressourcen, über die das Unternehmen infolge vergangener Ereignisse verfügen kann und aus denen es in Zukunft wirtschaftlichen Nutzen zu erzielen erwartet. Von einem zukünftigen ökonomischen Nutzen ist dann auszugehen, wenn ein asset durch interne Verwendung via Kosteneinsparung oder extern per Verkauf von Produkten und Dienstleistungen genutzt wird (IAS 38.17).

[1] vgl. IDW (2004): RS HFA 11, TZ 3-7

Zusätzlich wird die Erfüllung der Kriterien Identifizierbarkeit und Kontrolle verlangt: Identifizierbar (abgrenzbar) ist der Vermögensgegenstand, wenn er vom einzig nicht identifizierbaren Gegenstand, dem Geschäfts- oder Firmenwert getrennt werden kann (IAS 38.10). Ein Kriterium dafür, anders als im deutschen Bilanzrecht aber kein notwendiges Kriterium (IAS 38.12) ist die eigenständige Verwertbarkeit. Diese ist gegeben, wenn das Objekt veräußert, vermietet oder getauscht werden kann, ohne dass gleichzeitig der zukünftige ökonomische Nutzen anderer Vermögensgegenstände aufgegeben wird (IAS 38.11). Aktien, Anleihen, Investmentzertifikate und Optionsscheine sind durch eine sechsstellige Wertpapierkennnummer (WKN) eindeutig identifizierbar.

Kontrolle ist gegeben, wenn ein vermuteter zukünftiger Cash-flow Rückfluss sich auf gerichtlich durchsetzbare Rechte stützen kann (IAS 38.13). Die Kontrolle eines Unternehmens über einen asset ist durch ein subjektives Recht (Eigentumsrecht) beweisbar. Lizenzen, Urheberrechte und Patente erfüllen diese Bedingung. Keine ausreichende Kontrolle besteht dagegen beim Know-how der Mitarbeiter und Manager (IAS 38.15), Kundenbeziehungen sowie Marktanteilen, Werbung und Restrukturierung. Kontrolle ist aber gegeben wenn z. B. Dritte von der Nutzung einer Software ausgeschlossen sind.

Sind für einen immateriellen asset Identifizierbarkeit und Kontrolle gegeben, so verlangt IAS 38.19 eine bilanzielle Aktivierung, wenn folgende Kriterien erfüllt sind:

(1) Der Zufluss (Cash-flow) muss hinreichend wahrscheinlich sein bzw. es muss zu einem konkreten Zufluss (IAS 38.19) kommen (z. B. Einnahmeerzielung oder deutliche Verbesserung in der Produktion), der durch den asset generierte wirtschaftliche Nutzen muss also mit hinreichender Wahrscheinlichkeit zu künftigen Finanzmittelzuflüssen führen. Für die Beurteilung der Wahrscheinlichkeit des zukünftigen ökonomischen Nutzens gilt es, diese auf die Grundlage vernünftiger und nachweisbarer Annahmen zu stellen, auf der der Unternehmensleitung die bestmöglichste Vorhersage über die wirtschaftlichen Bedingungen, während der Nutzungsdauer des Vermögenswertes, gelingt (IAS 38.20).

(2) Eine objektive Mess- und Bewertbarkeit muss möglich sein (z. B. Kostenrechnung), eine zuverlässige Messbarkeit der Anschaffungs- oder Herstellungskosten des assets muss also gewährleistet werden können. Die Anschaffungskosten sind dabei zuverlässig messbar, wenn der immaterielle Vermögenswert separat erworben wurde und die Gegenleistung in Form von Geld bzw. anderen monetären Vermögenswerten besteht (IAS 38.23).

Ein immaterieller Vermögenswert wird nach IAS 38 also als ein identifizierbares Nutzenpotenzial definiert.

Die Ansatzkriterien für entgeltlich erworbene immaterielle Vermögenswerte des Anlagevermögens nach DRS 12 und IAS 38 sind also im Wesentlichen deckungsgleich.

Der Unterschied liegt bei den selbsterstellten immateriellen Vermögenswerten des Anlagevermögens, die nach IAS 38 aktiviert werden müssen, wenn sie die entsprechenden Ansatzkriterien erfüllen, nach den deutschen Rechnungslegungsvorschriften aber nicht angesetzt werden dürfen. Im deutschen Handelsrecht sind nach herrschender Meinung die ständige Verwertbarkeit und die objektivierbare Werthaltigkeit entscheidend. Immaterielle Vermögenswerte des Anlagevermögens werden als schwer schätzbare und unsichere Werte angesehen.[1] Sie sind deshalb nur aktivierungsfähig, wenn sie entgeltlich erworben wurden. DRS 12 macht für entgeltlich erworbene immaterielle Vermögenswerte des Anlagevermögens aus der Aktivierungsfähigkeit eine Aktivierungspflicht, wenn ein wahrscheinlicher künftiger Nutzenzufluss gegeben ist.

Bezüglich selbsterstellter immaterieller Vermögenswerte des Anlagevermögens orientieren sich die Regelungen der IAS und auch der US-GAAP zur Modifikation bestehender Software ebenfalls am Konzept des wahrscheinlichen künftigen Nutzenzuflusses:[2] Nach US-Statement of Position (SOP) 98-1.24 darf der Aufwand zur Modifikation der Software dann aktiviert werden, wenn die Modifikation mit großer Sicherheit zusätzliche Funktionalität liefert. IAS folgt diesem Konzept: SIC 6.4 sieht eine Aktivierung ebenfalls vor, wenn dadurch der wirtschaftliche Nutzen der Software erhöht wird.

Das Rechnungswesen und das Controlling sind für die Bewertung der Unternehmensressourcen und deren Abbildung in der Unternehmensplanung und im Berichtswesen zuständig. Die bestehenden Möglichkeiten und Standards des Rechnungswesens und des Controllings werden zunehmend als unzureichend zur Bewertung und Steuerung von Unternehmen angesehen. Buchhaltungsorientierte Bewertungsmaßstäbe genügen den erweiterten Ansprüchen bezüglich Führungs- und Steuerungssystemen nicht mehr, um etwa im Rahmen der Planung Wertsteigerungspotenziale zu berücksichtigen. Die traditionellen deutschen buchhalterischen Maßstäbe basieren auf dem im HGB kodifizierten Prinzip der kaufmännischen Vorsicht.[3] Die Berücksichtigung von Nutzenpotenzialen wird vom Ansatz her erst nach IAS oder US-GAAP möglich. Es fehlen z. B. Werkzeuge insbesondere für die gezielte Planung intangibler Güter. Die heute entscheidenden Werttreiber werden oftmals nicht ausreichend transparent. Es findet häufig keine Integration der Intangible-Asset-Ziele in den

[1] Bruns, Hans-G./Thuy, Michael.G./Zeimes Markus (2003), S.138
[2] vgl. Bruns, Hans-G./Thuy, Michael-G./Zeimes Markus (2003), S.140
[3] vgl. Wolf, Klaus (2003b, S.21,22

Management-Prozessen der Unternehmen, eine Abbildung von Intangibles in der Unternehmensplanung statt.[1]

Im Folgenden wird versucht, in diesem Sinne die Bedeutung der IT-Security herauszustellen. Dies wäre eine Basis, um den wie auch immer gearteten Ausweis eines IT-Security-Managementsystems in der externen Unternehmenskommunikation (z. B. im Rahmen der Rechnungslegung) anzuregen.

6.3 Analyse, Bewertung und Optimierung auf den Ebenen der Unternehmensplanung/zukünftige Bedeutung der IT-Security

Die Prüfungen der Revision im IT-Bereich werden nach den eindeutigen Strukturen und Vorgehensweisen der Prüfungsplanung vorgenommen, in deren Rahmen die Prüfobjekte klar definiert werden.[2] Prüfobjekt bei der ex-ante Revision der IT-Security ist die Bedeutung der IT-Security für die Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume.

Aufgrund der Dynamik im IT-Bereich mit der rasanten Weiterentwicklung der Technologien sowie den zunehmend ausgeklügelten Methoden potenzieller Angreifer ist die IT-Security als kontinuierlicher Prozess zu begreifen, für den mittels einer „strategischen Vorplanung ein solides Fundament aufzubauen“ ist. Diese Vorplanung besteht aus Definition des Schutzbedarfs (Schutzbedarfsfeststellung), Schutzbedarfsanalyse und Risikoanalyse. Bei der Schutzbedarfsanalyse, Sicherheitsanalyse, Bedrohungs- und Schwachstellenanalyse geht es um die Einordnung der Prozesse und der sie unterstützenden IT-Systeme in Schutzprofile und Schutzkonzepte entsprechend der Wichtigkeit und Kritikalität orientiert an der Bedeutung für die Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume. Durch die Orientierung an der Bedeutung für die Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume wird die auf der operativen Ebene (im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen) durchgeführte Vorplanung an strategischen Aspekten ausgerichtet.

Der Prozess der Entwicklung eines Sicherheitskonzepts inklusive Detailplanung der (operativen) Maßnahmen sollte auf einer Statusanalyse basieren, welche die für das Unternehmen vorgefundenen Rahmenbedingungen der Umgebung erfasst. Auf dieser Grundlage werden das aktuelle (operative) Sicherheitsniveau bewertet und die kritischen Geschäfts-

[1] vgl. Weber, Jürgen (2006), S.9-11
[2] vgl. Foth, Michael (2006b), S.40

prozesse ermittelt. Als Basis für die Erstellung der Sicherheitsarchitektur und die Strategie für Prävention und Notfallvorbereitung sind die Geschäftsprozesse in Schutzbedarfskategorien einzuordnen. Dies ergibt sich aus den Ergebnissen der Ermittlung der Geschäftsfunktionen, Anwendungen und wichtigsten Unternehmensdaten und der Untersuchung ihrer Abhängigkeit von den IT-Systemen.[1] Im Rahmen der Risikoanalyse sind darauf aufsetzend Gefährdungspotenziale zu identifizieren und auf ihre Bedeutung für die Aufrechterhaltung des Geschäftsbetriebs hin zu bewerten. Eine umfassende Risikobewertung muss dabei sowohl die Daten, als auch die Anwendungen und die Infrastruktur berücksichtigen. Für die Bestimmung der Schutzmaßnahmen darf den Gefährdungen nicht eine gleich hohe Bedeutung zugemessen werden. Dies ist relativ stark abhängig von den individuellen Gegebenheiten im Unternehmen.[2]

Man kann versuchen, über das Vorhandensein von Maßnahmen zur Begegnung potenzieller IT-Risiken die Sicherheit von Unternehmen vergleichbar zu machen. Das IT-Grundschutzhandbuch erlaubt so durch Abgleich mit einem Best-Pratice, Aussagen zur operativen Bewertung der Sicherheit. Dieser Ansatz muss des Weiteren jedoch auch die Wichtigkeit/Kritikalität der abgesicherten Daten, Systeme und Prozesse für das individuelle Unternehmen berücksichtigen. Dies wird durch die Orientierung an der Bedeutung im Kontext der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume abgedeckt.

Die Aspekte, die dabei eine Rolle spielen – unter dem Begriff „Kontext der Organisation“ zusammengefasst – müssen geeignet (z. B. mittels der Szenario-Technik) modelliert und in die Bewertung einbezogen werden. So kann z. B. bei der Betrachtung des Szenarios Feuer die unmittelbare Nachbarschaft eines Chemiewerkes ein Nachteil sein. Die Wichtigkeit einzelner Maßnahmen kann also nicht ohne Berücksichtigung des Kontexts bestimmt werden.[3] Auf technischer Ebene entspricht dies dem Ansatz, dass auch neueste Techniken für Vulnerabiltiy Scanning, Security Scanning, Penetration Testing usw. auf Tool gestützte Simulationen setzen, die die von Scannern entdeckten Systemverletzlichkeiten im Infrastrukturkontext bewerten.[4]

Im Folgenden geht es jedoch nicht um eine operative Bewertung, sondern um eine strategische Bewertung der IT-Security. Diese basiert auf einer Analyse der Unterstützung der Handlungsbefähigung/strategisch-operativen Beweglichkeit als Voraussetzung für die

[1] vgl. Coester, Ursula/Hein, Matthias (2005), S.58
[2] vgl. Coester, Ursula/Hein, Matthias (2005), S.36-40
[3] vgl. Weiß, Stefan (2005)
[4] vgl. Heimann, Holger (2006)

effiziente Umsetzung der Unternehmensstrategie und Abstimmung der Unternehmensziele und Geschäftsprozesse/des IT-Security-Prozesses, bzw. Umsetzung der IT-Security-Strategie und Abstimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander.

Strategie ist ein mehrdimensionales Gebilde, das sich durch Projektion auf verschiedenen Ebenen beschreiben lässt. Strategie hat im Allgemeinen eine politisch-kulturelle, eine ethisch-sozialpsychologische, eine wirtschaftlich-finanzielle, eine technisch-zeitliche, eine rationale/irrationale, eine berechenbare/unberechenbare und eine nationale/internationale Dimension. Diese Dimensionen sind im Prinzip auf jeder der Planungsebenen für eine Geschäftsfeld übergreifende Unternehmensstrategie zu betrachten.

Strategisches Management beinhaltet strategische Planung sowie Steuerungs- und Kontrollprozesse zur Strategiedurchsetzung.[1] Die Effizienz der Geschäftsprozesse/Time to Market wird neben der Kundenstärke/Kundenattraktivität sowie der Technologiestärke/Produktstärke zur Beschreibung von Wettbewerbspositionen in Markt- und Unternehmensdimensionen benutzt. Das strategische Management und die strategische Planung bestimmen die Art der zu generierenden und am Markt/bei den Kunden abzusetzenden Leistungen.[2]

Im Folgenden wird das in Kapitel 5.1.1.4 entwickelte Modell, mit dem in Kapitel 5.1.3 ein strategisch-operatives IT-Security-Management konzipiert wurde, zur Analyse herangezogen:

Die in das strategisch-operative Risiko-Controlling integrierten Komponenten des operativen und strategischen Performance Managements sollen die (im technisch-organisatorischen Kontext zu analysierende) IT-Sicherheit der die Prozesse des Unternehmens unterstützenden IT-Systeme in eine adäquate IT-Security und umgekehrt abbilden. Diese IT-Security soll die Strategie konforme und IT-Nutzenpotenzial absichernde Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume so weit möglich gewährleisten. Die Strategie-Konformität und Absicherung der IT-Nutzenpotenziale soll dadurch unterstützt werden, dass adäquate Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security in das strategische und operative Performance Managements integriert werden. Insgesamt werden durch diese Konzepte entsprechende Steuerungs- und Kontrollprozesse zur Strategieformulierung und -durchsetzung/-umsetzung bezüglich der IT-Security modelliert.

[1] vgl. Piser, Marc (2004), S.25
[2] vgl. Rosenkranz, Friedrich (2006), S.9,10

Das offene System Unternehmung muss die Nichtkalkulierbarkeit mit einplanen. Die Planung soll die Unsicherheit so handhabbar machen und eine höhere Transparenz in das unternehmerische Handeln bringen, einen möglichst kontinuierlichen und reibungslosen Ablauf der unternehmerischen Aktivitäten gewährleisten.[1] Im Rahmen der Planung wird vereinfacht und selektiert. Dies schafft handhabbare Entscheidungsfelder.[2] Die Planung soll jedoch so verlässlich sein, dass alle weiteren Managementaufgaben an der Planung ausgerichtet werden können.[3] Die Managementaufgabe der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume wird dazu auf den Planungsebenen für eine Geschäftsfeld übergreifende Unternehmensstrategie analysiert.

Der Planungsprozess ist ein Geschäftsprozess, der strukturiert, erfasst, abgestimmt, dokumentiert und kontrolliert wird. Er wird durch strategische Geschäftsprozesse unterstützt, die die Voraussetzung dafür schaffen sollen, dass strategische Ziele durch konkrete strategische Tätigkeiten/Aktivitäten erreicht, eventuelle Zielabweichungen gemessen und die Ursachen hierfür ermittelt werden. Strategische Geschäftsprozesse erhalten ihren Input auch aus operativen Geschäftsprozessen, deren Reengineering zu strategischen Vorteilen führt. Sie erlauben die Ermittlung von strategischen Treibern, die für den Unternehmenserfolg von entscheidender Bedeutung sind.[4] Eine Voraussetzung dafür, dass die strategischen Ziele erreicht werden, sei eine adäquate Handlungsbefähigung/strategisch-operative Beweglichkeit. Dazu soll das strategisch-operative Risiko-Controlling die in den Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse abgebildete IT-Security entsprechend ausrichten.

Für den Aufbau eines stringenten Planungsprozesses ist es erforderlich, die zukünftigen Anforderungen an die IT-Unterstützung zu einer integrierten Darstellung zwischen Prozessen, Produkten und Informationstechnologie zwecks grundlegender Koordination der Planung zwischen den Fachbereichen und der IT-Funktion zusammenzuführen. Dieser soll eine verbindliche Darstellung der geschäftsstrategischen Ausrichtung eines Fachbereichs sowie der benötigten organisatorischen und informationstechnischen Lösungen liefern. Er soll Verbindlichkeit in der Weiterentwicklung von Funktionalitäten mittels Ausfluss eines „machbaren“ Maßnahmenkatalogs erzielt werden. Anhand des in ihm zusammengeführten Informationsbildes ermöglicht er ein koordinierendes Umsetzungscontrolling. Dieses Steuerungsinstrument muss mittels eines schlüssigen Steuerungskonzepts zur Anwendung kommen, dem

[1] vgl. Peemöller, Volker H. (2005), S.42
[2] vgl. Piser, Marc (2004), S.38
[3] vgl. Piser, Marc (2004), S.25
[4] vgl. Rosenkranz, Friedrich (2006), S.15,16

Servicemanagement, das alle Leistungen zur übergreifenden Steuerung der IT-Betriebsleistungen, also des Regelbetriebs zusammenfasst.[1] Im Zusammenhang mit der vorliegenden Thematik geht es um die zukünftigen Anforderungen an die IT-Security-Unterstützung für das eine entsprechende Handlungsbefähigung/strategisch-operative Beweglichkeit voraussetzende Erreichen der strategischen Ziele des Unternehmens.

Die Strategische (Gesamt)Planung soll nicht der Formulierung quantitativer Ziele dienen, sondern Erfolgspotenziale erschließen und eine Position bestimmen, von der aus, nach Wegfall bestimmter Unsicherheitselemente, spezifische Ziele verfolgt werden können. Bei der strategischen Planung werden Hypothesen über eruierte bzw. angenommene Wirkungszusammenhänge formuliert. Die taktischen Verhaltensweisen müssen dabei von Fall zu Fall den impliziten Strategien der Unternehmung angepasst werden, die die grundlegende Ausrichtung der Unternehmung und ihrer Geschäftseinheiten bestimmen. Die Gesamtstrategie der Unternehmung wird in dem erwähnten strategischen Plan festgehalten, der die Entscheidungsträger unterstützen soll, die Strategie bewusst und initiativ umzusetzen. Die Strategie und die strategische Planung sind evolutionäre Phänomene, die im Laufe der Zeit die Ziele, als auch die Mittel und Wege zu deren Erreichung entsprechend den sich ändernden Gegebenheiten fortschreiben oder neu festlegen.[2]

Aber unabhängig von der Organisationsstruktur und der Ebenenplanung hinter dem Management von Strategien, kann es sein, dass die ursprünglich geplante Strategie nicht umgesetzt wird. Ebenso ist es möglich, dass ursprünglich nicht geplante Strategien (aus sich im Laufe der Zeit aus ursprünglich nicht geplanten Maßnahmen sich ergebenden Strategiemustern) realisiert werden. Ein Unternehmen benötigt damit nicht nur die Kompetenz, beabsichtigte Strategien erfolgreich umsetzen zu können, sondern auch die strategische Beweglichkeit, um solchen Veränderungsprozessen nachzukommen.[3] Der Prozess der Formulierung und Bewertung von Strategien enthält so auch eine Phase „Erarbeiten von Optionen in den Geschäftsbereichen, um die angestrebten Zielpositionen zu erreichen“. Es geht dabei um die Ausarbeitung strategischer Handlungspositionen. Prinzipiell werden dabei Wachstumsstrategien zum Auf- und Ausbau von Wettbewerbspositionen, Konsolidierungsstrategien zum Halten von Wettbewerbspositionen und Desinvestitionsstrategien zum Rückbilden von Wettbewerbspositionen unterschieden. Die Wettbewerbspositionen der Geschäftsbereiche in den Zielmärkten hängen dabei u. a. vom technischen Entwicklungspotenzial der Geschäftsbereiche ab. Bei der Strategieformulierung werden zur Bestimmung von Wettbewerbsposition

[1] vgl. Henkel, Sven/Schick, Andreas (2004)
[2] vgl. Hinterhuber, Hans H. (2004b), S.141-146
[3] vgl. Seidenschwarz, Werner/Huber, Christian (2002), S.131

Kriterien als Handlungsfelder herangezogen, u. a. das Handlungsfeld technisches Entwicklungspotenzial. Der Orientierungsrahmen für die Formulierung von Strategien zum technischen Entwicklungspotenzial und Innovationsverhalten kann z. B. in Basis-, Schlüssel- und Schrittmacher-Technologien gegliedert werden.[1]

Die strategische Planung soll die Umweltdynamik und die Unsicherheit über die künftige Entwicklung bewältigen.[2] Hauptanliegen ist die Sicherung von Erfolgspotenzialen. Das Problem der strategischen Planung besteht darin, dass in die Zukunft hineinreichende Entscheidungen getroffen werden müssen, die von unsicheren Umweltzuständen abhängen. Strategische Planung und strategisches Management sind gleichbedeutend mit Entscheidungen unter Unsicherheit und Risiko.[3] Um diesem Unsicherheits- und Informationsproblem zu entgegnen, bedient man sich in der Praxis häufig der Szenariotechnik. Interne Ressourcen und Fähigkeiten sollen so frühzeitig an externen Entwicklungen ausgerichtet werden. Wesentliches Ziel ist die Gewinnung von Frühwarninformationen und das Erkennen bedeutender Trends.[4]

Im Zusammenhang mit dem operativen Teil des strategisch-operativen IT-Security-Managements geht es um die Vorplanung, im Zusammenhang mit dem strategischen Teil des strategisch-operativen IT-Security-Managements geht es um die Gesamtplanung. Wie jedes (strategische) Problem hat auch die Vorplanung und die Gesamtplanung mehrere Dimensionen in denen das Problem überschaubar auf seine wesentlichen Elemente reduziert wird: Hier werden die Ressourcenebene, die sozio-technische Ebene, die Organisationsebene, die Geschäftsebene und die Unternehmensebene (das sind die Planungsebenen für eine geschäftsübergreifende Unternehmensstrategie) betrachtet. Die Betrachtung strategischer Handlungspositionen in Form von Realoptionen soll dabei bezüglich der mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens von der Gesamtplanung auf die Vorplanung übernommen werden.

So wie die entsprechenden Aufgaben bezüglich der Produktionsfaktoren für IT-Dienstleistungen (Anwendungsprogramme, Datenspeicher, Server, Netzwerke, Arbeitsplatzsysteme) eine zentrale Planungsaufgabe des Informationsmanagements sind,[5] ist auch die Optimierung auf allen fünf obigen Bewertungsebenen wegen der großen Abhängigkeiten voneinander eine schwierige Aufgabe. Rückwirkungen zu begrenzen und so die

[1] vgl. Seidenschwarz, Werner/Huber, Christian (2002), S.137-138
[2] Peemöller, Volker H. (2005), S.117
[3] vgl. Reichmann, Thomas (1993), S. 249
[4] vgl. Wolf, Klaus (2003b), S.181
[5] vgl. Zarnekow, Rüdiger (2005), S.5,6

Optimierungspotenziale zu steigern ist eine zentrale Planungsaufgabe des IT-Security-Managements. Analog ist die Methode, gemeinsame Strategien, technische Standards und Spielregeln auf allen fünf Ebenen festzulegen und fortzuschreiben.

Optimierung ist in dem Sinn gemeint, die zukünftigen Anforderungen an die IT-Security-Unterstützung für das eine entsprechende Handlungsbefähigung/strategisch-operative Beweglichkeit voraussetzende Erreichen der strategisch-operativen Ziele des Unternehmens abzudecken.

Eine operative Bewertung der IT-Security ist im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen möglich. In diesem Kontext läuft die Vorplanung ab. Der Kontext für eine strategische Bewertung ist der Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume. In diesem Kontext erfolgt die Gesamtplanung. Eine strategische Bewertung der IT-Security wird innerhalb der Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in die auf das System bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume ermöglicht, und zwar über die Analyse der drei Risikokomponenten Planungsrisiko (das mit strategischer und operativer Überwachung zu managen ist), Umsetzungsrisiko (das mit strategischer und operativer Durchführungskontrolle zu managen ist) und Überwachungsrisiko (das mit strategischer und operativer Prämissenkontrolle zu managen ist). Insgesamt soll so beurteilt werden, inwieweit die IT-Security die Strategie konforme und IT-Nutzenpotenzial absichernde Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume unterstützt.

Die (operative) Bewertung der IT-Security kann sich prinzipiell auch auf die Beurteilung des Vorliegens der notwendigen und/oder der hinreichenden Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security beziehen. Im Gegensatz dazu wird hier dem strategischen Ansatz, d. h. der Berücksichtigung des zukünftigen Einflusses auf die Geschäftsaktivität des Unternehmens gefolgt. In der Planungsphase erfolgt dabei eine Aufstellung potenzieller Auswirkungen, die sich durch geplante Maßnahmen ergeben können.

Dies entspricht der Aussage, dass Risiken nicht messbar, aber anhand ihrer Auswirkungen qualifizierbar sind.[1]

[1] vgl. Ibers, Tobias (2005), S.113

Die Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security wurden in das auf die strategisch-operative Beweglichkeit/Handlungsbefähigung abzielende Modell zum strategisch-operativen Risiko-Controlling integriert. Dadurch soll die IT-Security auf die Strategie-Konformität und IT-Nutzenpotenzial-Absicherung bezüglich der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume ausgerichtet werden. Bei IT-gestützten Geschäftsmodellen geht es um die IT-Sicherheit der für diese Geschäftsmöglichkeiten (bzw. der zur Umsetzung entsprechender IT-Projekte) notwendigen IT-Systeme, was sich in der Beherrschbarkeit und Verlässlichkeit der entsprechenden Geschäftsprozesse widerspiegelt.

Die Kritikalität der Konformitätsanforderungen mit externen und internen Ordnungsmäßigkeitsvorgaben ist wesentlicher Teil der Prämissen der Planung. Womit diese externen und internen Ordnungsmäßigkeitsvorgaben in Verbindung stehen, worauf sie sich beziehen, kann aus der notwendigen Bedingung und aus der hinreichenden Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security abgeleitet werden:

Bei den Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security geht es vor allem um Anforderungen zur Anpassung an das organisatorische Umfeld/Anpassung der Organisation an das Umfeld sowie Anpassung an das technische Umfeld/Anpassung der technisch-organisatorischen Konzepte an das Umfeld. Die Beurteilung des Vorliegens der notwendigen Bedingung für die Anpassung an die „Umgebung“ soll diesbezüglich analysieren, ob die Konformität mit externen und internen Ordnungsmäßigkeitsvorgaben in Verbindung mit Aufbau- und Ablauforganisation und dem Einsatz von Technologien, Methoden und Anwendungen zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse gewährleistet ist. Die Beurteilung des Vorliegens der hinreichenden Bedingung für die Anpassung an die „Umgebung“ soll analysieren, ob die Absicherung von Nutzenpotenzialen der IT (soweit durch die IT-Security möglich) gewährleistet ist.

Beurteilungshinweise für den Beitrag von Security-Maßnahmen zur Erreichung der (auf die Unterstützung/Herstellung der Handlungsbefähigung ausgerichteten) Strategie konformen und IT-Nutzenpotenzial absichernden Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse ergeben sich aus einer Analyse der drei Risikokomponenten Planungs-, Umsetzungs- und Überwachungsrisiko. Dies sind die ursachenbezogenen Risikokomponenten, deren Management in Form von strategischer und operativer Überwachung, strategischer und operativer Durchführungskontrolle und strategischer und operativer Prämissenkontrolle zur (Strategie konformen und IT-Nutzenpotenzial absichernden) Ableitung geeigneter Handlungsstrategien beitragen soll.

Bei der Analyse der drei Risikokomponenten Planungs-, Umsetzungs- und Überwachungsrisiko spielen z. B. Verlässlichkeitsanforderungen an die zur Umsetzung der IT-Projekte notwendigen, sowie Anforderungen an die Beherrschbarkeit der entsprechenden IT-Systeme eine wichtige Rolle. Modelltheoretisch lässt sich so begründen, dass das zum Management dieser Risikokomponenten herangezogenen Komponenten des strategischen und operativen Performance Managements integriert werden können in die Abbildung der IT-Sicherheit von Systemen (beurteilt im Kontext Verlässlichkeit und Beherrschbarkeit) in die entsprechende IT-Security im Kontext der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume. Die Anforderungen an die Verlässlichkeit und Beherrschbarkeit können aus der Wichtigkeit/Kritikalität der unterstützten Geschäftsprozesse abgeschätzt werden.

Die drei Risikokomponenten Planungs-, Umsetzungs- und Überwachungsrisiko ähneln denen in Risikomodellen[1] für das Prüfungsrisiko des Wirtschaftsprüfers bei der Abschlussprüfung. Dieses Prüfungsrisiko ist im Rahmen einer Risiko orientierten Abschlussprüfung definiert als Wahrscheinlichkeit, dass der Wirtschaftsprüfer den Abschluss bzw. ein Prüffeld als im Wesentlichen ordnungsgemäß akzeptiert, obwohl es nicht im Wesentlichen ordnungsgemäß ist. Bei der ex-ante Bewertung der IT-Security wäre das Prüffeld die Beurteilung z. B. des Managements, inwieweit das Erreichen der Unternehmensziele trotz Risiken der IT-Security gewährleistet ist. Bei der Beurteilung, ob ein Prüffeld als im Wesentlichen ordnungsgemäß angesehen wird, geht es letztlich darum, ob entsprechende interne/externe Vorgaben (Richtlinien, Standards, (gesetzliche) Vorschriften) als korrekt umgesetzt gelten können. Als Anhaltspunkt für die Gewährleistung des Erreichens der Unternehmensziele trotz Risiken der IT-Security kann analog die konsequente Umsetzung entsprechender bestehender Methoden, Standards, Tools und Best Practices herangezogen werden. Zudem ist zu prüfen, ob die an der Kritikalität/Sensitivität der Sachwerte und Prozesse orientierte korrekte Bestimmung der Relevanz und Anwendbarkeit dieser Methoden, Standards, Tools und Best Practices gewährleistet ist.

Auf Umfang der Prüfungshandlungen des Abschlussprüfers wirken sich immanente/inhärente Risiken des entsprechenden Prüfungsgebiets, Kontrollrisiken und Erkennungsrisiken aus. Das inhärente Risiko ist die Wahrscheinlichkeit für das Auftreten wesentlicher Fehler, unter der Annahme, dass keine internen Kontrollen existieren. Anhaltspunkte für inhärente Risiken des Prüffelds „Beurteilung z. B. des Managements, inwieweit das Erreichen der Unternehmensziele trotz Risiken der IT-Security gewährleistet ist“, sind mögliche Unzulänglichkeiten bei

[1] Marten, Kai-Uwe/Quick, Reiner/Ruhnke, Klaus (2006), S.698-702

der Bestimmung der Relevanz, Anwendbarkeit sowie der konsequenten Umsetzung der Methoden, Standards, Tools und Best Practices zur Erreichung der aus den Unternehmenszielen abgeleiteten IT-Security-Ziele und resultieren aus

- Fehleinschätzung, wie relevant die Konformität mit entsprechenden Ordnungsmäßigkeitsvorgaben st, und wie kritisch und sensitiv entsprechende Sachwerte und Prozesse sind,
- unzureichender Handlungsbefähigung z. B. des Managements bei der Umsetzung der IT-Security-Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses, bzw. der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander

Die Umsetzung der IT-Security-Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses, bzw. der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander erfolgt in Form der Umsetzung entsprechender IT-(Security)-Projekte, im Rahmen derer bestimmte Maßnahmen zu implementieren sind. Im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen ergeben sich aus diesen Unzulänglichkeiten bei der Bestimmung der Relevanz, Anwendbarkeit sowie der konsequenten Umsetzung der Methoden, Standards, Tools und Best Practices die IT-Risiken, dass

- aufgrund dieser Fehleinschätzungen, wie relevant die Konformität mit entsprechenden Ordnungsmäßigkeitsvorgaben ist, und wie kritisch und sensitiv die Sachwerte und Prozesse sind, keine adäquaten Maßnahmen bestimmt werden und somit auch nicht implementiert werden können,
- die notwendige Beherrschbarkeit und/oder Verlässlichkeit der von der Umsetzung entsprechender IT-(Security)-Projekte betroffenen und/oder der dafür notwendigen IT-Systeme bzw. der zu implementierenden Maßnahmen nicht gegeben ist

Das Kontrollrisiko in Risikomodellen für das Prüfungsrisiko des Wirtschaftsprüfers bei der Abschlussprüfung ist die Wahrscheinlichkeit, dass existierende wesentliche Fehler durch das interne Kontrollsystem nicht aufgedeckt werden. Anhaltspunkte für Kontrollrisiken des Prüfungsgebiets „Beurteilung z. B. des Managements, inwieweit das Erreichen der Unternehmensziele trotz Risiken der IT-Security gewährleistet ist“, ist die Nichtaufdeckung möglicher Unzulänglichkeiten bei der Bestimmung der Relevanz, Anwendbarkeit sowie der konsequenten Umsetzung der Methoden, Standards, Tools und Best Practices zur Erreichung der aus den Unternehmenszielen abgeleiteten IT-Security-Ziele bzw. der angestrebten Handlungsbefähigung/strategisch-operativen Beweglichkeit.

Die Beurteilung dieses Kontrollrisikos ist durch die Beurteilung der Ordnungsmäßigkeit des „management control“ im Rahmen des IT-Security-Managements möglich. Dieses „management control“ besteht für die „ex-ante IT-Security“ aus – in das Informationssicherheits-Managementsystem integrierter – (strategischer und operativer) Prämissenkontrolle, (strategischer und operativer) Durchführungskontrolle und (strategischer und operativer). Überwachung,

Diese Komponenten können als ein internes Kontrollsystem betrachtet werden, das auf die Unterstützung/Herstellung der strategisch-operativen Beweglichkeit/Handlungsbefähigung abzielt, um Veränderungsprozessen in Form der Revidierung beabsichtigter Strategien, Neuformulierung und erfolgreichen Umsetzung nachzukommen.

Wenn in Risikomodellen für das Prüfungsrisiko des Wirtschaftsprüfers bei der Abschlussprüfung das Kontrollrisiko aufgrund der Prüfung des internen Überwachungssystems als gering eingeschätzt wird, werden bei den immanenten Risiken des Prüfungsgebiets und gleich bleibendem Gesamt-Prüfungsrisiko die Anforderungen an das Erkennungsrisiko des Abschlussprüfers geringer. Das Erkennungsrisiko/Entdeckungsrisiko ist die Wahrscheinlichkeit, dass der Abschlussprüfer existierende und vom Internen Kontrollsystem nicht rechtzeitig verhinderte oder aufgedeckte wesentliche Fehler nicht aufdeckt.

Entsprechend könnte man folgern, dass – wenn bei der strategischen Bewertung der IT-Security das Risiko, dass Fehleinschätzungen durch interne Kontrollen nicht aufgedeckt werden, als gering eingeschätzt wird – bei den gegebenen immanenten Risiken und bei gleich bleibendem Gesamt-Risiko einer Falschbewertung die Anforderungen an die Aufdeckung der Fehleinschätzungen durch einen Revisor geringer werden. Fehleinschätzungen beziehen sich darauf, wie kritisch und sensitiv die Sachwerte und Prozesse sind (orientiert am strategisch-operativen Ziel der Handlungsbefähigung) und auf die Relevanz und Anwendbarkeit entsprechender (IT-Security) Methoden, Standards, Tools und Best Practices. Aus unzureichender Handlungsbefähigung bei der Implementierung/Umsetzung der als relevant und anwendbar erachteten, bestehenden Methoden, Standards, Tools und Best Practices sowie der mangelnden Verlässlichkeit und/oder Beherrschbarkeit der zur Umsetzung der IT-Projekte notwendigen bzw. von der Umsetzung betroffenen IT-Systeme und zu implementierenden Maßnahmen resultieren die Umsetzungsrisiken. Das inhärente Risiko bezieht sich also auf die Planungsrisiken und die entsprechenden Umsetzungsrisiken unter der Annahme, dass keine internen Kontrollen existieren.

Die Zieldimensionen der Handlungsbefähigung/strategisch-operativen Beweglichkeit sollen in Realoptionen ausgedrückt werden. Es wird so im Prinzip analysiert, welche grundlegenden strategischen Optionen mit welcher IT-Security-Unterstützung gewählt werden können.

Im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen werden so indirekt mögliche Auswirkungen auf das Erreichen der Ziele des Unternehmens auf den Ebenen der Unternehmensplanung untersucht.

Es werden Anforderungen an die Komponenten des strategischen und des operativen Performance Managements gesucht, die den Bedingungen zur Strategie konformen und IT-Nutzenpotenzial absichernden Anpassung an die „Umgebung“ bezüglich der IT-Security genügen. Das strategische Performance Management dient der Steuerung der Formulierung und Realisierung von Strategien, das operative Performance Management dient der Abstimmung der Unternehmensziele und der Geschäftsprozesse/des IT-Security-Prozesses aufeinander. Es werden somit Bedingungen gesucht, mit denen das entwickelte strategisch-operative IT-Security-Management einen Anpassungsprozess an die „Umgebung“ bezüglich der IT-Security implementiert, der die Formulierung und Realisierung der IT-Security-Strategie steuert, und die Unternehmensziele und den IT-Security-Prozess aufeinander abstimmen soll.

Im Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse wird die Unterstützung der in Realoptionen ausgedrückten Handlungsbefähigung analysiert. Die ex-ante Bewertung beurteilt dann, inwieweit das Erreichen unternehmerischer Zielsetzung (bei der Formulierung und Umsetzung der Strategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander) in diesen Zieldimensionen durch die untersuchten Aspekte gefährdet ist oder – positiv ausgedrückt – unterstützt wird.

Der Realoptionsansatz gibt die Annahme auf, dass die Quellen der zugrunde liegenden Unsicherheit privater Natur sind.[1], d. h., dass Unsicherheit z. B. nicht mehr nur an die Unkenntnis nicht öffentlich verfügbarer Informationen gebunden sein soll. Bezogen auf die hinreichende Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security bedeutet dies, dass neben der trivialen Lösung die Existenz einer weiteren Lösung unterstellt wird. Die triviale Lösung lautete: bezüglich der Anpassung an die Umgebung kommt es zu survival of the fittest, unabhängig von der Struktur des Umfelds generell rational dann, wenn „Mitakteure“ (Hacker, Angreifer, Saboteure) nicht auf subjektive Strategieänderungen anderer reagieren, was insbesondere bei völliger Unkenntnis anderer über die eigenen Ziele zutrifft. Diese weitere Lösung wird mit der auf die IT-Security bezogenen Optimierung des Nutzenpotenzials der IT (welches darin liegt, über die IT-Unterstützung der Geschäfts-

[1] vgl. Hommel, Ulrich (2001), S.23

prozesse die Geschäftsprozesse des Unternehmens effizienter zu gestalten) in Verbindung gebracht.

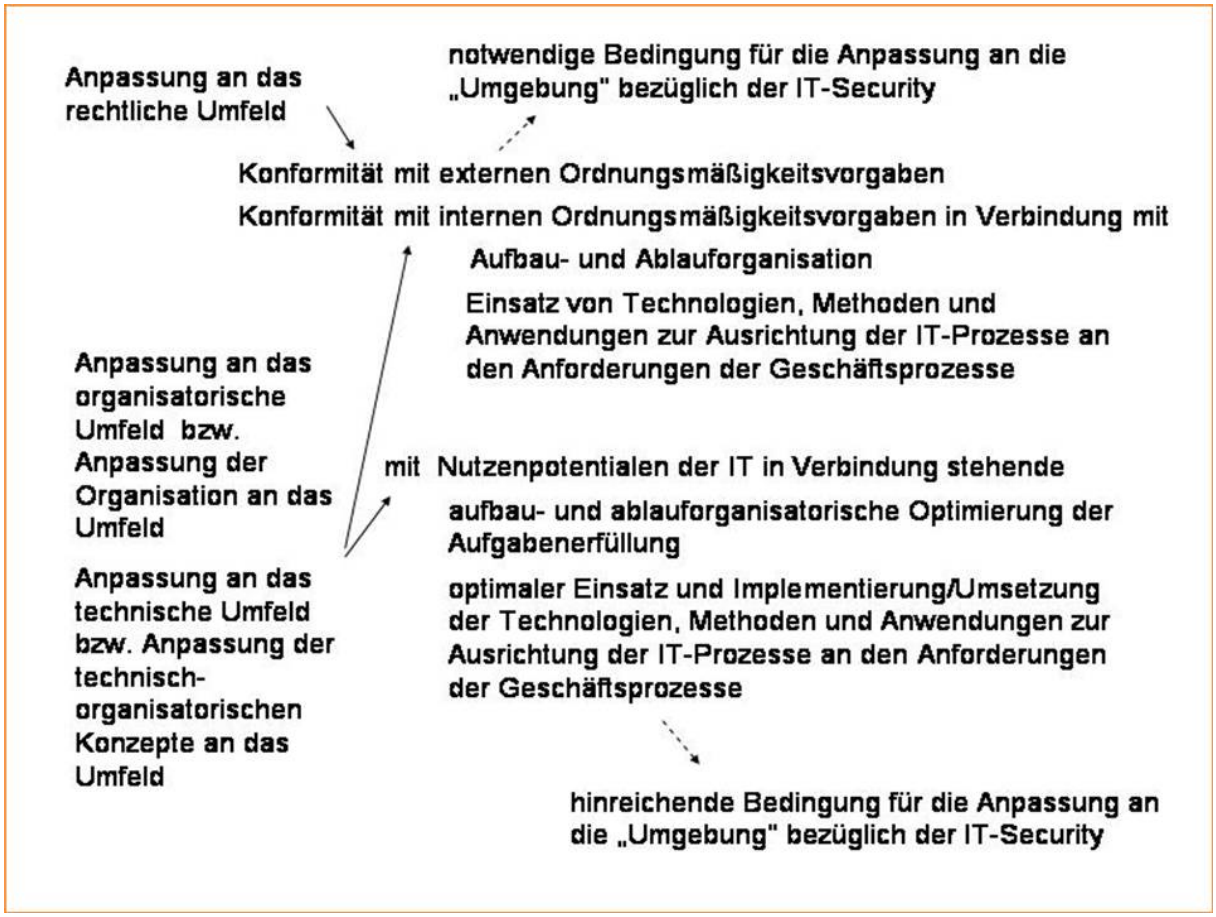


Abb. 26 Bedingungen für die Anpassung an die „Umgebung“

Die notwendige Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security ist die Konformität mit externen und internen Ordnungsmäßigkeitsvorgaben. Die Kritikalität dieser Konformitätsanforderungen ist der Hauptteil der Prämissen der Planung. Die internen Ordnungsmäßigkeitsvorgaben ergeben sich aus der Notwendigkeit

- zur Anpassung an das organisatorische Umfeld/Anpassung der Organisation an das Umfeld sowie
- zur Anpassung an das technische Umfeld/Anpassung der technisch-organisatorischen Konzepte an das Umfeld.

Externe Risiken aus dem Finanz-, Branchen- und Wettbewerbsumfeld stehen im Mittelpunkt des Risikomanagements. Geringere Beachtung finden Risiken aus den politisch-rechtlichen

Bedingungen.[1] Entsprechend haben die Überlegungen zur Anpassung an das organisatorische und das technische Umfeld die mit einem entsprechenden Risikomanagement in Verbindung stehende hinreichende Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security identifiziert. Diese verlangt, die Nutzenpotenziale der IT auf Basis der IT-Unterstützung zur effizienteren Gestaltung der Geschäftsprozesse des Unternehmens, bezüglich der IT-Security zu optimieren. Das IT-Management muss sich ständig an den Einsatz immer neuer Technologien, Methoden und Anwendungen sowie wachsender Anforderungen an die IT-Services anpassen. Dies gilt selbstverständlich auch für die mit den Anforderungen an die IT-Security in Verbindung stehenden IT-Ressourcen, Systeme, Geschäftsprozesse und für das IT-Security-Management.

Der technisch-organisatorische Kontext für die IT-Sicherheit von Systemen wird über die Komponenten (strategische und operative) Prämissenkontrolle, (strategische und operative) Durchführungskontrolle und (strategische und operative) Überwachung in den Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume (Handlungsbefähigung) abgebildet. Die Überlegungen zur Anpassung an das organisatorische und das technische Umfeld können dabei Bedingungen zur (Strategie konformen und IT-Nutzenpotenzial absichernden) Gestaltung der Komponenten (strategische und operative) Prämissenkontrolle, (strategische und operative) Überwachung und (strategische und operative) Durchführungskontrolle ableiten.

Diese Bedingungen sind in Abhängigkeit davon, welche Seite des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen auf der jeweiligen Planungsebene diese Komponenten in den Kontext Handlungsbefähigung abbilden, auf den verschiedenen Planungsebenen zu konkretisieren. Die Sicht des Systems auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen betrifft technologische Aspekte. Hinweise zur Gestaltung von (strategischer und operativer) Prämissenkontrolle, (strategischer und operativer) Durchführungskontrolle und (strategischer und operativer) Überwachung auf Seite der Sicht des Systems auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen ergeben sich also aus Überlegungen zur Anpassung an das technische Umfeld/Anpassung der technisch-organisatorischen Konzepte an das Umfeld. Die Sicht der Benutzer/Anwender auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen betrifft vor allem organisatorische Aspekte. Hinweise zur Gestaltung von (strategischer und operativer) Prämissenkontrolle, (strategischer und operativer) Durchführungskontrolle und (strategischer und operativer) Überwachung auf Seite der Sicht der

[1] vgl. Wolf, Klaus (2003b), S.6

Benutzer/Anwender auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen ergeben sich aus Überlegungen zur Anpassung an das organisatorische Umfeld/Anpassung der Organisation an das Umfeld.

Aus der notwendigen Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security soll entnommen werden, dass es bei den Prämissen darum geht, wie kritisch die Konformität mit externen Ordnungsmäßigkeitsvorgaben sowie internen Ordnungsmäßigkeitsvorgaben in Verbindung mit

- Aufbau- und Ablauforganisation

und/oder dem

- Einsatz von Technologien, Methoden und Anwendungen

zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse ist, wobei „Aufbau- und Ablauforganisation“ die Sicht der Benutzer/Anwender auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen, und „Einsatz von Technologien, Methoden und Anwendungen“ die Sicht des Systems auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen betrifft. Bei den Prämissen handelt es sich um die Prämissen

- der Formulierung und Umsetzung der Strategie/IT-Security-Strategie und der Abstimmung der Unternehmensziele und der IT-Security-Strategie aufeinander (strategische Ebene bzw. strategisches Performance Management)
- Abstimmung der Unternehmensziele und des IT-Security-Prozesses bzw. der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander (operative Ebene bzw. operatives Performance Management)

in Form der Umsetzung entsprechender IT-(Security)-Projekte, im Rahmen derer bestimmte Maßnahmen zu implementieren sind. Auf den verschiedenen Planungsebenen geht es darum, die internen Ordnungsmäßigkeitsvorgaben bezüglich der Unterstützung/Herstellung der Handlungsbefähigung/strategisch-operativen Beweglichkeit zu konkretisieren. Dieser Bezug zur Unterstützung/Herstellung der Handlungsbefähigung/strategisch-operativen Beweglichkeit ist durch die Modellbildung gegeben. Diese Modellbildung zielt in Form des strategisch-operativen Risiko-Controllings auf die Abbildung der IT-Sicherheit von Systemen in die entsprechende IT-Security im Kontext der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume ab.

Strategische und operative Prämissenkontrolle sollen die Prämissen auf ihre auch zukünftige Gültigkeit prüfen.

Die strategische und operative Durchführungskontrolle soll Auswirkungen unvorhergesehener Störungen in der zukünftigen Entwicklung als Abweichungen sichtbar machen um Strategie-Umsetzungsgefahren/Gefahren bei der Abstimmung der Unternehmensziele und Geschäftsprozesse bzw. des IT-Security-Prozesses aufeinander aufdecken. So soll sie dem Management die Ergreifung geeigneter Maßnahmen ermöglichen und soll im Endeffekt gewährleistet werden, dass die notwendige Beherrschbarkeit und/oder Verlässlichkeit der

- von der Umsetzung der in der Sicherheitsrichtlinie des Unternehmens festgelegten Standards und Best Practices
- in Verbindung mit dem Einsatz entsprechender Technologien, Methoden, Tools und Anwendungen

betroffenen Systeme bzw. der zu implementierenden Maßnahmen gegeben ist, wobei Beherrschbarkeit die Sicht der Benutzer/Anwender auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen, und Verlässlichkeit die Sicht des Systems auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen betrifft.

Die strategische und die operative Überwachung haben zu gewährleisten, dass

- Fehleinschätzung, wie kritisch die Konformität mit entsprechenden internen Ordnungsmäßigkeitsvorgaben ist

sowie

- Fehleinschätzungen der Relevanz und Anwendbarkeit der festgelegten Methoden, Standards, Tools und Best Practices

aufgedeckt werden.

Aus der hinreichenden Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security soll entnommen werden, dass Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse auf – mit Nutzenpotenzialen der IT in Verbindung stehende -

- aufbau- und ablauforganisatorische Optimierung der Aufgabenerfüllung

und/oder

- optimalen Einsatz und Implementierung/Umsetzung der entsprechenden Technologien, Methoden und Anwendungen

abzielt. „Aufbau- und ablauforganisatorische Optimierung der Aufgabenerfüllung“ betrifft die Sicht der Benutzer/Anwender auf den technisch-organisatorischen Kontext für die IT-

Sicherheit von Systemen. „Optimaler Einsatz und Implementierung/Umsetzung der entsprechenden Technologien, Methoden und Anwendungen“ betrifft die Sicht des Systems auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen.

Im Folgenden geht es nicht direkt um die Beurteilung des Vorliegens der notwendigen und/oder der hinreichenden Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security, noch um die Beurteilung des inhärenten Risikos oder des Kontrollrisikos des Prüffelds „Beurteilung z. B. des Managements, inwieweit das Erreichen der Unternehmensziele trotz Risiken der IT-Security gewährleistet ist“.. Es wird der Einfluss der IT-Security auf die (das Vorliegen der notwendigen und hinreichenden Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security voraussetzende) strategisch-operative Beweglichkeit/Handlungsbefähigung beurteilt, um Veränderungsprozessen in Form der Revidierung beabsichtigter Strategien, Neuformulierung und erfolgreichen Umsetzung (auch bei der Abstimmung der Unternehmensziele und der IT-Security-Strategie aufeinander) nachzukommen. Dabei geht es um die strategische und operative Absicherung von neuen Geschäftsmöglichkeiten und letztlich darum, IT-Security bezogene Aktivitäten zur Sicherung der Koordinations-, Reaktions- und Adaptionsfähigkeit der Führung festzulegen.

Es wird dann untersucht, welche Aspekte im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen (unabhängig von bestehenden IT-Security Methoden, Standards, Tools und Best Practices) bezüglich möglicher Auswirkungen auf die Erreichung der Unternehmensziele relevant sind. Es sollen so Informationen geliefert werden, auf Basis derer sich eine Einschätzung treffen lässt, in welchem Umfang die betrachteten Risiken das Erreichen der Ziele des Unternehmens gefährden.[1] Es wird damit auf die entsprechenden Aspekte der strategischen und operativen Durchführungskontrolle fokussiert. Umsetzungsrisiken werden im Rahmen des Controllings vom technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen in den Kontext der Handlungsbefähigung/strategisch-operativen Beweglichkeit und umgekehrt abgebildet.

So sollen auf den verschiedenen Planungsebenen die internen Ordnungsmäßigkeitsvorgaben konkretisiert werden. Die Kritikalität der Konformitätsanforderungen mit diesen internen Ordnungsmäßigkeitsvorgaben ist wesentlicher Teil der Prämissen der Planung, und Gegenstand der strategischen und operativen Prämissenkontrolle und der strategischen und operativen Überwachung.

[1] vgl. Hölscher, Reinhold (2002), S.259

Auf Basis der Einflussfaktoren für das Erreichen der Zieldimensionen der strategisch-operativen Beweglichkeit/Handlungsbefähigung leiten sich Hinweise für die ex-ante Optimierung im Zusammenhang mit der Effektivität und Effizienz des auf die Unterstützung/Herstellung der strategisch-operativen Beweglichkeit/Handlungsbefähigung abzielenden IT-Security-Managements (gesteuert und gelenkt durch das beschriebene strategisch-operative Risiko-Controlling) ab. Diese Einflussfaktoren sind u. a. die notwendige Verlässlichkeit und Beherrschbarkeit der von der Umsetzung der strategisch-operativen Ziele betroffenen Systeme bzw. zu implementierender Maßnahmen.

Auf den Planungsebenen für eine Geschäftsfeld übergreifende Unternehmensstrategie und in den Zieldimensionen der Handlungsbefähigung (Realoptionen) erfolgt so die Analyse der Zielerreichung als abhängig von den im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen relevanten Aspekten/den Anforderungskriterien an die IT-Security. Die im Folgenden auf den Planungsebenen für eine Geschäftsfeld übergreifende Unternehmensstrategie untersuchten Zieldimensionen der Handlungsbefähigung können im Prinzip mit den Dimensionen der Erfolgsfaktoren des E-Business (E-Readiness) verknüpft werden: Die Dimension (offene) Informationskultur (und Nutzen bringende Inhalte) kann mit der Ressourcenebene, die Dimension (massenhaften und einfachen) Access mit der sozio-technischen Ebene, die Dimension Collaboration mit der Organisationsebene, die Dimension Standards mit der Geschäftsebene und die Dimension Adaptive Organisation mit der Unternehmensebene identifiziert werden..

Ergebnis dieser Analyse ist, dass entsprechende Schutzfunktionen in der IT-Sicherheitsinfrastruktur konfiguriert bzw. aufgebaut und proaktiv gesteuert werden müssen. Damit soll gewährleistet werden, dass ex-ante die Erreichung der strategisch-operativen Ziele des Unternehmens durch eine mangelnde IT-Security nicht (negativ) beeinflusst wird.

Die für die IT-Sicherheit von Systemen relevanten Aspekte/die Anforderungskriterien an die IT-Security. beziehen sich auf die von Formulierung und Umsetzung der Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander betroffenen Systeme bzw. zu implementierenden Maßnahmen. Die Zieldimensionen der Handlungsbefähigung (Realoptionen) beziehen sich auf die (zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse) eingesetzten Technologien, Methoden und Anwendungen sowie die entsprechende Aufbau- und Ablauforganisation der IT-Projekte (zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens). Denn diese IT-Projekte dienen der Unterstützung/Herstellung der Handlungsbefähigung/strategisch-operativen Beweglichkeit bei der Formulierung und Umsetzung der

Strategie und der Abstimmung der angestrebten Unternehmensziele und des IT-Security-Prozesses aufeinander.

Ähnlich wie im Rahmen der Umsetzung der Anforderungen des KonTraG eine wertorientierte Risikokontrollstruktur auf allen Konzern- bzw. Unternehmensebenen etabliert werden soll[1], wird hier quasi eine Risikosteuerungsstruktur auf allen Unternehmensplanungsebenen konzeptioniert.

Damit können die Anforderungen der die IT-Sicherheit beibehaltenden Unterstützung/Herstellung der Handlungsbefähigung/strategisch-operativen Beweglichkeit bei der Formulierung und Umsetzung der Strategie und der Abstimmung der angestrebten Unternehmensziele und des IT-Security-Prozesses aufeinander auf den verschiedenen Unternehmensplanungsebenen präzisiert werden. Und zwar dergestalt, dass sie z. B. in den so genannten „Protection Profiles“ (Schutzprofilen) oder „Security Targets“ (Sicherheitszielen) zum Ausdruck kommen. Der Prüfer/Zertifizierer bewertet dazu die in den Security Targets umgesetzten Sicherheitsforderungen, die in den Protection Profiles spezifiziert wurden.

Die ex-ante Optimierung der IT-Security bzw. des IT-Security-Managements auf der jeweiligen Planungsebene basiert auf einer Analyse des Einflusses

- der im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen relevanten Aspekte/der Anforderungskriterien an die IT-Sicherheit (zur Erreichung der aus den Unternehmenszielen abgeleiteten IT-Security-Ziele)
- auf de strategisch-operative Beweglichkeit bzw. die Unterstützung/Herstellung der Handlungsbefähigung (bei der Umsetzung der IT-Security-Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses bzw. Abstimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander)
- im Zusammenhang mit den auf der entsprechenden Planungsebene relevanten Realoptionen

Dabei geht es im Wesentlichen um, mit der strategischen und operativen Durchführungskontrolle aufzudeckende Security-Strategie-Umsetzungsgefahren.

Die Optimierung innerhalb des hier entwickelten Modells zum strategisch-operativen Risiko-Controlling der IT-Security fokussiert, je nach betrachteter Planungsebene, verschiedene Teilbereiche/Kombinationen von Komponenten dieses Modells. So ist (innerhalb der Abbildung des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in den Kontext Handlungsbefähigung) bezüglich des technisch-organisatorischen Kontexts für die

[1] vgl. Seidel, Uwe M. (2002), S.116

IT-Sicherheit von Systemen auf der Ressourcenebene die Sicht des IT-Systems (der Kontext Verlässlichkeit) und auf der Unternehmensebene die Sicht der Betroffenen/Anwender/Benutzer (der Kontext Beherrschbarkeit) relevant. Von der Ressourcenebene über die sozio-technische, die Organisations-, die Geschäfts- bis zur Unternehmensebene wird die Sicht der Betroffenen/Anwender/Benutzer (der Kontext Beherrschbarkeit) wichtiger, und von der Unternehmensebene über die Geschäfts-, die Organisations-, die Sozio-technische zur Ressourcenebene die Sicht des IT-Systems (der Kontext Verlässlichkeit) wichtiger. Denn die Sicht des Systems auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen ist ein technologischer Kontext, dessen Kriterien von der sozio-technischen Ebene abwärts von Bedeutung sind. Und die Sicht der Benutzer/Anwender auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen ist ein organisatorischer Kontext, dessen Kriterien von der Organisationsebene aufwärts von Bedeutung sind. Entsprechend sind die Komponenten (strategische und operative) Prämissenkontrolle, (strategische und operative) Durchführungskontrolle und (strategische und operative) Überwachung bei der Optimierung der IT-Security auf den verschiedenen Planungsebenen unterschiedlich auszurichten.

Aus Überlegungen zur Anpassung an das technische Umfeld bzw. Anpassung der technisch-organisatorischen Konzepte an das Umfeld sowie zur Anpassung an das organisatorische Umfeld bzw. Anpassung der Organisation an das Umfeld werden die (auf die Unterstützung/Herstellung der Handlungsbefähigung/strategisch-operativen Beweglichkeit ausgerichteten) internen Ordnungsmäßigkeitsvorgaben (zur Anpassung an die Umgebung bezüglich der IT-Security auf den verschiedenen Planungsebenen konkretisiert. Dies zielt darauf ab, die möglichen zukünftigen Anforderungen an die IT-Security-Unterstützung für das eine entsprechende Handlungsbefähigung/strategisch-operativen Beweglichkeit voraussetzende (IT-Nutzenpotenzial absicherndes) Erreichen der strategisch-operativen Ziele des Unternehmens zu analysieren. Diese Anforderungen sind im Sinne einer kontinuierlichen Verbesserung des IT-Security-Managements mit adäquaten Maßnahmen abzudecken.

Eine Anwendung der Bewertung der Sicherheit von Informationssystemen ist die Prüfung und Zertifizierung von Software. Software besteht aus Programmen und Dokumenten und ist i. d. R. fehleranfällig, schwer prüfbar und Fehlerzustände können sich gegenseitig beeinflussen. Bei Systemsoftware wie Betriebssystemen ist die Zuverlässigkeit von besonderer Bedeutung.

Das zuverlässige Funktionieren von komplexen Software-Systemen ist insbesondere für die Sicherheit von technischen Systemen von großer Bedeutung, wenn aufgrund fehlerhaften Verhaltens entsprechender IT-Systeme z. B. bei der Kommunikation und Verwaltung von Daten der Bruch der Vertraulichkeit, Verlust oder Verfälschung von Daten mit damit einhergehendem erheblichem wirtschaftlichen Schaden droht.[1]

Ein Beispiel für einen Standard zur Prüfung und Zertifizierung von Software bezüglich der Ordnungsmäßigkeit i. S. der Einhaltung der Buchführungsgrundsätze ist der Prüfungsstandard „Erteilung und Verwendung von Softwarebescheinigungen“ (IDW PS 880). Es wird aufgezeigt, welche Anforderungen bei der Prüfung von Softwareprodukten und der Erteilung von Bescheinigungen zu Softwareprodukten von Wirtschaftsprüfern zu beachten sind, wenn diese Produkte für die Ordnungsmäßigkeit der Rechnungslegung von Bedeutung sind. Neben Prüfungsschritten zur Beurteilung

- der für die Einhaltung der Grundsätze ordnungsmäßiger Buchführung bedeutsamen Verarbeitungsfunktionen (insbesondere die Beleg-, Journal- und die Kontenfunktion),
- von Umfang und Wirksamkeit maschineninterner Plausibilitätskontrollen, die sowohl Eingabekontrollen als auch maschinelle Kontroll- und Abstimmverfahren im Verarbeitungsablauf umfasst,

wird auch Art und Umfang der Prüfung der Softwaresicherheit erörtert, die Zugriffsschutz, Datensicherungs- und Wiederanlaufverfahren sowie die Beurteilung der Programmentwicklung, -wartung und -freigabe umfasst.

Der IDW PS 880 beinhaltet aber nicht den Aspekt der Analyse der Bedeutung der Verlässlichkeit und Beherrschbarkeit für das Erreichen der strategisch-operativen Zielsetzungen des Unternehmens. Die mit dem Ablauf der Software in der Einsatzumgebung verbundenen Prüfbereiche

- Systemumgebung einschließlich der entsprechenden internen Kontrollen,
- richtige Bedienung des Programms, sowie zutreffende Einstellungen der Softwaresteuerungsparameter (die während des Customizings festgelegt wurden),
- Arbeitsabwicklung in der DV korrespondierend mit der Arbeitsabwicklung in der Fachabteilung, Funktionentrennung innerhalb der DV-Abteilung sowie Sicherung der Funktionsfähigkeit der DV

können den im Folgenden betrachteten drei untersten Planungsebenen für eine geschäftsübergreifende Unternehmensstrategie (Ressourcenebene, Sozio-technische Ebene und

[1] vgl. BSI (2007), S.50

Organisationsebene) zugeordnet werden: „Systemumgebung einschließlich der entsprechenden internen Kontrollen“ soll der Ressourcenebene zugeordnet werden. „richtige Bedienung des Programms sowie zutreffende Einstellungen der Softwaresteuerungsparameter (die während des Customizings festgelegt wurden)“ soll der sozio-technischen Ebene zugeordnet werden. „Arbeitsabwicklung in der DV korrespondierend mit der Arbeitsabwicklung in der Fachabteilung, Funktionentrennung innerhalb der DV-Abteilung sowie Sicherung der Funktionsfähigkeit der DV“ sind die Bereiche für eine DV-Systemprüfung im Bereich der Ablauforganisation des DV-Bereichs und sollen der Organisationsebene zugeordnet werden.

Der Grundsatz der Funktionstrennung besagt, dass Aufgabenbearbeitung und Aufgabenüberwachung bei Tätigkeiten getrennt voneinander durchgeführt werden müssen, die es ermöglichen, Fehler oder betrügerische Absichten sowohl zu veranlassen, als auch zu verschleiern.[1]

Das strategisch-operative Risiko-Controlling soll den auf die Handlungsbefähigung/strategisch-operative Beweglichkeit bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens abzielenden ex-ante „sicheren“ Ablauf der Software in der Einsatzumgebung gewährleisten. Das entwickelte Modell zum strategisch-operativen Risiko-Controlling impliziert, dass dafür entsprechende Realoptionen unterstützt werden müssen. D. h., wenn das Unternehmen

- zur Optimierung der Geschäftsprozesse und Geschäftsmodelle) bei der Umsetzung der Unternehmensstrategie/IT-Security-Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses/der IT-gestützten Geschäftsmodelle bzw. Abstimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander

Realoptionen (bezüglich der eingesetzten Technologien, Methoden und Anwendungen der IT-Projekte sowie der entsprechenden Aufbau- und Ablauforganisation) ausübt, welche typischerweise ein entsprechendes Customizing der Software bedingt, so müssen die Anforderungen der Ordnungsmäßigkeit (Beherrschbarkeit) und Softwaresicherheit (Verlässlichkeit) weiterhin erfüllt sein. Dabei geht es letztlich um die Beherrschbarkeit und Verlässlichkeit der von der Software unterstützen Geschäftsprozesse.

Insgesamt ist dazu ein auf einer Basisinstallation und optimalerweise einer mehrstufigen Sicherheitsrichtlinie basierendes Konfigurations-Management notwendig.[2]

[1] vgl. Martin, Thomas A. (2002), S.131,132
[2] vgl Rudolph, Heiko (2006), S.45

Von großer Bedeutung scheint eine solche ex-ante Optimierung der IT-Security vor allem bezüglich der Sicherheit in virtuellen Umgebungen, wo viele physikalische Systeme auf einer Maschine virtuell zusammengeführt werden, um Kapazitäten optimal auszuschöpfen:

Die Flexibilität einer solchen virtualisierten Umgebung ist der entscheidende Aspekt: In Sekundenschnelle lassen sich unterschiedliche Betriebssystemumgebungen oder sogar virtualisierte Netzwerkkomponenten aufbauen.[1] Die im Folgenden beschriebenen Ebenen sind prinzipiell geeignet, die Sicherheit solcher Infrastrukturen zu analysieren.

6.3.1 Ressourcenebene

Auf dieser Ebene geht es um Fragen wie „Welche Input-Anforderungen, steuernden Größen und notwendigen Ressourcen können sich negativ auf die angestrebten Ziele auswirken?/In welchem Ausmaß sind die Werttreiber davon tangiert?“. Falls erforderlich, lassen sich hier erprobte Methoden und Instrumente, wie die Fehlermöglichkeits- und -einflussanalyse hinzuziehen.

Ein auf der Ressourcenebene angesiedelter Forschungsansatz ist der resource-based view. Dieser stellt bei der Inhaltsforschung, wo die strategischen Ursachen für nachhaltige Erfolgsunterschiede liegen, die Ressourcenausstattung eines Unternehmens (Know-how, Technologien ….) in den Mittelpunkt.[2] Einer der entscheidenden Erfolgsfaktoren für Unternehmen im Informationszeitalter ist dabei die Mobilisierung von nicht-physischen Vermögenswerten und intellektuellem Kapital, sog. „weiche“, immaterielle Werte wie z. B. die Fähigkeit der Mitarbeiter richtig zu erkennen und zu verwerten (mit dem Ziel, die internen Geschäftsabläufe, die Qualität der Produkte sowie die Reaktionszeiten nachhaltig zu verbessern) oder Informationssysteme strategisch sinnvoll einzusetzen.[3] In diesem Strategiedenken kommt dem Human-Ressource-Ansatz eine immer größere Bedeutung zu: Die Auflösung zeitlicher und räumlicher Begrenzungen in einer sich globalisierenden, netzartigen Economy stellt hohe Anforderungen an das Wissen und die Fähigkeiten der Mitarbeiter.[4] Diese Economy ist durch gute Ideen und schnelle Entscheidungen geprägt.[5] Das Unternehmen muss die Fähigkeit haben, sich selbstständig von innen heraus getragen zu erneuern. Nur das verleiht der Institution die notwendige Dauerhaftigkeit.[6] Als Potenzial für die Wertgenerierung im Unternehmen spielen diese bilanziell zumeist nicht erfassbaren immateriellen Werte wie Fähig-

[1] vgl. Karpinsky, Jörg (2007), S.22
[2] vgl. Eschenbach, Rolf (2003), S.14
[3] vgl. Horváth, Peter. (2000), S.213,214
[4] vgl. Oetinger, Bolko von (2000), S.22
[5] vgl. Oetinger, Bolko von (2000), S.23
[6] vgl. Oetinger, Bolko von (2000), S.24

keiten und Erfahrungen eine entscheidende Rolle.[1] Zentral sind die im Unternehmen entwickelten Problemlösungsmuster und -techniken, also die Fähigkeiten (capability based view) bzw. das kollektive Wissen einer Organisation (knowledge based view).[2] In diesem strategischen Ansatz des knowledge based view verankert sich Wissen als vierter Produktionsfaktor (neben Boden, Kapital und Arbeit), Wettbewerbsfaktor, Erfolgsfaktor oder kritische organisationale Ressource.[3] (Organisationale Ressourcen sind z. B. Managementsysteme wie Planungs- und Kontrollsystem oder Informationssysteme.[4]) Das Ergebnis sind Modelle der Strategieentwicklung, mit deren Hilfe das Unternehmen die eigene Ressourcenausstattung analysieren und gestalten soll.[5]

Auch die Sicherheit bezüglich Human Ressources spielt eine wichtige Rolle. Dabei geht es z. B. um das während eines Anstellungsverhältnisses erworbene unternehmensspezifische Wissen des Mitarbeiters, das dieser möglicherweise geschäftsschädigend einsetzen könnte oder das Rücksetzen der entsprechenden Rechte im Firmennetz beim Ausscheiden des Mitarbeiters.

Im Zusammenhang mit dem IT-Security-Management geht es z. B. um Anforderungen aus dem mit der Verschmelzung der Informations- und Kommunikationstechnik verbundenen schnellen Austausch von Daten und Informationen mittels elektronischer Kommunikation. Auf der Ressourcenebene können daraus Anforderungen für die gemeinsame Nutzung von Ressourcen wie IT-Systemen (bestehend auf physikalischer Ebene u. a. aus Dateisystem, Drucker, Rechnerkapazitäten) abgeleitet werden. Die (sich aus logischer Sicht ergebenden) IT-Lösungen sollen sich der Wertschöpfungskette im Unternehmen anpassen. Die Ressourcen sind dahin gehend zu konsolidieren, dass sie flexibler eingesetzt und skaliert werden können. Dadurch können Ressourcen eingespart oder zumindest effektiver genutzt werden. Dies wird durch die Einbindung offener IT-Architekturen in die Unternehmensstruktur erreicht. Auch IT-Ressourcen sollten dabei nutzbringend eingesetzt werden. Der Nutzen entsteht durch Einbringung in die Geschäftsprozesse, sie müssen zur Wertschöpfung der unterstützten Prozesse beitragen. Der Ressourceneinsatz ist dabei, u. a. im Hinblick auf das Suchen neuer Geschäftsmöglichkeiten, „sowohl finanziell als auch personell angemessen zu dimensionieren“.[6]

[1] vgl. Wallmüller, Ernest (2004), S.2
[2] vgl. Eschenbach, Rolf (2003), S.20
[3] vgl. Hanke, Thomas (2006), S.2
[4] vgl. Hanke, Thomas (2006), S.15
[5] vgl. Eschenbach, Rolf (2003), S.14
[6] Seidenschwarz, Werner/Huber, Christian (2002), S.135

Auf der Ressourcenebene steht die Verfügbarkeit der von den Geschäftsprozessen genutzten Ressourcen im Mittelpunkt.[1] Auf Basis der Business Impact-Analyse kann z. B. abgeschätzt werden, welche Auswirkungen der Ausfall von Ressourcen grundsätzlich hat.[2] Die Abhängigkeit der Geschäftsprozesse des Unternehmens von bestimmten Ressourcen setzt dabei die detaillierte strategische und operative Planung dieser Ressourcen und ihres Nutzen bringenden Einsatzes voraus.

Die Analyse der Geschäftsprozesse in Hinblick auf die Anforderungen an die Verfügbarkeit der von ihnen genutzten Ressourcen ist ein wichtiges Element bei der Prozessanalyse z. B. im Rahmen eines integrierten Notfallmanagements (im Zusammenspiel von Technik, Notfallverfahren und Organisation). Bei der Prozessanalyse werden dabei vor allem die Abhängigkeiten der Geschäftsprozesse von Ressourcen und der Prozesse untereinander ermittelt. Voraussetzung dafür ist, dass das Unternehmen bezüglich der allgemeinen IT-Notfallrisiken beleuchtet wurde (auch im Hinblick auf diejenigen Risiken, die speziell z. B. aufgrund der geografischen Lage oder bestimmter kritischer Geschäftsprozesse relevant sind).[3]

Anforderungen an die Verfügbarkeit der von den Geschäftsprozessen genutzten Ressourcen und an die gemeinsame Nutzung von Ressourcen fließen in die Planung ein. Die ex-ante mögliche Nichterfüllung der Anforderungen an die Verfügbarkeit der von den Geschäftsprozessen genutzten Ressourcen und an die gemeinsame Nutzung von Ressourcen kann die erfolgreiche Umsetzung strategisch-operativer Ziele negativ beeinflussen. Die durch eine mangelnde IT-Security beeinflusste Nichterfüllung obiger Anforderungen induziert also einen wichtigen Teil des Umsetzungsrisikos bezüglich strategisch-operativer Ziele.

Bei der Betrachtung strategischer Handlungspositionen (Realoptionen) bezüglich der mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens geht es vor allem um Wechseloption, Expansionsoption, und Option zur Variation des Inputs/Outputs. Die internen Ordnungsmäßigkeitsvorgaben auf dieser Planungsebene beziehen sich darauf, dass die Betriebszustände der Ressourcen (Daten, Anwendungen, Technologien, Anlagen und Personal) gewechselt, die Ressourcenbasis verbreitert und so der Output der IT-Projekte variiert werden kann. Dabei geht es um die Ressourcen zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse. Aktivitäten eines Geschäftsprozesses unterliegen aufgrund mangelnder Wechselbarkeit der

[1] Dahmer, Ralf (2007)
[2] vgl. Kullmann, Peter (2005)
[3] vgl. Kullmann, Peter (2006), S.25,26

Betriebszustände (im einfachsten Fall Zu-/Abschaltbarkeit(der Ressourcen, mangelnder Verbreiterbarkeit der Ressourcenbasis, und daraus folgender mangelnder Variierbarkeit des Outputs der IT-Projekte, bei ihrer Ausführung zeitlichen, sachlich/logischen und anderweitigen Restriktionen.

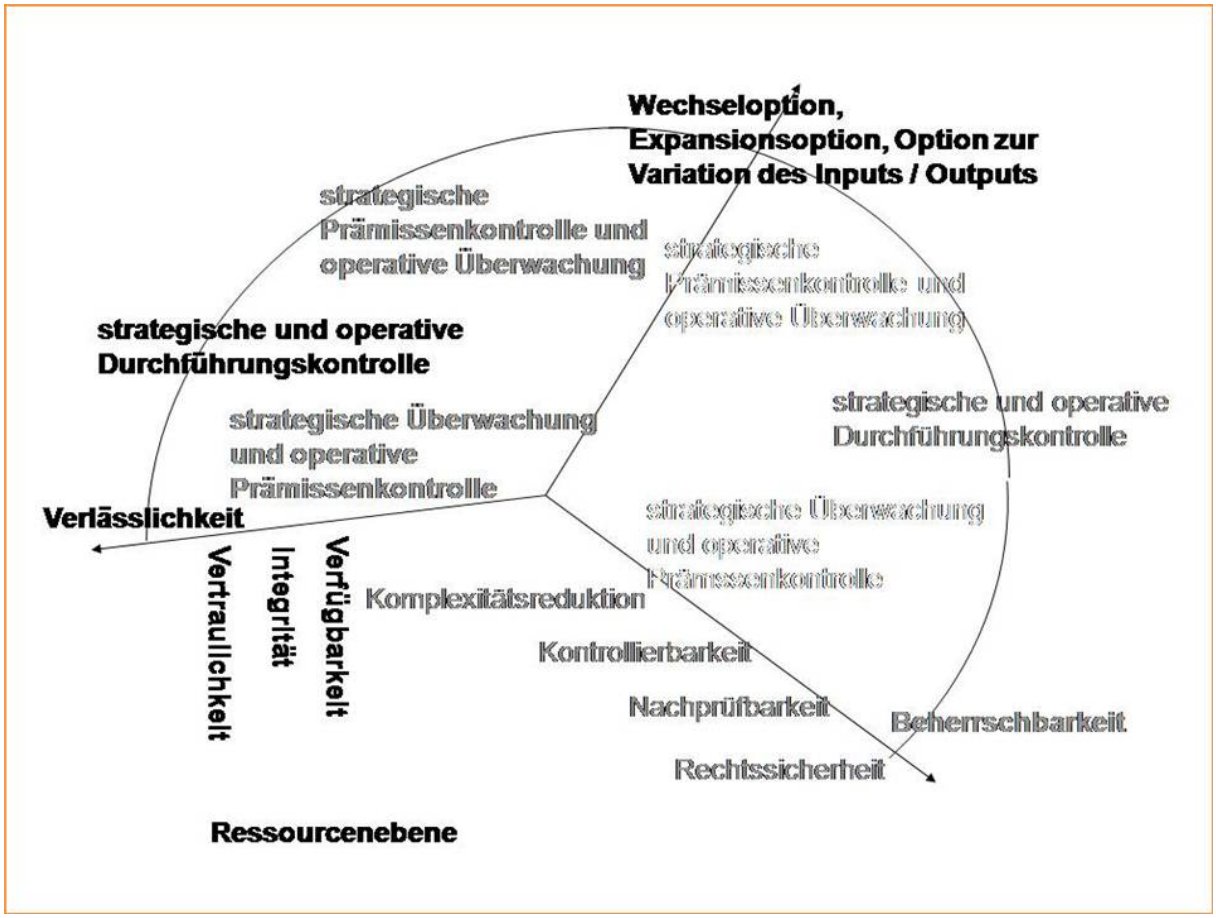


Abb. 27 *Ressourcenebene im strategisch-operativen Risiko-Controlling*

Es ist zu beurteilen, inwieweit die im Zusammenhang mit diesen Optionen stehende Handlungsbefähigung/strategisch-operative Beweglichkeit von den im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen relevanten Aspekten/den Anforderungskriterien an die Verlässlichkeit der von der Umsetzung strategisch-operativer Ziele betroffenen Systeme bzw. zu implementierenden Maßnahmen abhängig ist.. Die Anforderungen an die Verlässlichkeit der betreffenden Systeme bzw. zu implementierenden Maßnahmen sollten unabhängig von einem Betriebszustandswechsel der Ressourcen, der Verbreiterung der Ressourcenbasis und der damit eventuell einhergehenden Variation des Outputs der IT-Projekte, der

- (zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse) eingesetzten Technologien, Methoden und An-

wendungen der IT-Projekte (zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens)

erfüllt sein.

Bezüglich der mit dem Ablauf von Software in der Einsatzumgebung verbundenen Prüfbereiche kann der Ressourcenebene der Prüfbereich des IDW PS 880 „Systemumgebung einschließlich der entsprechenden internen Kontrollen“ zugeordnet werden: Für eine vertrauenswürdige, authentische und manipulationssichere Datenübertragung in Netzwerken muss z. B. sichergestellt werden, dass der Absender den Versand, und der Empfänger den Erhalt einer Nachricht nicht bestreiten kann. Die Security-Funktionalitäten des Systems sollen dazu /auf der Ressourcenebene/dem Prüfbereich ‚Systemumgebung einschließlich der entsprechenden internen Kontrollen“ zugeordnet) Methoden bereitstellen, die gewährleisten, dass a.) der Empfänger der Nachricht während des Datenaustausches den Beweis der Existenz/Korrektheit des Absenders der Nachricht erhält und b.) der Absender der Nachricht während des Datenaustausches den Beweis der Existenz/Korrektheit des Empfängers der Nachricht erhält. Nutzer schützen sollen. Zur Sicherstellung der Privatheit z. B. für datenschutzrechtliche Anforderungen sind neben der Anonymität und Pseudonymität auch die Unlinkbarkeit und Unbeobachtbarkeit:zu gewährleisten. Unlinkbarkeit bedeutet sicherzustellen, dass der Nutzer Ressourcen oder Services mehrfach nutzen kann, ohne dass jemand andres in der Lage ist, diese Nutzungen in irgendeiner Form zu verbinden. Unbeobachtbarkeit soll sicherstellen, dass der Nutzer eine Ressource oder einen Service nutzen kann, ohne dass andere Nutzer die Nutzung dieser Ressource oder dieses Services durch den anderen Nutzer beobachten können.

Für einen ex-ante „sicheren“ Ablauf der Software in der Einsatzumgebung sollten die beschriebenen Anforderungen an die Security-Funktionalität und Verlässlichkeit unabhängig von einem Betriebszustandswechsel der Ressourcen, der Verbreiterung der Ressourcenbasis und der damit eventuell einhergehenden Variation des Outputs der IT-Projekte, der (zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse) eingesetzten Technologien, Methoden und Anwendungen der IT-Projekte (zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens) erfüllt sein. Z. B. müssen die Anforderungen an die Verlässlichkeit des Softwaresystems auch bei einer Vergrößerung der mit den eingesetzten Technologien, Methoden und Anwendungen ver-/bearbeiteten Datenmenge erfüllt sein.

6.3.2 Sozio-technische Ebene

Auf der sozio-technischen Ebene werden die systemimmanenten Erfolgspotenziale im operativen Geschäft erschlossen. Es geht auch um das Management von Risiken, um die systemimmanenten Erfolgspotenziale im operativen Geschäft nicht zu gefährden. Dazu ist eine geeignete Sicherheitsinfrastruktur aufzubauen. Diese bildet die Basis zur Auswahl von Sicherheitsprodukten, die in die IT-Infrastruktur implementiert werden. Die IT-Sicherheitsorganisation soll die zielgerichtete Nutzung der Sicherheitsprodukte und -komponenten gewährleisten.

Ein Erfolg versprechendes Portfolio im operativen Geschäft lässt sich nur aufbauen, wenn die einzelnen Aktivitäten im Lichte möglicher Zukunftsentwicklungen bewertet werden. Auch sozio-technische Systeme – die sozio-technische Ebene beinhaltet die Entwicklung von Nutzungskonzepten für spezifische Technologien oder sozio-technische Systeme – bedürfen der Überprüfung im Lichte möglicher technologischer Entwicklungen oder Produktkonzepte.[1]

Betrachtet werden als wichtigste Nutzenpotenziale hier direkte Netzwerkeffekte, welche durch Veränderung der Anzahl der Nutzer eines Produkts/einer Dienstleistung den Nutzen des Produkts/der Dienstleistung für den einzelnen Nutzer verändern. Der einzelwirtschaftliche Nutzen eines informationstechnologischen Produkts hängt stark von der Anzahl seiner Anwender ab. Bei Einführung eines neuen Produkts sind die Unternehmen um ein schnelles und nachhaltiges Wachstum der Kundenbasis und möglichst große Besetzung des Markts bemüht.[2] Gelingt es dem Unternehmen dabei nicht, sich den Bedürfnissen der Kunden anzupassen, so wird selbst eine exzellente Performance interner Prozesse zwecklos („doing the wrong things right“). Dies ist im Umfeld sich verkürzender Technologievorsprünge und einem Wandel vom Verkäufer zum Käufermarkt erfolgsentscheidend.[3] So versuchen viele Unternehmen, möglichst schnell die kritische Masse an Anwendern zu erreichen und De-facto-Standards zu etablieren. Der Anbieter mit den meisten Anwendern bietet ja den größten Nutzen für den einzelnen Anwender und wird sich am Markt durchsetzen. Der schnelle ständige technologische Wandel sorgt dabei dafür, dass diese Tendenzen zu natürlichen Monopolen nur kurz andauern.[4] Klassisches Beispiel für diesen Effekt ist das Telekommunikationsnetz.[5]

Vor allem im E-Business kann nicht mehr von der Loyalität des Kunden ausgegangen werden. Niedrige Wechselbarrieren, kritische Masseneffekte und positive Netzwerkeffekte

[1] vgl. Fink, Alexander (2001), S.52,53
[2] vgl. Stoi, Roman (2002, S.154
[3] vgl. Seidenschwarz, Werner/Huber, Christian (2002), S.126
[4] vgl. Stoi, Roman (2002, S.154
[5] vgl. Berens, Wolfgang (2004), S.82

können jederzeit zur Abwanderung von erheblichen Kundenpotenzialen führen. Eine Kundenbindung erfolgt hier vor allem durch eine erfolgreiche Entwicklung, Vermarktung und Durchsetzung von Standardprodukten.[1]

Voraussetzung für die Kunden-Loyalität ist dabei, dass die Grundlagen für Sicherheit und Vertrauen gelegt sind. Zu den damit verbundenen Sorgfaltspflichten gehört u. a.[2]

- regelmäßige (operative) Überprüfung der Sicherheit gegebenenfalls durch externe Experten
- verständliche Sicherheitspolitik
- Maßnahmen zur Verhinderung von Diebstahl und Betrug
- Festlegung der Prozesse für die Eskalation im Fall von Sicherheitsvorfällen
- effiziente Kommunikationsstrategie bezüglich Information zum Schutz des Kunden

Im Zusammenhang mit dem IT-Security-Management geht es um die Gefährdung systemimmanenter Erfolgspotenziale im operativen Geschäft aufgrund unzureichender IT-Security z. B. bei der Unterstützung der Entwicklung von Nutzungskonzepten für spezifische Technologien oder sozio-technische Systeme: die strategisch-operative Beweglichkeit, die Unterstützung/Herstellung der Handlungsbefähigung um sich den Bedürfnissen der Kunden anzupassen und so z. B. positive Netzwerkeffekte zu ermöglichen.

Bei der Betrachtung strategischer Handlungspositionen (Realoptionen) bezüglich der mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens geht es um Erweiterungs- bzw. Konsolidierungsoption. Um z. B. bei Einführung eines neuen Produkts ein schnelles und nachhaltiges Wachstum der Kundenbasis zu ermöglichen, d. h. den Produktionsumfang flexibel vergrößern und gegebenenfalls Kapazitäten verschieben zu können, ist diesbezüglichen Umsetzungsrisiken entgegenzuwirken. Einflussfaktoren dieser Umsetzungsrisiken sind die notwendige Verlässlichkeit und Beherrschbarkeit der von der Umsetzung strategisch-operativer Ziele in Zusammenhang mit dieser Erweiterung bzw. Konsolidierung betroffenen Systeme bzw. zu implementierenden Maßnahmen. Die internen Ordnungsmäßigkeitsvorgaben auf dieser Planungsebene beziehen sich also darauf, dass die zur Ausrichtung der IT-Prozesse an den

[1] vgl. Kirchner, Michael (2002), S.103
[2] vgl. Kirchner, Michael (2002), S.104

Anforderungen der Geschäftsprozesse eingesetzten Technologien, Methoden und Anwendungen (aber auch die entsprechende Aufbau- und Ablauforganisation) zum

- Management von Risiken, um die systemimmanenten Erfolgspotenziale im operativen Geschäft nicht zu gefährden und dem dazu erforderlichen Aufbau einer geeigneten Sicherheitsinfrastruktur

erweitert oder zusammengelegt werden können.

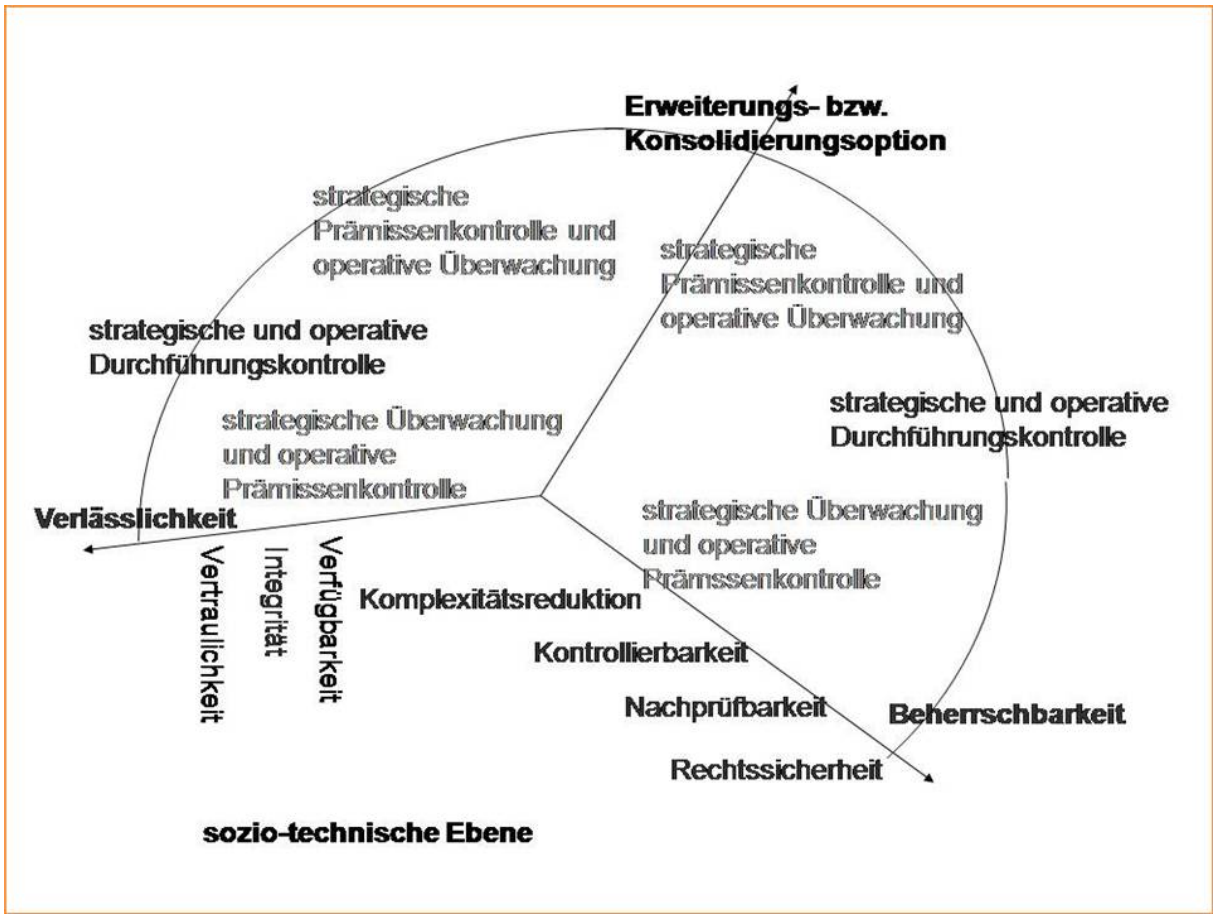


Abb. 28 *Sozio-technische Ebene im strategisch-operativen Risiko-Controlling*

Es ist zu beurteilen, inwieweit die im Zusammenhang mit diesen Optionen stehenden Anforderungen an die Verlässlichkeit (aber auch die Beherrschbarkeit) der von der Umsetzung strategisch-operativer Ziele betroffenen Systeme bzw. zu implementierenden Maßnahmen von den im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen relevanten Aspekten/den Anforderungskriterien an die IT-Security abhängig sind. Die Anforderungen an die Verlässlichkeit und die Beherrschbarkeit der betreffenden Systeme bzw. zu implementierenden Maßnahmen sollten unabhängig von einer Erweiterung oder Zusammenführung der

– (zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse und zur Optimierung der Geschäftsprozesse/Geschäftsmodelle des Unternehmens) eingesetzten Technologien, Methoden und Anwendungen und der entsprechenden Aufbau- und Ablauforganisation der IT-Projekte

erfüllt sein.

Bezüglich der mit dem Ablauf von Software in der Einsatzumgebung verbundenen Prüfbereiche kann der sozio-technischen Ebene der Prüfbereich des IDW PS 880 ‚richtige Bedienung des Programms sowie zutreffende Einstellungen der Softwaresteuerungsparameter (die während des Customizings festgelegt wurden)“ zugeordnet werden. Um zu erreichen, dass die funktionalen Anforderungen und Spezifikationen des Systems auch in der Implementierung erreicht werden, dazu soll ein in das Produkt//System integriertes Konfigurations-Management-System eine Methode bereitstellen, die es erlaubt, alle Anpassungen und Modifikationen nachzuverfolgen, und gewährleistet, dass nur autorisierte Änderungen erfolgen. Es soll ein Automatismus vorhanden sein, der dabei unterstützt zu ermitteln, dass korrekte Konfigurations-Einstellungen benutzt werden; es soll gewährleistet sein, dass die Implementierung des Produkts/Systems einem automatisierten Kontrollmechanismus unterliegt. Das Produkt/System hat die Protokollierung von Übermittlungs-, Anwender- und Wartungsaktivitäten zu unterstützen. Dazu soll das Produkt/System eine Informationsflusskontrolle enthalten. Außerdem muss gewährleistet sein, dass die Security-Funktonalitäten nicht umgangen, deaktiviert, korrumpiert, annulliert oder beschädigt werden können.

Für einen ex-ante „sicheren“ Ablauf der Software in der Einsatzumgebung sollten die beschriebenen Anforderungen an die Vertrauenswürdigkeit, Verlässlichkeit und Beherrschbarkeit des Softwaresystems unabhängig von einer Erweiterung oder Zusammenführung der (zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse und zur Optimierung der Geschäftsprozesse/Geschäftsmodelle des Unternehmens) eingesetzten Technologien, Methoden und Anwendungen und der entsprechenden Aufbau- und Ablauforganisation) der IT-Projekte erfüllt sein. Müssen bei der ‚Erschließung von Nutzungskonzepten für spezifische Technologien oder sozio-technische Systeme zur Gewährleistung von systemimmanenten Erfolgspotenzialen im operativen Geschäft“ die eingesetzten Technologien, Methoden oder Anwendungen oder die entsprechende Aufbau- oder Ablauforganisation erweitert oder zusammengelegt werden, so sollen die mit ‚der richtigen Bedienung des Programms sowie der zutreffenden Einstellung der Softwaresteuerungspara-

meter“ verbundenen Anforderungen an die Verlässlichkeit und Beherrschbarkeit des Softwaresystems unabhängig von dieser Erweiterung oder Zusammenführung erfüllt sein. Werden im Zuge der Anpassung an die Bedürfnisse der Kunden z. B. zur Erweiterung der Produktlinie interne Prozesse (z. B. bezüglich Aufbau- oder Ablauforganisation) zusammengelegt, und zu diesem Zweck Steuerungsparameter eines Softwaresystems im Zusammenhang mit diesen internen Prozessen neu eingestellt, so darf die Verlässlichkeit und Beherrschbarkeit des Softwaresystems nicht beeinträchtigt werden.

6.3.3 Organisationsebene

Auf der Organisationsebene werden die strategischen Geschäftsziele durch Organisation optimierter Prozesse umgesetzt. Auf dieser Ebene kann auch das Business Process Management (BPM) angesiedelt werden:

Im Mittelpunkt dieses Managementansatzes steht eine Managementphilosophie, die sich um die fortlaufende Verbesserung der Geschäftsprozesse kümmert und ein ausgeklügeltes System zur Unterstützung liefern will, das „Entscheidungsträgern, Anwendern und IT-Fachleuten ermöglicht, zusammenzuarbeiten und die Organisationsstrukturen auf den neuesten Stand zu halten“. So erlauben moderne Business Process Management – Systeme mittels XML das Modell der Geschäftslogik beliebig anzupassen; bei neuen Anforderungen (neue Vorgaben, zusätzliche Verordnungen usw.) muss die Ablauflogik bereits ablaufender Prozesse verlässlich geändert werden können.[1] Dies basiert bei einer Service orientierten Architektur basierendem BPM darauf, dass bei Änderungen im Geschäftsprozess nur die Kombination der benutzen Services angepasst werden muss. Häufig werden dabei Services externer Dienstleister kooperativ kombiniert.[2]

Ein wichtiges strategisches Mittel zur Vergrößerung von Gestaltungsmöglichkeiten sind also Netzwerke, Kooperationen und Verbünde von Unternehmen.[3] Schaffung unternehmerischer Entscheidungs- und Handlungsspielräume zwingen u. a. zu einem kooperativen Führungsstil.[4] Kooperationen können Markttransaktionen substituieren und bieten sich als Alternative zum immer wieder notwendigen Abschluss von Verträgen bezüglich gehandelter Produkte/Leistungen an.[5] Die flexiblen Möglichkeiten zur Übertragung von Know-how kreieren eine weltweite Kommunikationsbasis, die eine Verbreitung von Wissen ohne hohen finanziellen Aufwand bedeutet. Entscheidend ist, inwieweit Organisationen bereit sind,

[1] vgl. Armbruster, Marcus/Niegel, Andreas /2006)
[2] vgl. Amann, Marion (2006)
[3] vgl. Becker, Thomas (2005)
[4] vgl. Hahn, Dietger (2006), S.31
[5] vgl. Bischof, Jürgen (2002), S.36

Wissensentwicklung zu fördern und Kooperationen mit einem integrierten, vernetzten, weitsichtigen Denkansatz im Unternehmen und über dessen Grenzen hinaus zu allen beteiligten Partnern zu entwickeln.[1] Unterstützt werden muss dies durch IT-Systeme welche eine entsprechende IT-Security erfordern.

Im dynamischen Netzwerk ermöglichen kleine Einheiten mit flachen Hierarchien und kurzen Entscheidungswegen flexible Reaktionen auf Veränderungen des Marktes. Globale Unternehmensnetzwerke bieten die Möglichkeit, Risiken effektiver und effizienter zu „hedgen" und so den Unternehmenswert zu steigern.[2] Die Koordination verteilter, selbstständig arbeitender Einheiten wird dabei durch moderne Informations- und Kommunikationstechnologie ermöglicht.[3] Solche innovativen Informationstechnologien müssen die Unternehmen dabei unterstützen, als Glied eines komplexen wirtschaftlichen Netzwerks zu agieren und auf Anforderungen des Umfelds flexibel reagieren zu können.[4] Die Weiter- bzw. Neuentwicklung von unternehmensrelevanten Technologien ist also eine notwendige Bedingung der ökonomischen Treiber der organisatorischen Vernetzung von Unternehmen. Diese wiederum ist ein entscheidender Erfolgsfaktor, um den komplexer werdenden Anforderungen der Nachfrager und dem wachsenden Wettbewerb gerecht zu werden.

Um dem Wettbewerbsumfeld gerecht zu werden, hat sich z. B. das E-Procurement des Unternehmens entsprechend den sich ändernden Marktverhältnissen immer neu an die Gegebenheiten anzupassen. Dies zwingt zur steigenden Flexibilität hinsichtlich des organisatorischen Wandels. Für das Bestehen im dynamischen Wettbewerbsumfeld, die Sicherstellung wettbewerbsfähiger Kostenstrukturen, ist neben der Produktaktualität, die Aktualität der aufbau- und ablauforganisatorischen Prozesse bzw. Organisation notwendige Voraussetzung.[5]

Bei dem Wettbewerbszuwachs im Markt führen nicht mehr das Produkt/die Leistung selber unbedingt zu einer Kaufentscheidung der Kunden, sondern zusätzliche Faktoren wie Service, Wartung, Weiterentwicklung. Diese ökonomischen Treiber führen zu einer konzeptionellen und operativen Weiterentwicklung von Organisations- und Kooperationsformen sowie der entsprechenden inter- und intraorganisatorischen Prozesse. Dies bedeutet Arbeitsteiligkeit aufseiten der Anbieter, wobei sich jeder auf seine Kernkompetenzen im Leistungserstellungsprozess konzentriert, und die anderen Teilaufgaben von vernetzten Kooperations-Unternehmen wahrgenommen werden.[6]

[1] vgl. Kremin-Buch, Beate/Unger, Fritz/Walz, Hartmut (2004), S.16-18
[2] vgl. Hommel, Ulrich (2001):, S.207-227
[3] vgl. Stoi, Roman (2002, S.154
[4] vgl. Chamoni, Peter (2004), S.I
[5] vgl. Kirchner, Michael (2002), S.105
[6] vgl. Berens, Wolfgang (2004), S.65-70

Im Zusammenhang mit dem IT-Security-Management geht es um die Gefährdung der Umsetzung/Organisation optimierter Prozesse und somit die Umsetzung damit zusammenhängender strategischer Geschäftsziele aufgrund unzureichender IT-Security: die strategisch-operative Beweglichkeit und Unterstützung/Herstellung der Handlungsbefähigung durch den Einsatz innovativer Informationstechnologien (die von einer entsprechenden IT-Security abhängen) um steigende Flexibilität hinsichtlich des organisatorischen Wandels zu erreichen und z. B. als Glied eines komplexen wirtschaftlichen Netzwerks zu agieren und auf Anforderungen des Umfelds flexibel reagieren zu können.

Bei der Betrachtung strategischer Handlungspositionen (Realoptionen) bezüglich der mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens geht es von dieser Ebene her um Kontraktoption, d. h. die Option, z. B. an solchen dynamischen Netzwerken oder globalen Unternehmensnetzwerken teilzunehmen.

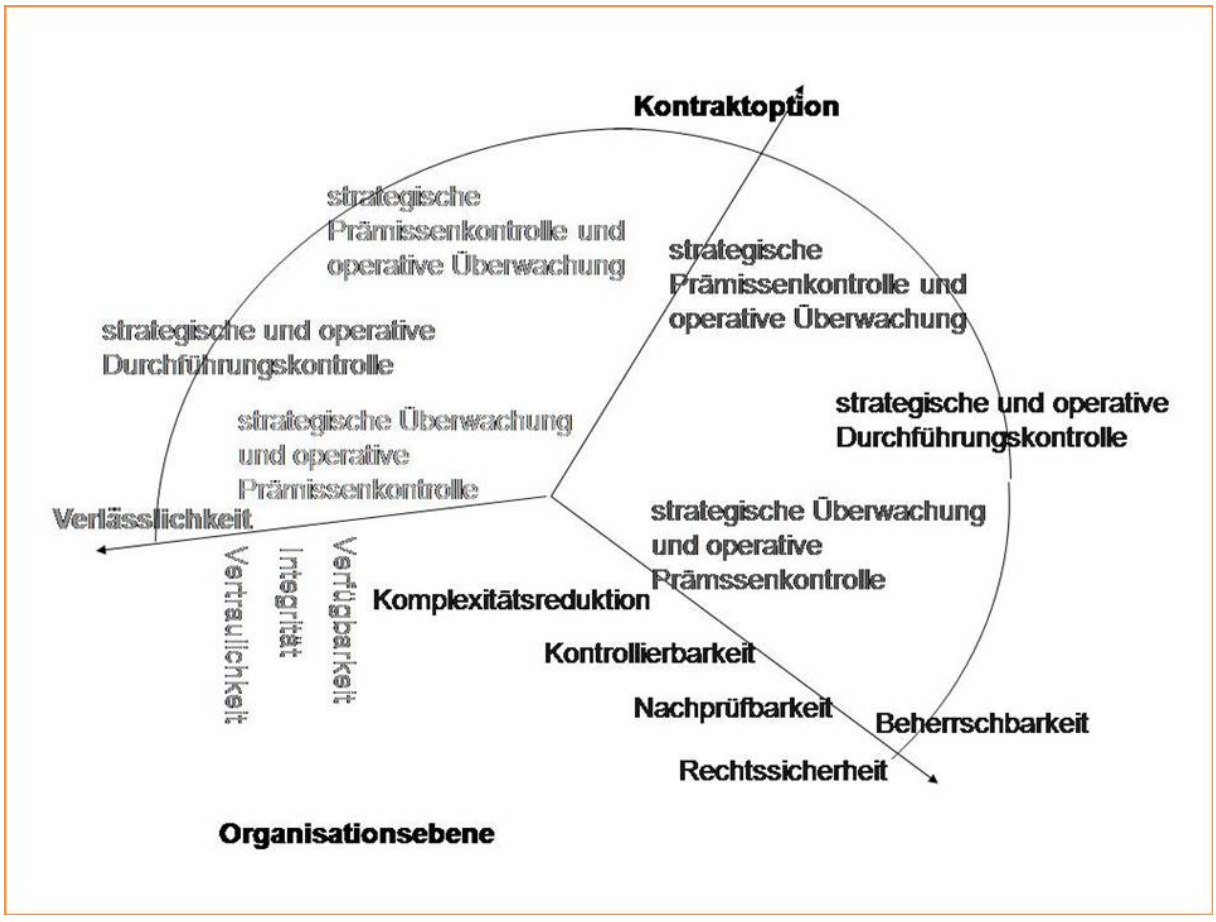


Abb. 29 Organisationsebene im strategisch-operativen Risiko-Controlling

Die ex-ante Bewertung der IT-Security bzw. des IT-Security-Managements auf der Organisationsebene beurteilt dann die Bedeutung der im technisch-organisatorischen Kontext

für die IT-Sicherheit von Systemen relevanten Aspekte/der Anforderungskriterien an die IT-Security für Treiber und Aktionsmuster der Unternehmensvernetzung.

Mittels automatisierter Informations- und Kommunikationstechnologie kooperierende Unternehmen müssen sich auf die Zuverlässigkeit und Integrität der gekoppelten Komponenten und Prozesse verlassen können.[1] Hierunter fallen Risiken, dass Fehler oder Versagen in Informationssystemen, internen Kontrollen oder in Unzulänglichkeiten der Mitarbeiter begründete Fehlhandlungen auftreten und z. B. zu einer fehlerhaften Datenbasis führen,

Um einen maximalen Grad an operativer Flexibilität zu erreichen, müssen flexible Technologien eingesetzt werden und alle Absatzmärkte von jedem Standort aus bedient werden können.[2] Grundlage für den elektronischen Datenaustausch (EDI) zwischen Unternehmen bildet dabei die serviceorientierte Architektur (SOA) auf XML-Basis. Über SOA und EDI können Kooperationspartner ihre gemeinsamen Geschäftsprozesse optimieren und ihre Kommunikation flexibler gestalten. Doch die enge Verknüpfung mit Geschäftspartnern und Kunden stellt hohe Sicherheitsanforderungen. Es muss sehr genau darauf geachtet werden, dass nur autorisierte Nutzer auf sensible Geschäftsdaten und -prozesse Zugriff haben (Identity-Management).[3]

Die internen Ordnungsmäßigkeitsvorgaben auf dieser Planungsebene beziehen sich also darauf, dass die zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse eingesetzten Technologien, Methoden und Anwendungen und die entsprechende Aufbau- und Ablauforganisation der IT-Projekte (zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle) der beteiligten Unternehmen,

- um als Glied eines komplexen wirtschaftlichen Netzwerks zu agieren und auf Anforderungen des Umfelds flexibel reagieren zu können,

kooperativ zusammengelegt/gemeinsam genutzt werden können. Es ist zu beurteilen, inwieweit die im Zusammenhang mit dieser Option stehenden Anforderungen an die Verlässlichkeit und die Beherrschbarkeit der von der Umsetzung der strategisch-operativen Ziele betroffenen Systeme bzw. zu implementierenden Maßnahmen von den im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen relevanten Aspekten/den Anforderungskriterien an die IT-Security abhängig sind.

Die Anforderungen an die Verlässlichkeit und die Beherrschbarkeit der betreffenden Systeme bzw. zu implementierenden Maßnahmen

[1] vgl. Krcmar, Helmut/Junginger, Markus (2003), S.252
[2] vgl. Hommel, Ulrich (2001):, S.214
[3] vgl. Parthier, Ulrich (2005b)

– bei der Umsetzung strategischer Geschäftsziele durch Organisation optimierter Prozesse zur Vergrößerung von Gestaltungsmöglichkeiten z. B. mit dem strategischen Mittel Netzwerke, Kooperationen und Verbünde

sollten unabhängig von einer kooperativen Zusammenführung/gemeinsamen Nutzung der

– (zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse) eingesetzten Technologien, Methoden und Anwendungen und der entsprechenden Aufbau- und Ablauforganisation der IT-Projekte (zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens)

erfüllt sein.

Bezüglich der mit dem Ablauf von Software in der Einsatzumgebung verbundenen Prüfbereiche können der Organisationsebene die Prüfbereiche des IDW PS 880 ‚Arbeitsabwicklung in der DV korrespondierend mit der Arbeitsabwicklung in der Fachabteilung, Funktionentrennung innerhalb der DV-Abteilung sowie Sicherung der Funktionsfähigkeit der DV“ zugeordnet werden: Die Umsetzung strategischer Geschäftsziele durch Organisation optimierter Prozesse, insbesondere die Koordination verteilter, selbstständig arbeitender Einheiten, erfordert eine Arbeitsabwicklung in der DV, die an der Arbeitsabwicklung in der Fachabteilung ausgerichtet ist; die ordnungsgemäße Organisation erfordert die Funktionentrennung innerhalb der DV-Abteilung; und setzt die Funktionsfähigkeit der DV voraus.

Für einen ex-ante „sicheren“ Ablauf der Software in der Einsatzumgebung sollten die Anforderungen an die Verlässlichkeit und die Beherrschbarkeit des Softwaresystems unabhängig von einer kooperativen Zusammenführung/gemeinsamen Nutzung der (zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse) eingesetzten Technologien, Methoden und Anwendungen und der entsprechenden Aufbau- und Ablauforganisation der IT-Projekte (zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens) erfüllt sein. Müssen bei der ‚Umsetzung strategischer Geschäftsziele durch Organisation optimierter Prozesse zur Vergrößerung von Gestaltungsmöglichkeiten z. B. mit dem strategischen Mittel Netzwerke, Kooperationen und Verbünde“ die ‚eingesetzten Technologien, Methoden oder Anwendungen oder die entsprechenden Aufbau- und Ablauforganisationen“ kooperativ zusammengelegt/gemeinsam genutzt werden, so sollen die mit der ‚Arbeitsabwicklung in der DV korrespondierend mit der Arbeitsabwicklung in der

Fachabteilung“, „Funktionentrennung innerhalb der DV-Abteilung“ sowie „Sicherung der Funktionsfähigkeit der DV“ verbundenen Anforderungen an die Verlässlichkeit und die Beherrschbarkeit des Softwaresystems unabhängig von dieser kooperativen Zusammenführung/gemeinsamen Nutzung erfüllt sein. Werden im Zuge einer Unternehmenskooperation, zur Optimierung der Ablauforganisation des DV-Bereichs (Abstimmung der Arbeitsabwicklung, Aufgabenbearbeitung und Aufgabenüberwachung, Sicherung der Funktionsfähigkeit der DV) z. B. Technologien, Methoden und Anwendungen der Unternehmens übergreifenden IT-Projekte gemeinsam genutzt, so darf die Beherrschbarkeit der davon betroffenen Softwaresysteme nicht beeinträchtigt werden.

6.3.4 Geschäftsebene

Auf der Geschäftsebene erfolgt die Identifikation und Erschließung von Marktpotenzialen im Rahmen strategischer Geschäftsfelder. Auf der Ebene von Geschäftsbereichen werden die Vorgaben der Unternehmensstrategie umgesetzt. Bei der Ausgestaltung steht die Frage nach Ansatzpunkten für die Erzielung von Wettbewerbsvorteilen im Vordergrund.[1]

Im Zusammenhang mit dem IT-Security-Management geht es um die Bedeutung der IT-Security für die Umsetzung der Vorgaben der Unternehmensstrategie, d. h., z. B. für die Unterstützung/Ermöglichung/Sicherung bestehender und neuer Geschäftsprozesse/Geschäftsmodelle: die strategisch-operative Beweglichkeit und Unterstützung/Herstellung der Handlungsbefähigung durch den Einsatz innovativer Informationstechnologien (die von einer entsprechenden IT-Security abhängen) um Wettbewerbsvorteile und auf den Vorgaben der Unternehmensstrategie basierende Wachstumsmöglichkeiten zu erschließen.

Bei der Betrachtung strategischer Handlungspositionen (Realoptionen) bezüglich der mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens geht es um Wachstumsoptionen, d. h. die Option, neue Geschäftsprozesse/Geschäftsmodelle zu ermöglichen. Diese Geschäftsprozesse/Geschäftsmodelle basieren auf der Bereitstellung entsprechender IT-Dienstleistungen/IT-Services mit nachvollziehbarem Wertbeitrag, die die geschäftlichen Anforderungen der einzelnen Unternehmensbereiche optimal unterstützen. Die internen Ordnungsmäßigkeitsvorgaben auf dieser Planungsebene beziehen sich darauf, dass die zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse eingesetzte Auf-

[1] vgl. Seidenschwarz, Werner/Huber, Christian. (2002), S.129

bau- und Ablauforganisation (aber auch die entsprechenden Technologien, Methoden und Anwendungen) der IT-Projekte (zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens) neue Geschäftsprozesse/Geschäftsmodelle bzw. die Umsetzung der Vorgaben der Unternehmensstrategie ermöglicht.

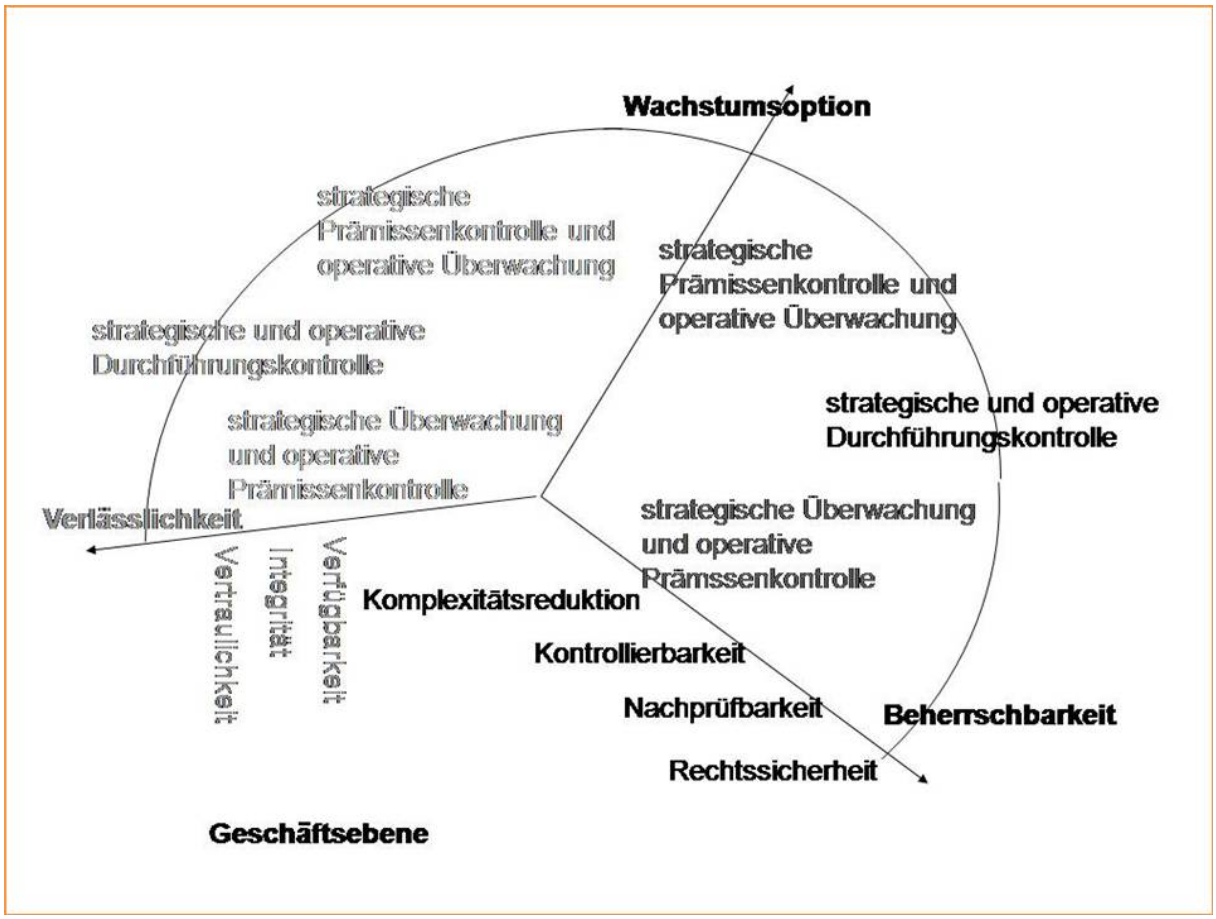


Abb. 30 *Geschäftsebene im strategisch-operativen Risiko-Controlling*

Es ist zu beurteilen, inwieweit die im Zusammenhang mit dieser Option stehenden Anforderungen an die Beherrschbarkeit (aber auch die Verlässlichkeit) der von der Umsetzung der strategisch-operativen Ziele betroffenen Systeme bzw. zu implementierenden Maßnahmen von den im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen relevanten Aspekten/den Anforderungskriterien an die IT-Security abhängig sind.

Die Anforderungen an die Beherrschbarkeit (und auch die Verlässlichkeit) der betreffenden Systeme bzw. zu implementierenden Maßnahmen

- bei der Umsetzung der Vorgaben der Unternehmensstrategie auf der Ebene von Geschäftsbereichen, zur Identifikation und Erschließung von Marktpotenzialen im Rahmen strategischer Geschäftsfelder

sollten unabhängig von neuen Geschäftsprozessen/-modellen (ermöglicht mit Hilfe der

– (zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse) eingesetzten Aufbau- und Ablauforganisation (und auch der entsprechenden Technologien, Methoden und Anwendungen) der IT-Projekte (zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens))

erfüllt sein.

Für einen ex-ante „sicheren“ Ablauf der Software in der Einsatzumgebung sollten die Anforderungen an die Beherrschbarkeit (und auch die Verlässlichkeit) des Softwaresystems unabhängig von neuen Geschäftsprozessen/-modellen (ermöglicht mithilfe der zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse eingesetzten Aufbau- und Ablauforganisation (und der entsprechenden Technologien, Methoden und Anwendungen) der IT-Projekte (zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens)) erfüllt sein. Müssen bei der ‚Umsetzung der Vorgaben der Unternehmensstrategie auf der Ebene von Geschäftsbereichen, zur Identifikation und Erschließung von Marktpotenzialen im Rahmen strategischer Geschäftsfelder“ neue Geschäftsprozesse/Geschäftsmodelle ermöglicht werden, so sollen die Anforderungen an die Beherrschbarkeit (und auch die Verlässlichkeit) des Softwaresystems unabhängig von diesen neuen Geschäftsprozessen/-modellen erfüllt sein. Werden zur Ermöglichung neuer Geschäftsprozesse/Geschäftsmodelle z. B. Aufbau- und Ablauforganisation der IT-Projekte neu ausgerichtet, so darf die Verlässlichkeit des Softwaresysteme nicht beeinträchtigt werden.

6.3.5 Unternehmensebene

Unternehmerische Aktivitäten vollziehen sich unter steigender Geschwindigkeit und zunehmendem Neuigkeitsgrad des Wandels der Rahmenbedingungen der Unternehmensumwelt. Dies ist in der erhöhten Komplexität der Unternehmensumwelt sowie der wachsenden Intensität der Unternehmensverflechtungen begründet. Auf der Unternehmensebene erfolgt die Führung der Geschäftsfelder sowie Entwicklung und Pflege der Unternehmensstrategie. Es werden die langfristigen Entwicklungsrichtungen des Unternehmens festgelegt und langfristige Entscheidungen zu Wachstums-, Stabilisierungs- und Desinvestitionsstrategien getroffen. Dies beinhaltet u. a. Fragen zu Produkt-Markt Kombinationen, Kooperationen und nach Geschäftsaufträgen für darunter liegende Einheiten.[1] Diese Ebene ist also sehr stark mit der darunter liegenden Geschäftsebene und Organisationsebene korreliert. Eine konsequente

[1] vgl. Seidenschwarz, Werner/Huber, Christian (2002), S.129

Investitions- und Desinvestitionspolitik, die eine „profitablere Unternehmenswertentwicklung“ ermöglicht, ist mit den Vorgaben der Planung von Profitabilitätszielen, andererseits der Ressourcenverteilung auf die Geschäftsbereiche entsprechend deren Zielerreichungsgraden möglich.[1]

Im Zusammenhang mit dem IT-Security-Management geht es um die Bedeutung der IT-Security für die Führung der Geschäftsfelder sowie Entwicklung und Pflege der Unternehmensstrategie., d. h., z. B. für eine konsequente Investitions- und Desinvestitionspolitik: die strategisch-operative Beweglichkeit und Unterstützung/Herstellung der Handlungsbefähigung durch den Einsatz innovativer Informationstechnologien (die von einer entsprechenden IT-Security abhängen) um eine solche Investitions- und Desinvestitionspolitik: unter steigender Geschwindigkeit und zunehmendem Neuigkeitsgrad des Wandels der Rahmenbedingungen der Unternehmensumwelt zu ermöglichen.

Bei der Betrachtung von Realoptionen bezüglich der mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens sind also die Realoptionen der darunter liegenden Geschäftsebene und Organisationsebene (Wachstumsoptionen und Kontraktoptionen) relevant.

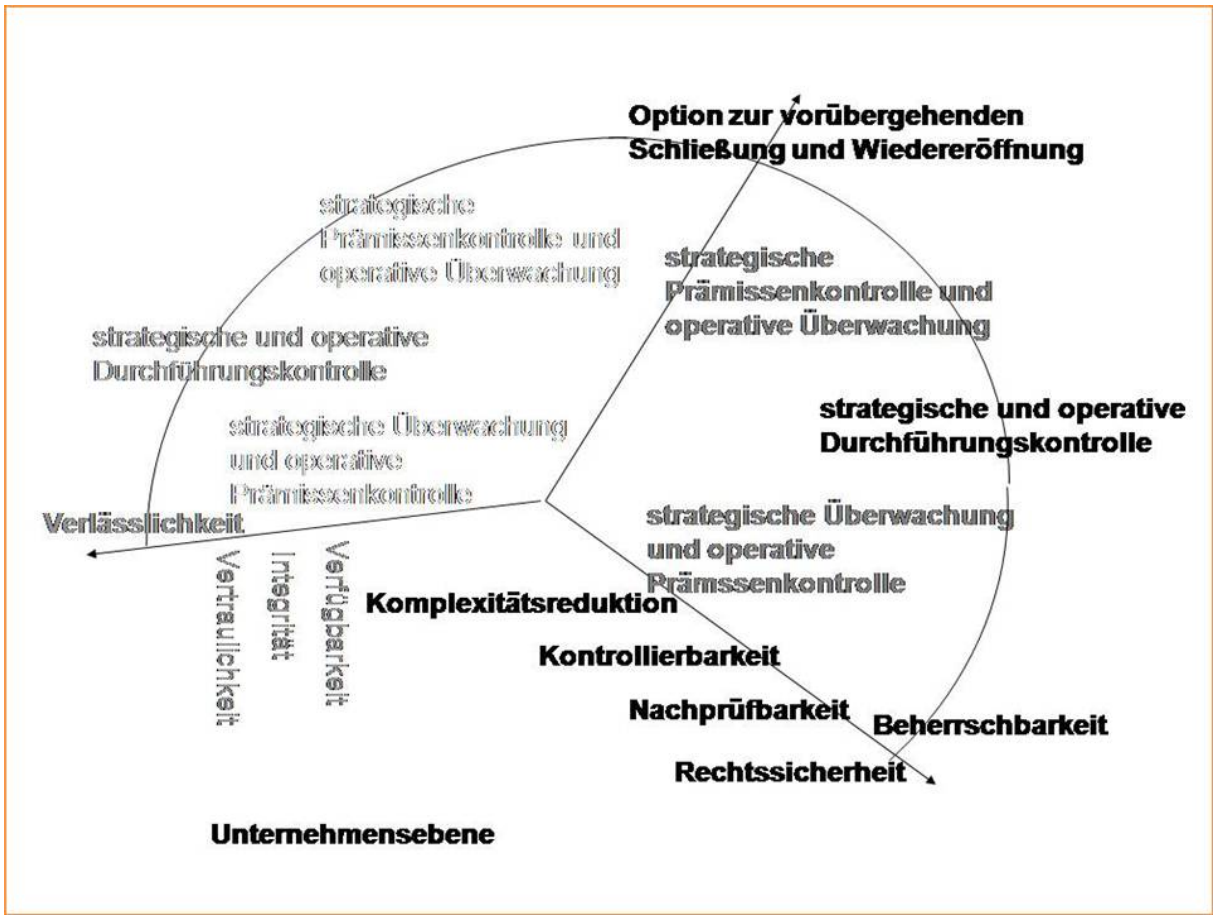


Abb. 31 Unternehmensebene im strategisch-operativen Risiko-Controlling

[1] vgl. Wolf, Klaus (2003b), S.23

In Zusammenhang mit der Führung der Geschäftsfelder sowie Entwicklung und Pflege der Unternehmensstrategie stehen die Minimierung des Realisierungsaufwands der alternativen Geschäftsstrategieoptionen sowie der Beitrag zur Sicherung zwischen- und innerbetrieblicher Kooperation im Mittelpunkt. Von der Unternehmensebene selber her geht es im Zusammenhang mit Stabilisierungs- und Desinvestitionsstrategien um die Option zur vorübergehenden Schließung und Wiedereröffnung.

Die internen Ordnungsmäßigkeitsvorgaben auf dieser Planungsebene geben vor, dass die (zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse) eingesetzte Aufbau- und Ablauforganisation der IT-Projekte zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens vorübergehend ausgesetzt werden kann, um sie später wieder aufzunehmen. Dabei geht es um Geschäftsprozesse und Geschäftsmodelle im Zusammenhang mit der

- Minimierung des Realisierungsaufwands der alternativen Geschäftsstrategieoptionen sowie dem Beitrag zur Sicherung zwischen- und innerbetrieblicher Kooperation

auch bezüglich der Bedeutung

- für Treiber und Aktionsmuster der Unternehmensvernetzung.

Im Rahmen einer Unternehmensvernetzung oder der Evaluierung eines neuen Geschäftsmodells z. B. muss die Möglichkeit bestehen, eine veränderte Aufbau- und Ablauforganisation zu implementieren, und diese Änderungen gegebenenfalls wieder rückgängig machen zu können.

Es ist zu beurteilen, inwieweit die notwendige Beherrschbarkeit

- der für die vorübergehende Aussetzung und spätere Wiederaufnahme benötigten Systeme bzw. zu implementierenden Maßnahmen
- der durch die vorübergehende Aussetzung und spätere Wiederaufnahme beeinflussten Systeme bzw. Maßnahmen

von den im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen relevanten Aspekten/den Anforderungskriterien an die IT-Security abhängig ist.

Die Anforderungen an die Beherrschbarkeit der von der Umsetzung der strategisch-operativen Ziele betroffenen Systeme bzw. zu implementierenden Maßnahmen

- bei der Führung der Geschäftsfelder sowie der Minimierung des Realisierungsaufwands der alternativen Geschäftsstrategieoptionen

sowie dem Beitrag zur Sicherung zwischen- und innerbetrieblicher Kooperation

sollten unabhängig von einer vorübergehenden Neugestaltung der

- (zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse) eingesetzten Aufbau- und Ablauforganisation der IT-Projekte (zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens)

erfüllt sein.

Für einen ex-ante „sicheren“ Ablauf der Software in der Einsatzumgebung sollten die Anforderungen an die Beherrschbarkeit des Softwaresystems unabhängig von einer vorübergehenden Neugestaltung der (zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse) eingesetzten Aufbau- und Ablauforganisation der IT-Projekte (zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens) erfüllt sein. Müssen bei der ‚Führung der Geschäftsfelder sowie der Minimierung des Realisierungsaufwands der alternativen Geschäftsstrategieoptionen sowie dem Beitrag zur Sicherung zwischen- und innerbetrieblicher Kooperation“ Aufbau- oder Ablauforganisation vorübergehend neu gestaltet werden, so sollen die Anforderungen an die Beherrschbarkeit des Softwaresystems unabhängig von dieser vorübergehenden Neugestaltung der Aufbau- oder Ablauforganisation erfüllt sein. Werden z. B. zur Minimierung des Realisierungsaufwands der alternativen Geschäftsstrategieoptionen Aufbau- und Ablauforganisation der IT-Projekte vorübergehend neu gestaltet, so darf die Beherrschbarkeit des Softwaresysteme nicht beeinträchtigt werden.

7 Nutzen der IT-Security

Allgemein wird direkter und indirekter Nutzen unterschieden. Der direkte Nutzen bezeichnet Nutzenpotenziale, die unmittelbar generiert werden, z. B. Senkung der Hardware-, Betriebs- und Wartungskosten in Multiserviceanwendungen. Indirekter Nutzen bezeichnet mittelbar generierten Nutzen (z. B. Mitarbeiterproduktivität) etwa durch Vermeidung indirekter Kosten: Neben Produktivitätsverlusten der Mitarbeiter (z. B. bei fehlender Ausbildung) und Ausfallzeiten von IT-Systemen bei unzureichender Wartung oder Fehlfunktion sind als solche nicht transparente Kosten hier auch Opportunitätsverluste durch die Nichtnutzung technologischer Möglichkeiten (z. B. Datensicherungskonzept) zu nennen.

Das IT-Nutzenpotenzial liegt darin, über die IT-Unterstützung der Geschäftsprozesse die Geschäftsprozesse des Unternehmens effizienter zu gestalten. Die Verbesserung von internen Geschäftsprozessen kann z. B. durch die Beseitigung eventuell vorhandener Medienbrüche bei der Übertragung von Daten über Unternehmensgrenzen hinweg erfolgen. Idealerweise sollte der Informationsfluss von der Datenerfassung vor Ort bis ins Backend-System und umgekehrt nahtlos sein. So wird die Informationsqualität verbessert und der Informationsfluss beschleunigt. Dies setzt eine hohe IT-Sicherheit (im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen: Verlässlichkeit und Beherrschbarkeit) der betroffenen IT-Systeme voraus. Insbesondere für Mobile Business Lösungen sind entsprechende Überlegungen sehr erfolgskritisch.[1]

Um funktionale Kundenanforderungen an IT-Produkte effizient und effektiv in technische IT-Leistungen umzusetzen, wird in der Literatur eine duale Sicht empfohlen, die die technische Sicht der IT mit der Kundensicht der Fachabteilungen verbindet. Der Problemlösungsansatz setzt an der Schnittstelle zwischen IT und Fachabteilung an. Durch die Bereitstellung eines standardisierten IT-Produktkatalogs soll eine effiziente Kommunikation zwischen den beiden Unternehmensbereichen ermöglicht werden. Die Basis des Wandlungsprozesses der bisher technikfokussierten IT-Abteilung hin zur konsequenten Produktorientierung bilden die in dem Produktkatalog abgebildeten Prozess-orientierten IT-Produkte. Ausgangspunkt dafür bilden die Kunden mit ihren Geschäftsprozessen. Diese beziehen IT-Produkte, die einen Nutzen innerhalb ihrer Geschäftsprozesse bringen müssen. IT-Produkte bestehen aus einer oder einem Bündel von IT-Leistungen und sind Output der IT-Produktion. Um den Kunden/die Kundenanforderungen in die Produktentwicklung einzubinden, beschäftigt sich das Service-Engineering mit der „systematischen und methodisch unterstützenden Transformation von

[1] vgl. Tscherwitschke, Hans (2007)

Konzepten in marktfähige Dienstleistungen“. Im Fokus stehen Themen wie Kundenorientierung, Prozessorientierung, Dienstleistungsdesign und Qualitätsmanagement. Der vom Kunden subjektiv empfundene Nutzen eines IT-Produkts macht sich an Kriterien wie Kosten(transparenz), Service-Qualität oder Benutzerzufriedenheit fest. Es ist laufend zu überprüfen, ob der vom Kunden gewünschte Nutzen auch eingetreten ist.[1]

Der Nutzen einer IT-Anwendung wird vor allem in der erfolgreichen Umsetzung der von den Anwendergruppen selbst gestellten Anforderungen, z. B. [2]

- Verbesserung der Datenqualität und Reaktion(szeiten) (auch auf erhöhten Informationsbedarf an neuen Geschäftsobjekten oder Primär-Prozessen, etwa Vertragsanbahnung im Außendienst oder Policierung bei einer Versicherung),
- Verringerung des Personalaufwands,
- Umsetzung von gesetzlichen und betriebsinternen Vorgaben zwischen Unternehmen und (externem) IT-Dienstleister

gesehen. Vor allem bei der Datenqualität (Konsistenz, Korrektheit, Vollständigkeit, Genauigkeit, Zuverlässigkeit, Verständlichkeit) als Nutzenaspekt spielt die IT-Sicherheit operativ eine wichtige Rolle. Im Zusammenhang mit dem Controlling der IT-Security geht es vor allem um strategische Nutzenpotenziale. Der ex-ante Nutzen eines solchen strategischen IT-Security-Managements wurde als Absicherung der Umsetzung von IT-Projekten identifiziert.

Geschäftsprozess-bezogener Nutzen ist auf die Unterstützung von Geschäftsprozessen (auf Basis der umgesetzten IT-Projekte) zurückzuführen, z. B. [3]

- Virtualisierung von Arbeitsplätzen oder
- Optimierung des Kundenservice, d. h. Reaktionsgeschwindigkeit, Erreichbarkeit, freie Wahl und auch Wechsel des Kommunikationsmediums während einer laufenden Transaktion durch den Kunden.

Der Nutzen der Informations- und Kommunikationstechnologie ist indirekter Nutzen und beruht auf Schnelligkeit des Datenaustauschs „sofort, überall, zu allen“ („flächendeckende Vernetzung aller Akteure des beruflichen wie privaten Bereichs“[4]) mittels offener Standards und z. B. dem Internet als Kommunikationsmedium. Zentral ist die IT-Sicherheit bei der Netzintegration mit Kunden, Lieferanten und anderen Geschäftspartnern sowie der Öffnung des

[1] vgl. Zarnekow, Rüdiger (2006)
[2] vgl. Funk-Kadir, Thomas (2006)
[3] vgl. Redenius, Jens O. (2004)
[4] vgl. Stahlknecht, Peter (2003), S.116

Netzes für Fremdgeräte.[1] Dabei spielt das problemlose Roaming zwischen verschiedenen Technologien eine wichtige Rolle.[2]

Von den vier Dimensionen, in denen Wirkungszusammenhänge zur Wertschöpfung im Unternehmen abgebildet werden (Finanzperspektive, Kundenperspektive, interne Prozessperspektive sowie Lern- und Entwicklungsperspektive) ist bezüglich der IT-Sicherheit vor allem die interne Prozessperspektive relevant. IT-Sicherheit liefert ihren Nutzen über die Anwendungen und Applikationen, die diesen Zustand voraussetzen und die Geschäftsprozesse des Unternehmens unterstützen:

Über die Unterstützung der Geschäftsprozesse hat sich die IT zum Business Enabler entwickelt. Dabei führt vor allem das Vertrauen externen Kunden und Partner in die IT-Sicherheit des Unternehmens potenziell zum Aufbau neuer Geschäftsbeziehungen. Produktivitätsbezogene und Business Value Vorhaben bieten die Möglichkeit, den wirtschaftlichen Nutzen der IT zu erhöhen. Dabei stehen als Ziele u. a. die Steigerung der Effektivität (die richtigen Dinge tun) und Effizienz (die Dinge richtig tun) der IT im Mittelpunkt.[3] Bei der Wirtschaftlichkeitsanalyse für neue IT-Anwendungssysteme werden zumeist die Nutzenpotenziale

- Straffung der Geschäftsprozesse bzw. Arbeitsabläufe,
- Verkürzung von Bearbeitungs- und Durchlaufzeiten,
- Steigerung der Produktivität,
- Einsparung von Kosten,
- Erhöhung der Marktanteile oder
- schnellere Verfügbarkeit, erweiterter Umfang, verbesserte Aktualität der Informationen über den betrachteten Geschäftsprozessen

genannt.[4] Die Integration von Unternehmensdaten und -applikationen zur Vereinfachung und Automatisierung von Geschäftsprozessen ermöglicht dabei die gemeinsame Nutzung von Daten und Geschäftsfunktionen über die Grenzen heterogener Applikationen hinweg.

Als Nutzen eines Informations-Sicherheits-Management-Systems nach BS 7799-2:2002 (ISO 27001) wird angegeben [5]

[1] vgl. Helden von, Josef (2006), S.29
[2] vgl. Keuper, Frank (2003), S.246-248
[3] vgl. Pobbig, Heiko (2005)
[4] vgl. Stahlknecht, Peter (2003), S.13
[5] vgl. Rubenschuh, M. (2003)

- Risiken können definiert, eingeschätzt und damit beherrscht werden
- Sicherung der Geschäftskontinuität und Fortbestand des Unternehmens
- Haftungsrisiko (§ 276 BGB) aus Verträgen, aus Delikten (§ 823 ff. BGB) gegenüber Dritten, aus unmittelbaren gesetzlichen Verpflichtungen (z. B. Anlage zu § 9 BDSG, § 87 TKG) wird reduziert
- Nachweis eines geforderten Sicherheitsniveaus (für WP/WPG) Konzentration der Bestandsführung (Klassifizierung und Überwachung von Anlagen und Beständen (HW und SW), Zugriffsüberwachung, Personelle Sicherheit), Sorgfaltspflicht, Risikovorsorge (KonTraG)
- Vertrauensförderung bei Kunden und Investoren durch Orientierung an international anerkanntem Standard
- jede Verbindung des Unternehmens nach innen und außen ist klar definiert (Politik zur Nutzung von Signaturen und Verschlüsselungstechniken, Schutz vor Datenmissbrauch oder Datenverlust, sinnvoller Umgang mit Sicherheitswerkzeugen)

Zur Optimierung dieser Nutzenpotenziale sind diese zu maximieren und abzusichern. Eine adäquate IT-Security/ein adäquates IT-Security-Management kann die Nutzenpotenziale der IT absichern. In Form von geeigneten Eskalations- und Risikobewältigungsstrategien sowie einem geeigneten Business Continuity Planning (Notfallplanung/Incident Management) zielt dies auf die Unterstützung/Herstellung der Handlungsbefähigung ab.

Im Zusammenhang mit dem hier entwickelten IT-Security-Management stehen Maßnahmen zur Risikobeseitigung und Risikoakzeptanz (bezüglich der entsprechenden IT-Projekte) im Mittelpunkt. Der Nutzen einer Maßnahme zur Risikobeseitigung ergibt sich über die Verringerung von Risiken der Unterstützung der Ziele der Geschäftsprozesse, welche sich aus den angestrebten Geschäftsmöglichkeiten ableiten.

Die Risikobewertung kann dadurch objektiviert werden, dass objektive Nutzenfunktionen gesucht werden. Eine Risikoanalyse, welche dabei die subjektive/intersubjektive Komponente bei der Risikobewertung objektiviert, muss Risiken auf der Kostenseite (das sind Risiken vonseiten der IT-Infrastruktur) mit objektiven Nutzenfunktionen aufseiten der Handlungsbefähigung trotz Unsicherheit bewerten. Prozesse, Systeme und Komponenten mit objektiven Nutzenfunktionen können über das Kriterium „Kritikalität“ identifiziert werden. Über eine CMDB (Configuration Management Database) lässt sich aus einer Kritikalitätsbewertung der Prozesse eine Bewertung auch auf Service- und Systemebene ermitteln.

7.1 Security-“Kapital”, Nutzenzufluss der IT-Security, Sarbanes-Oxley-Act-Konformität

Die materiellen Vermögenswerte verlieren für die Steigerung des Unternehmenswerts zunehmend an Bedeutung. Entscheidender sind die immateriellen Vermögenswerte. Immaterielle Vermögenswerte bilden einen erheblichen Anteil am Unternehmenswert. Darüber hinaus gilt für „Intagibles“ das Gesetz vom abnehmenden Grenznutzen nicht, weil immateriellen Gütern die Knappheitseigenschaft fehlt. Der Schlüssel zum wirtschaftlichen Wachstum liegt beim Übergang in eine Wissensgesellschaft in der Geschwindigkeit der kumulativen Wissensverarbeitung mit ihrer unbegrenzten Variation und Verfeinerung.[1]

Der Unterschied zwischen Marktwert und Finanzkapital des Unternehmens wird auf die immateriellen Ressourcen zurückgeführt, die einen Beitrag zum Unternehmenswert liefern. Diese immateriellen Ressourcen können am ehesten durch den Begriff „intellektuelles Kapital“ beschrieben werden. Dieses wird in internes und externes intellektuelles Kapital unterteilt. Das interne intellektuelle Kapital befindet sich im Gegensatz zum externen intellektuellen Kapital im Eigentum des Unternehmens. Es wird auch als Strukturkapital bezeichnet und bezieht sich auf die Leistungsfähigkeit der internen Organisation und das Image des Unternehmens (inklusive Unternehmenskultur und Führungsstruktur). Das Strukturkapital ist dabei Voraussetzung für Aufbau und Nutzung des externen intellektuellen Kapitals. Verfügungsrechte am externen intellektuellen Kapital sind nur im Rahmen vertraglicher Regelungen durchsetzbar. Dieses externe intellektuelle Kapital kann in Human-, Kunden- und Partner-/Allianzkapital differenziert werden. Das Humankapital umfasst das Wissen und die Kompetenz der Mitarbeiter, das Kundenkapital den Kundenstamm und Kundenbeziehungen und das Partner-/Allianzkapital das Potenzial von Partnerschaften/Kooperationen in der Wertschöpfungskette.[2]

Das fundamentale intellektuelle Kapital eines Unternehmens sind seine Geschäftsprozesse (mit dem darin eingebrachten Wissen); angesichts des Wettbewerbs gilt es, diese (z. B. mithilfe von BPM und SOA) so effizient und flexibel wie möglich zu gestalten. Der wichtigste Vorteil der Verknüpfung von Geschäftsprozessmanagement und SOA liegt dabei in der Trennung von Geschäftslogik und IT-Implementierung.[3]

[1] vgl. Kremin-Buch, Beate/ Unger, Fritz/Walz, Hartmut (2004), S.14-16
[2] vgl. Stoi, Roman. (2003), S.175-176
[3] vgl. Peisl, Roland (2006)

Der Wert des intellektuellen Kapitals ist das Ausmaß, in welchem dieses Wissenskapital in einen Finanzertrag für die Unternehmung umgewandelt werden kann.[1] Der Aufbau intellektuellen Kapitals verursacht hohe Kosten. Es ist jedoch ohne resultierende Wertminderung gleichzeitig und mehrfach für verschiedene Zwecke verwendbar. Der Wert wird durch die Nutzung nicht gemindert, sondern teilweise sogar noch erhöht. Beispielsweise steigt das im Rahmen eines Projekts genutzte Wissen eines Mitarbeiters durch die im Projekt gemachten Erfahrungen. Bei der Schaffung von immateriellen Vermögenswerten spielt die Qualität und Adäquanz der investierten (materiellen und immateriellen) Vermögenswerte die entscheidende Rolle. Beispielsweise ist die Erhöhung der internen Prozessexzellenz durch Anschaffung einer neuen Software davon abhängig, ob sich diese für das Unternehmen eignet und wie deren Implementierung erfolgt.[2]

Zu unternehmerischen Erfolgsvoraussetzungen wie Effizienz, Produktivität und Innovation kommen immer stärker Faktoren wie Schnelligkeit, Flexibilität und Früherkennung hinzu. Die Unternehmungen müssen sich zunehmend auf Aspekte wie z. B. Schnelligkeit bei der Erfüllung von Sonderwünschen, die Kommunikation mit den Abnehmern usw. konzentrieren. Die Unternehmen haben zunehmend keine Verhandlungsstärke mehr gegenüber den Kunden, sondern müssen Interaktionen mit potenziellen Kunden anbahnen.[3]

Es reicht nicht mehr aus, nur die klassischen Finanzkennzahlen als Basis für die Unternehmenssteuerung heranzuziehen. Diese Zahlen sind generell vergangenheitsorientiert und für ein schnelles Reagieren sowie zum Ableiten kurzfristiger Korrekturen im operativen Geschäft ungeeignet.[4] Der Bedarf nach aktuellen Informationen steigt also ständig an, nicht zuletzt aufgrund gesetzlicher Verpflichtungen im Rahmen der Corporate Governance. So verpflichtet Section 302 SOX, die Veröffentlichung aller unternehmensrelevanten Meldungen sicherzustellen. Zusammen mit Section 404 werden Anforderungen an das professionelle Management des internen Kontrollsystems gestellt. Section 404 SOX fokussiert auf die Finanzberichterstattung und schreibt die Einrichtung eines internen Kontrollsystems (IKS) vor. Die Forderung nach zeitgerechter Bekanntgabe offenlegungspflichtiger Informationen rückt die Bedeutung von transparenten Abläufen und Kontrollprozessen in den Fokus der Unternehmensleitung. Die Unternehmensleitung wird verpflichtet, das IKS mit einer klar strukturierten und dokumentierten Vorgehensweise zu bewerten. Diese Bewertung wird Be-

[1] vgl. Gomez, Peter (2002), S.140
[2] vgl. Stoi, Roman (2003), S.177
[3] vgl. Hinterhuber, Hans H. (2004a), S.15-17
[4] vgl. Scheer, August-Wilhelm (2005), S.5

standteil der Finanzberichterstattung.[1] Über die Optimierung hinaus gewinnt das Monitoring von Prozessen z. B. aufgrund gesetzlicher Vorschriften zur Corporate Governance und zum Risikomanagement, wie dem Sarbanes-Oxley-Act an Bedeutung. Die Forderung des Nachweises der Effektivität des internen Kontrollsystems im Rahmen des periodischen Unternehmensreportings bedingt, dass die wesentlichen Prozesskontrollen und die zugehörigen Prozesse regelmäßig dokumentiert und auf ihre Wirksamkeit hin überprüft werden. Wenn Prozesse outgesourct (an einen Dienstanbieter ausgelagert) werden, ist ein geeignetes Monitoring zur permanenten Überprüfung der Service Level Agreements auf Einhaltung der Prozessperformance notwendig.[2]

SOX bietet die Chance für eine vollumfängliche „Renovierung" der IT. Die tief greifende Überprüfung aller für Finanzinformationen relevanten Prozesse ist in Bezug auf Sicherheit und Stabilität der darunter liegenden IT-Prozesse und IT-Systeme mit einem aktuellen „Fitness-Check" der IT verbunden. Die Kontrollabläufe in den anwendungsbezogenen Prozessen („IT-Application Controls") sind regelmäßig (intern) zu überprüfen hinsichtlich Vollständigkeit, Genauigkeit, Richtigkeit, Berechtigung und Verteilung der Verantwortung. Die Finanzberichterstattung resultiert aus allen Geschäftsprozessen und Abläufen, die Einfluss auf das Finanzergebnis haben, das sind grundsätzlich alle Geschäftsprozesse im Unternehmen. Diese sind zumeist in Business-Applikationen eingebunden, welche auf der installierten IT-Infrastruktur basieren. Zu den Ebenen der IT-Infrastruktur, die damit ebenfalls im Fokus der SOX-Compliance stehen, gehören Datenbanken, Betriebssysteme und Netzwerke. Die Kontrollprozesse und -abläufe der IT-Infrastruktur („IT General Controls") sind hinsichtlich der Kernaspekte Entwicklungsprozesse, Änderungs-Management, Systembetrieb, Zugriff auf Daten und Anwendungen und Kontrollmechanismen regelmäßig (intern) zu überprüfen. Über die IT-Application Controls und die IT General Controls Kontrollprozesse ist eine Eingrenzung der IT-Prozesse und IT-Systeme des Unternehmens bezüglich der SOX-Compliance Relevanz möglich. Es muss jedoch nicht nur die so definierte Ordnungsmäßigkeit sichergestellt werden. SOX-Compliance fordert auch, entsprechende Kontrollabläufe zu installieren, die belegen können, dass keine Umgehung der Ordnungsmäßigkeit stattgefunden hat.[3]

Information stellt also einen der wichtigsten zu schützenden Werte dar. In Form von Wissen muss sie bei Bedarf schnell und strukturiert nutzbar sein.[4] Unternehmen schützen ihre Werte

[1] vgl. Menzies, Christof (2004)
[2] vgl. Scheer, August-Wilhelm (2005), S.V,VI
[3] vgl. Schäfer, Gernot (2006)
[4] vgl. Elsässer, Wolfgang (2005), S.127

durch technische und organisatorische Maßnahmen. Zu diesen Werten gehören auch die IT-Systeme und Daten, welche die Grundlage wesentlicher Geschäftsprozesse bilden. Die Daten, die Nutzer über Websites und Internet-Portale (z. B. als E-Mail) hinterlassen, gelten als das Kapital des Internet-Handels. Diese Daten sind vor Missbrauch zu schützen. Der Wert von Informationen wird durch die Größen Vertraulichkeit, Integrität und Verfügbarkeit determiniert. Daraus abgeleitete Aspekte sind z. B. Privacy, Authentizität und Verifizierbarkeit. Security bildet einen Zusatzwert eines Informationssystems. Sie ermöglicht die revisionssichere und verantwortungsvolle Ausführung von Applikationen auf diesem IT-System.[1] IT-Sicherheit soll zudem neue Möglichkeiten für computer- bzw. internetbasierte Geschäftsprozesse eröffnen, indem z. B. der flexible und komfortable elektronische Informationsaustausch abgesichert wird.[2]

IT-Sicherheitslücken und die von ihnen ausgehenden Gefährdungspotenziale sind nicht unmittelbar sichtbar und somit ihre Auswirkungen schwer abschätzbar. Sicherheitslücken entstehen dabei auch durch unkoordinierte oder unvollständige Maßnahmen. Vor diesem Hintergrund ist ein konkreter IT-Sicherheitsprozess (z. B. nach den Vorgaben des Grundschutzhandbuchs des BSI) ausgehend von Planung über Umsetzung bis zur kontinuierlichen Überwachung notwendig, um die mit der Anwendung der Informationstechnik verbundenen Risiken zu minimieren.[3]

Ein Ansatz für eine Ertragsrechnung auf das in die IT-Sicherheit investierte Kapital geht davon aus, dass Sicherheitsinvestitionen den Abzug von Werten verhindern.[4] Dies ist aber nicht qualifizier- noch quantifizierbar. Wichtiger sind positive Effekte (Nutzenzufluss), z. B.:

- Das AktG und das KonTraG stellen an AGs und große GmbHs die Forderung, dass sich aus dem Geschäftsbetrieb ergebende Risiken (dies betrifft auch IT-Risiken z. B. bei einem Unternehmen, das auf eine funktionierende Netzwerkinfrastruktur angewiesen ist) abgesichert, d. h. z. B. versichert oder durch Rückstellungen berücksichtigt werden müssen. Kann z. B. infolge von IT-Security-Investitionen nun nachgewiesenermaßen das Gefährdungspotenzial reduziert werden, so lassen sich Rückstellungen auflösen, was unmittelbar den free cash flow des Unternehmens erhöht.
- Bei Versicherungen z. B. gegen Geschäftsausfälle durch IT-Katastrophen belohnen Versicherungen Sicherungsmaßnahmen zur Absicherung des versicherten Risikos bei

[1] vgl. Cazemier, Jacques A./Overbeek Paul L./ Peters, Louk M.C. (2004), S.9,10
[2] vgl. Rieger Holger (2005a), S.26
[3] vgl. Rieger Holger (2005a), S.19
[4] vgl. Kruth, Wilhelm (2004), S.6

ihrem Versicherungsnehmer häufig mit geringeren Versicherungsprämien. Dies wirkt sich noch schneller positiv auf die Barmittel aus.

- Das Rating des Unternehmens durch Kreditinstitute wird bei nachgewiesener IT-Sicherheit positiv beeinflusst
- Umsatzsteigerungen infolge von Zusatzgeschäften durch sichere, neue Geschäftsmöglichkeiten oder Reduzierung des Administrationsaufwands z. B. in der Benutzerverwaltung durch moderne Single Sign-on Lösungen.

Das „Kapital“ der IT-Security ist die Effektivität und Effizienz des IT-Security-Managements und soll dem organisatorisch-technischen Strukturkapital zugeordnet werden. Das organisatorisch-technische Strukturkapital wieder rum ist Teil des „organisationalem Kapital“. „Kapital“ der IT-Security stellt kein Kapital im Sinne des Finanziellen Kapitals dar, man kann hier auch keinen Kapitalfluss annehmen. Es ist auch nicht quantitativ bewertbar. Im Zusammenhang mit der SOX-Compliance resultieren Effektivität und Effizienz, mithin „Kapital“ der IT-Security aus der regelmäßigen internen Anpassung und Optimierung die Kontrollabläufe in den anwendungsbezogenen Prozessen („IT Application Controls“) und der Kontrollprozesse und -abläufe der IT-Infrastruktur („IT General Controls“).

Nimmt man an, dass das Unternehmen nur dann „überlebt“, solange es über eine ausreichende Menge an „organisationalem“ Kapital verfügt[1], so wird auch modelltheoretisch der Zusammenhang zwischen IT-Security und „Überleben“ des Unternehmens klar.

Das Organisationswissen und die Analyse der organisatorischen Beziehungen gewinnen immer mehr an Bedeutung. In Unternehmen mit flachen Hierarchien und stark vom Wissen der Mitarbeiter abhängigen Prozessen hängt der Erfolg z. B. immer stärker davon ab, dass die richtigen Mitarbeiter effizient, über zeitliche und räumliche Grenzen hinweg zusammenarbeiten und kommunizieren. Ad-hoc Interaktion, Collaboration und Arbeiten in Communities vermischen sich mit gut strukturierten Abläufen. Hier ist das Management gefragt, um Freiheitsgrade und Motivation des einzelnen Mitarbeiters mit Ergebnisorientierung und Erwartungen bezüglich Effektivität und Effizienz zu verbinden.[2]

[1] vgl. Woywode, Michael (1998), S.50,51
[2] vgl. Scheer, August-Wilhelm (2005), S.VI

7.2 Risikowirkung: Einfluss auf Unternehmenswert/Rating nach Basel II

Vor allem im Rahmen des Ratings nach Basel II ist das „organisationale Kapital“ (Finanzielles Kapital, Soziales Kapital und Humankapital) der entscheidende Faktor für die Beurteilung der Zukunftsfähigkeit des Unternehmens. Finanzielles Kapital wird ex-post aus dem Jahresabschluss ersichtlich. Soziales Kapital und Humankapital sind im Jahresabschluss aber nicht erkennbar, da sie weder quantifizierbar noch (nach geltendem Recht) bilanziell aktivierbar sind. Die Überprüfung dieser qualitativen Größen soll aber ermöglichen, Gefahrenpotenziale frühzeitig zu erkennen. Die Effektivität und Effizienz des IT-Security-Managements ist als Teil des organisatorisch-technischen Strukturkapitals Teil des internen intellektuellen Kapitals und ein Faktor im Rahmen eines Ratings nach Basel II.

Wichtigster Erfolgsmaßstab im Zusammenhang mit Risikomanagement ist stets die Steigerung des Unternehmenswerts.[1] Mit zunehmender Shareholder-Value-Orientierung/ Ausrichtung der Unternehmensziele auf den Unternehmenswert soll das Risikomanagement in die wertorientierten Managementsysteme integriert werden. So soll sich eine verbesserte Unternehmensführung und -kontrolle (Corporate Governance) ergeben.[2]

Wesentliche Bestandteile einer wertorientierten Unternehmensführung sind Risiko- und Ertragsmanagement.[3] Leitidee des Shareholder-Value-Konzepts ist die Ausrichtung der Unternehmensführung auf die ökonomischen Interessen der Eigentümer. Danach wird der Shareholder-Value als „ein auf die Marktwertmaximierung ausgerichtetes wertorientiertes Konzept der Unternehmensführung definiert, das den Nutzen des Aktionärs als Maßstab unternehmerischen Handelns vorgibt“. Dabei geht es um die Aktivierung und Nutzung aller unternehmerischen Potenziale.[4]

Bei der Bewertung von Unternehmen ermittelt der Wirtschaftsprüfer in der Rolle eines neutralen Gutachters mit nachvollziehbarer Methodik einen objektivierten Wert des Unternehmens. Der objektivierte Unternehmenswert wird dabei als „typisierter Zukunftserfolgswert“ definiert, der sich „bei Fortführung des Unternehmens in unverändertem Konzept und mit allen realistischen Zukunftserwartungen“ im Rahmen u. a. „sonstiger Einflussfaktoren“ ergibt. Eine sachgerechte Unternehmensbewertung erfordert die Herleitung der dem Bewertungszweck entsprechenden Annahmen. Unternehmensbewertungen werden dabei u. a.

[1] vgl. Finke, Robert (2005), S.23
[2] vgl. Wolf, Klaus (2003b), S.3
[3] vgl. Horváth, Péter (2006), S.747
[4] vgl. Ritter, Michael (2000), S.5

vor dem Hintergrund des Kaufs, Verkaufs von Unternehmen, Fusionen, Management Buy Out oder im Rahmen von wertorientierten Managementkonzepten vorgenommen.[1]

Eine Erhöhung des Unternehmenswerts ist nicht alleine durch eine Verbesserung der Ertragsaussichten möglich: Ein proaktives Risikomanagement ist zur Sicherung des Fortbestands des Unternehmens unverzichtbar. Aber auch im Zusammenhang mit einem Rating nach Basel II können sich durch ein dokumentiertes Risikomanagement beim Unternehmen direkte finanzielle Vorteile in Form besserer Kreditkonditionen ergeben. Diesen Vorteil kann das Unternehmen z. B. an die Eigenkapitalgeber weitergeben, was in der Regel zu einer höheren Börsenkapitalisierung führt.

Auch organisatorische und strukturelle Maßnahmen für die IT-Sicherheit wie auch Security-Projekte können darüber hinaus Einfluss auf den Unternehmenswert haben:

- durch ein konstant hoch aufrechterhaltenes IT-Sicherheitsniveau werden Kosten infolge von Schäden der IT des Unternehmens durch innere und äußere Angriffe vermieden. Eine negative Differenz der Investitionen zur Aufrechterhaltung eines konstant hohen IT-Sicherheitsniveaus und der ohne diese Investitionen zu erwartenden Kosten infolge von Schäden der IT des Unternehmens durch innere und äußere Angriffe stellen einen zusätzlich dem Unternehmen entziehbaren Überschuss dar. Allerdings ergibt sich hier das Problem, diese Kostenersparnis zu quantifizieren.
- IT-Sicherheit kann Voraussetzung für die Realisierbarkeit von Projekten (Strategieänderung, Produktionsprogrammerweiterung, Globalisierung) des potenziellen Unternehmenserwerbers sein, welche zusätzlichen Einzahlungsüberschuss erwarten lassen.

Das Shareholder-Value-Konzept verlangt u. a., dass die Unternehmensmittel in die „besten“ Verwendungsmöglichkeiten gelenkt werden.[2] Die gezielte Steigerung des Unternehmenswerts ist durch die Nutzung realwirtschaftlicher Flexibilität (Realoptionen) möglich.[3] Um solche Realoptionen zu „erzeugen“ sind Investitionen notwendig[4], eventuell auch in IT-Security-Projekte. Auf die Nutzung von Realoptionen bezüglich der mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens bei der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse zielt das in dieser Arbeit entwickelte Modell ab. Bezüglich der IT-Security ist dies innerhalb der

[1] vgl. IDW (2000a): S1, TZ 11,12,17
[2] vgl. Ritter, Michael (2000), S.5
[3] vgl. Hommel, Ulrich (2001), S.26
[4] vgl. Niemann, Rainer (2001, S.40

Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in den Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume zu analysieren.

7.3 Dauerhafte, nachhaltige IT-Sicherheit als langfristiger Wachstumsfaktor/Werttreiber?

Der Wert eines Unternehmens kann im Wesentlichen anhand der Parameter Rentabilität, Wachstum und Risiko ausgemacht werden, die direkt miteinander verknüpft sind. Bei steigendem Risiko und gleich bleibender Rentabilität sinkt der Unternehmenswert.[1]

Damit hat eine dauerhafte, nachhaltige IT-Sicherheit, die Risiken der IT-Sicherheit vermeidet oder begrenzt bei gleich bleibender Rentabilität einen direkt den Unternehmenswert steigernden Effekt.

Darüber hinaus wird in zunehmendem Maße erkannt, dass beeinflussbare, nicht monetäre Erfolgsfaktoren für die Erreichung strategischer Ziele maßgeblich sind. So wird z. B. beim Ansatz der Balanced Scorecard erkannt, dass einzelne Prozesse, Teilprozesse, Bündel von Aktivitäten/Funktionen strategische Treibergrößen darstellen können.[2]

Die Operationalisierung der Wertorientierung durch sog. Werttreiber steht im Mittelpunkt der Geschäftssteuerung. Unter Werttreibern sind die „inhaltlichen Ursachen für die markt- und kundenbezogenen Wirkungen in den Erfolgsfaktoren“ zu verstehen.[3]

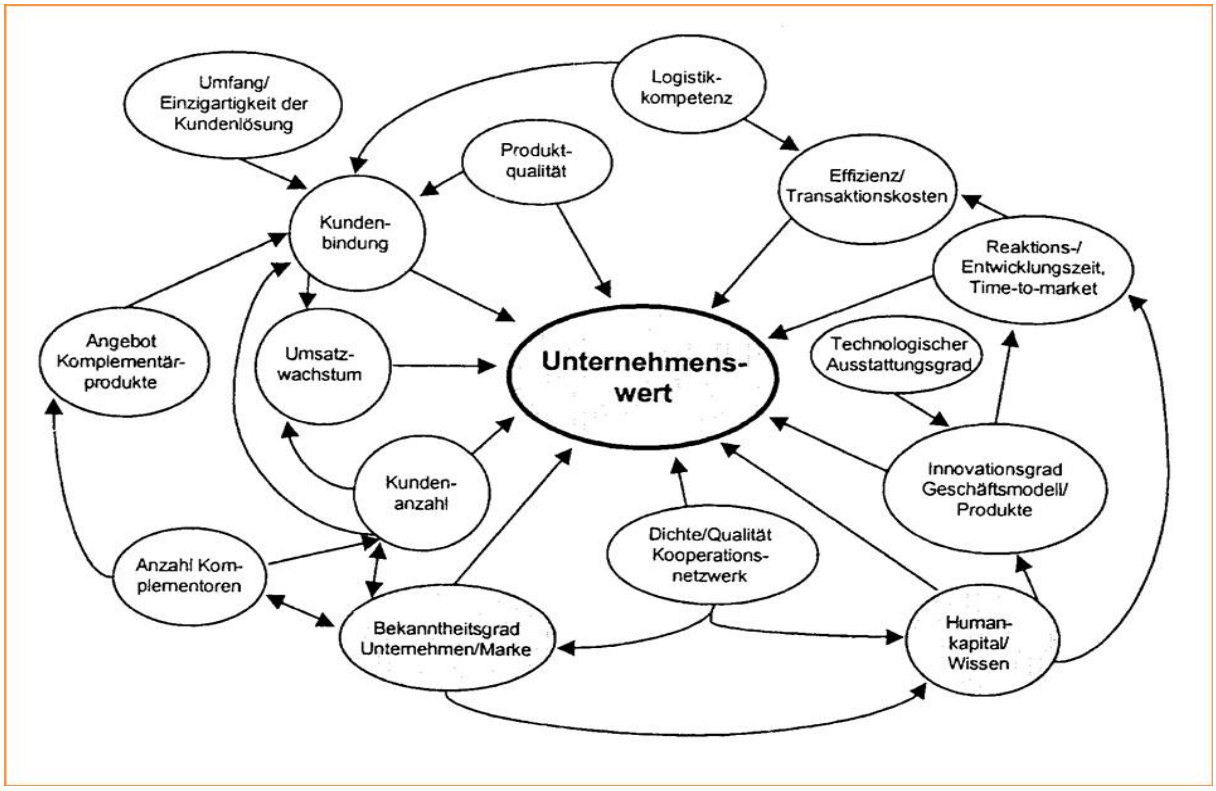
Die Balanced Scorecard wurde entwickelt, um das Herausarbeiten der Werttreiber nicht nur auf die finanzielle Ebene zu beschränken, sondern dies – auch in ihren Zusammenhängen – über die Kunden-, die Performance- und die infrastrukturelle Perspektive hinweg zu forcieren und dies „im Sinne einer Entwicklungsperspektive zu dynamisieren“. Der Effekt z. B. von „Ressourcen getriebenen Strategien“, im Sinne von intra- oder interorganisationalen Kombinationen oder des Innovationsmanagements (Geschäftskonzeptinnovation, technische Wertinnovation, einfache Neuentwicklung von Produkten und Systemen) werden damit hinterfragt und beantwortet. Fragen der Strategieentwicklung und -implementierung gehen so ineinander über.[4]

Strategien zielen darauf ab, den Wert des Unternehmens zu steigern. Wenn klar ist, wie sich der Weg dahin darstellt, was dabei die zentralen Werttreiber sind, und wie diese zusammen-

[1] vgl. Romeike, Frank (2004), S.253
[2] vgl. Rosenkranz, Friedrich (2006), S.11
[3] vgl. Wolf, Klaus (2003b), S.24
[4] vgl. Seidenschwarz, Werner/Huber, Christian (2002), S.127,128

wirken, dann wird auch die Bewertung von Strategien im Selektionsprozess wertschöpfend. Werttreiber sind Einflussfaktoren der zukünftigen Free Cash Flows und damit des Shareholder Values. Neben dem Umsatzwachstum und der Rentabilität ist das Risiko ein primärer Werttreiber im Unternehmen. Unternehmen, die einen effizienten Risikomanagementprozess einführen, haben Kostenvorteile und damit auch Wettbewerbsvorteile. Wer am Markt überleben will, muss das Risiko-Chancen-Profil der Unternehmen optimieren. Risikomanagement muss als Basis einer wertorientierten Unternehmenssteuerung verstanden werden. In den ursprünglichen Ansätzen der wertorientierten Konzepte wird mit sog. Wertgeneratoren gearbeitet. Diese ermöglichen grundsätzlich eine Schnittstelle zur strategischen Planung. Dabei werden fünf Arten von Wertgeneratoren unterschieden: Umsatzwachstum, Gewinnmarge, Investitionen ins Anlage- und Umlaufvermögen sowie Kapitalkosten und Ertragssteuern.[1]

Der für eine praktische Umsetzung dieses wertorientierten Konzepts notwendige Konkretisierungsgrad erfordert die Identifizierung der Antriebskräfte dieser Wertgeneratoren und die Darstellung und Quantifizierung dieser Antriebskräfte in ihrem Zusammenwirken.[2]



(Quelle: Stoi, Roman. (2002), S.157)

Abb. 32 Wichtiger Werttreiber der New Economy

Natürlich besitzen nicht alle „weichen" Faktoren die gleiche Relevanz für den Unternehmenserfolg. So birgt eine schwache Performance in einem sehr relevanten Erfolgsfaktor ein hohes

[1] vgl. Seidenschwarz, Werner/Huber, Christian (2002), S.127
[2] vgl. Seidenschwarz, Werner/Huber, Christian (2002), S.127

Risikopotenzial, während eine hohe Performance in einem weniger relevanten Erfolgsfaktor auch auf die Ineffizienz hindeutet, sich nicht auf die relevanten Faktoren konzentrieren zu können.[1] Der Business Value der IT ergibt sich aus der Unterstützung der Geschäftsprozesse. Der Business Value der IT-Sicherheit ergibt sich aus Anwendersicht aus der Beherrschbarkeit und damit der Akzeptanz der die IT-gestützten Geschäftsprozesse unterstützenden IT-Systeme und -Prozesse. Dabei ist Compliance als „negativer Treiber" zu sehen: Der Nutzen entsteht hier dadurch, dass es keine rechtlichen Risiken in Form drohender Sanktionen gibt. Für das Unternehmensmanagement stehen die Optimierung der vorhandenen, und die Ermöglichung neuer, sicherer Geschäftsprozesse im Vordergrund.

Diese Optimierung der Geschäftsprozesse ist heute ohne eine serviceorientierte Architektur als technischer Basis-Infrastruktur nicht mehr denkbar. SOA-basierte Anwendungen funktionieren aber z. B. nicht ohne Identity Management. „Man kann keine sicheren Geschäftsprozesse realisieren, die sich über mehrere Anwendungen oder sogar die Unternehmensgrenzen hinweg erstrecken, ohne die Identitäten über diese Anwendungen hinweg zu beherrschen".[2]

Identity Management ist Grundlage für die Umsetzung von Geschäftsprozessen, neuen Anwendungen und Geschäftsmodellen. In der technischen Sichtweise geht es um die Authentifizierung von Benutzern und die Autorisierung von Zugriffen. Auf mehr organisatorischer Ebene stehen z. B. Rights Management, Privacy und Compliance.[3]

Eine dauerhafte, nachhaltige IT-Sicherheit könnte als langfristiger Wachstumsfaktor des Unternehmens folgendermaßen angesetzt und modelliert werden: Basis dafür ist z. B. das Value-Driven-Modell von Copeland/Koller/Murrin, in dem das durch das Produkt aus Nettoinvestitionsrate (NIR) und Rentabilität der Nettoinvestition (ROIC Return on Invested Capital) bestimmte Wachstum des Unternehmens dem Wachstum des NOPLAT (Net operating profit less adjusted taxes) folgt. Dieses Modell eignet sich besonders für Planungen auf Basis eines ex-ante festgelegten Unternehmenskonzepts. Der entscheidende Faktor in diesem Modell ist die Rentabilität der Nettoinvestition, Return on Invested Capital (ROIC) = Net operating profit less adjusted taxes (NOPLAT)/invested capital.[4]

[1] vgl. Reichling, Peter (2003), S.122
[2] Kuppinger, Martin (2005b), S.16
[3] vgl. Kuppinger, Martin. (2005a)
[4] vgl. Dolezch, Timm (2003), S.17-19

Betrachtet man als Teil des ROIC den Return on Security Investment, welcher z. B. als (ALE + Net Present Value)/invested capital definiert wird[1] (ALE Annulized Loss Expectance), und wird drohender Schaden aus der Fehlfunktion einer von der Sicherheitsinvestition betroffenen IT-Komponente (als eher kurzfristigem und nicht sinnvollem Teil des Return on Security Investment) nicht betrachtet, so entspricht der NOPLAT dem Net Present Value der Investition in IT-Sicherheit.

Der NOPLAT einer Investition in IT-Sicherheit ergibt sich also als Net Present Value aus den neuen Geschäftsmöglichkeiten, die durch die Sicherheitsinvestition ermöglicht werden sowie den direkten und indirekten Kosteneinsparungen durch die Sicherheitsinvestition.

Zur Unterstützung der Möglichkeit zur Aktivierung und Nutzung aller unternehmerischen Potenziale bei gleichzeitig Strategie-bezogenem IT-Management und Nutzen bringendem Einsatz der IT, gewährleistet das entwickelte strategisch-operative IT-Security-Management die Unterstützung/Herstellung der Handlungsbefähigung

- zur Absicherung der Strategiebezogenheit (Effektivität) und von Nutzenpotenzialen (Effizienz) der IT

Dies unterstützt auch die zu unternehmerischen Erfolgsvoraussetzungen wie Produktivität und Innovation hinzukommenden Faktoren wie Schnelligkeit und Flexibilität in Form der Nutzung von Realoptionen bezüglich der (mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden) Geschäftsprozesse und Geschäftsmodelle des Unternehmens bei der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse. Gleichzeitig ist der Business Value der IT-Sicherheit bzw. Security als Zusatzwert eines Informationssystems zu beachten. Security als Zusatzwert eines Informationssystems ermöglicht die revisionssichere und verantwortungsvolle Ausführung von Applikationen auf diesem IT-System. Der Business Value der IT-Sicherheit ergibt sich darauf basierend aus der Beherrschbarkeit und Verlässlichkeit der die IT-gestützten Geschäftsprozesse unterstützenden IT-Systeme und –Prozesse.

Wenn das Unternehmen

- (zur Optimierung der Geschäftsprozesse und Geschäftsmodelle) bei der Umsetzung der Unternehmensstrategie/IT-Security-Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses/der IT-gestützten Geschäftsmodelle bzw. Ab-

[1] vgl. Mayer, Barbara (2003)

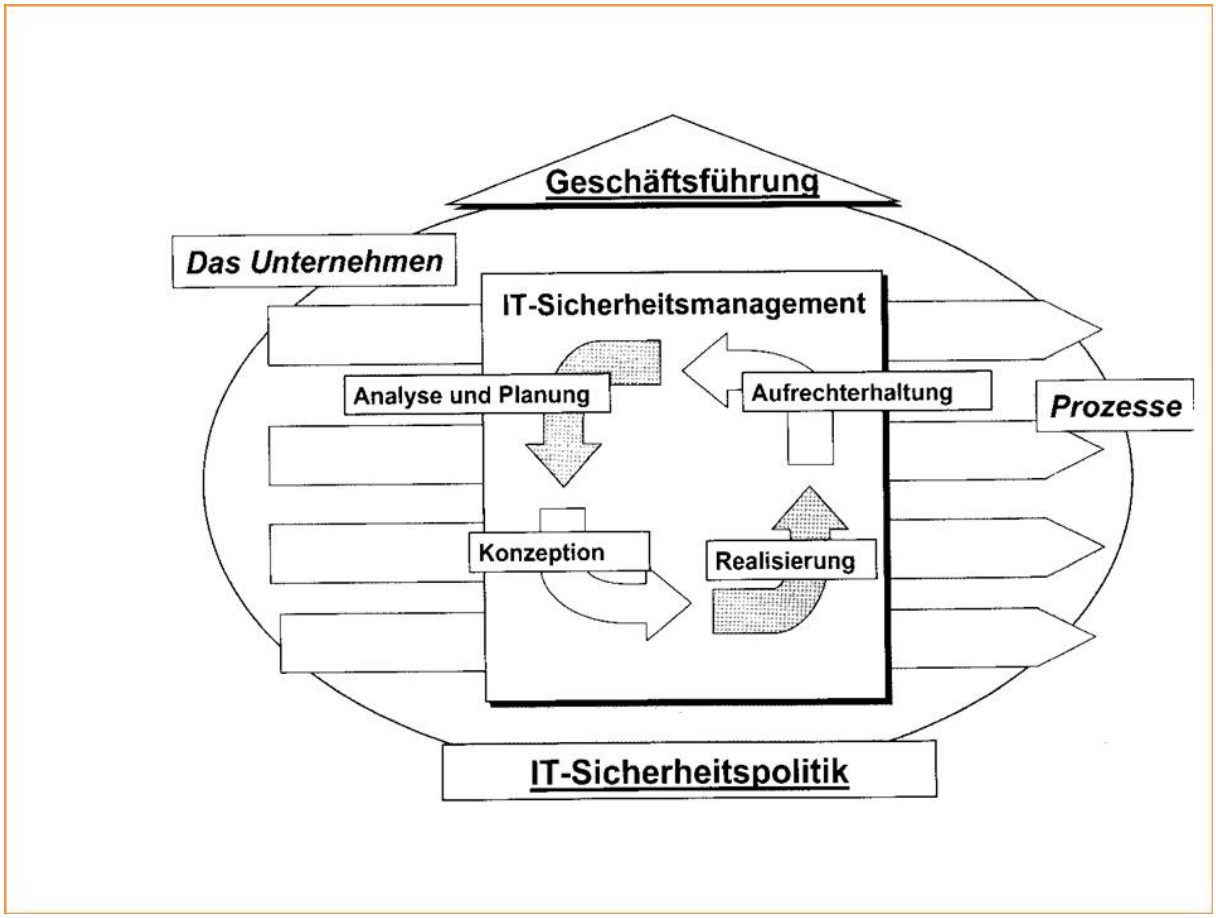
stimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander

Realoptionen (bezüglich der eingesetzten Technologien, Methoden und Anwendungen der IT-Projekte sowie der entsprechenden Aufbau- und Ablauforganisation) ausübt, so müssen die Anforderungen der Beherrschbarkeit und Verlässlichkeit weiterhin erfüllt sein.

Die ex-ante Absicherung der Strategiebezogenheit und von Nutzenpotenzialen der IT bzw. die Absicherung der Effektivität und Effizienz der IT erfolgt durch die Absicherung der Priorisierung und Umsetzung von IT-Projekten. Die Priorisierung - in Form der auf die Entwicklungen im Umfeld des Unternehmens (Strategie konform) angepassten Auswahl der Projekte - wird durch die Integration der Bedingungen zur Anpassung an die Umgebung bezüglich der IT-Security in das entwickelte strategisch-operative IT-Security-Management abgesichert. Die Umsetzung wird dadurch abgesichert, dass die Möglichkeiten zur Wahl von Optionen in den Projekten unterstützt werden sollen ohne dass die Sicherheit der betroffenen IT-Systeme beeinträchtigt wird.

8 Vorgehensmodell zur Sicherheitsstandard-unabhängigen Ausgestaltung der Sicherheit von Informationssystemen

Als Arbeitsobjekt der Revision und des Controllings der IT-Security kann der IT-Security-Prozess betrachtet werden. Dieser implementiert ein koordiniertes Vorgehen, um kontinuierlich den IT-Security-Bedarf zu ermitteln (Analyse und Planung), IT-Security-Konzepte zu erstellen (Konzeption), umzusetzen (Realisierung) und regelmäßig zu prüfen, ob die realisierten Sicherheitsmaßnahmen immer noch den aktuellen Anforderungen entsprechen (Aufrechterhaltung, Analyse): Das entsprechende Sicherheitsmanagement kann ebenfalls in diesen vier Phasen beschrieben werden.



(Quelle: Rieger, Holger (2005b), S.64)

Abb. 33 Der IT-Security-Prozess

Aufgabe der Revision der IT-Security ist u. a. die Ausgestaltung der Effektivität dieses IT-Security-Managements derart, dass dieses die – sich aus der Anpassung an das rechtliche Umfeld ergebende – notwendige Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security erfüllt. Das Vorgehensmodell zur Sicherheitsstandard-unabhängigen Ausgestaltung der Sicherheit von Informationssystemen soll die Effektivität und Effizienz dieses

IT-Security-Managements so gestalten, dass diese nicht nur die notwendige, sondern auch die hinreichende Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security ist. Diese hinreichende Bedingung leitet sich aus Überlegungen zur Anpassung an das organisatorische und das technische Umfeld ab. Sie besagt, dass das Nutzenpotenzial der IT, welches darin liegt, über die IT-Unterstützung der Geschäftsprozesse die Geschäftsprozesse des Unternehmens effizienter zu gestalten, bezüglich der IT-Security optimiert werden soll. Die Optimierung dieses Nutzenpotenzials ist u. a. Aufgabe des Controllings der IT-Security.

Der IT-Security-Prozess kann mit einem Informationssicherheits-Managementsystem implementiert werden, wobei das strategische Informationssicherheits-Managementsystem (der strategische Teil des entwickelten strategisch-operativen IT-Security-Managementsystems) das operative Informationssicherheits-Managementsystem (den operativen Teil des entwickelten strategisch-operativen IT-Security-Managementsystems) führt und steuert. Zur Steuerung des IT-Security-Prozesses kann das Informationssicherheits-Managementsystem die Werkzeuge IT-Risikomanagement und IT-Prozesscontrolling verwenden. In Form von (strategischer und operativer) Prämissenkontrolle, (strategischer und operativer) Überwachung und (strategischer und operativer) Durchführungskontrolle werden damit Komponenten modelliert, die der Unterstützung der Strategieformulierung und -umsetzung sowie zur Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander dienen.

Das IT-Risikomanagement und das IT-Prozesscontrolling können sich an dem in Kapitel 5 entwickelten IT-Security-Framework orientieren, welches die Strategieebene mit der Ebene der IT-Security/IT-Sicherheit verbindet. Dieses Framework verbindet diese beiden Ebenen in Form der Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in den Kontext Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume.

In das entwickelte Modell zum strategischen Risiko-Controlling integriert, bildet das so ausgestaltete IT-Security-Management den Anpassungsprozess bezüglich der IT-Security an das rechtliche und technisch-organisatorische Umfeld des Unternehmens ab:

Insgesamt sollen die auf die Unterstützung/Herstellung der strategisch-operativen Beweglichkeit/Handlungsbefähigung ausgerichteten Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security gewährleistet werden. Es soll ein Anpassungsprozess an die „Umgebung“ bezüglich der IT-Security abgebildet werden, der über die Komponenten strategische Prämissenkontrolle, strategische Durchführungskontrolle und strategische Überwachung die

Formulierung und Realisierung der IT-Security-Strategie steuert, über die Komponenten operative Prämissenkontrolle, operative Durchführungskontrolle und operative Überwachung die angestrebte IT-Security und die Geschäftsprozesse aufeinander abstimmt, und auf die Unterstützung/Herstellung der strategisch-operativen Beweglichkeit/Handlungsbefähigung abzielt.

Das strategisch-operative Risiko-Controlling steuert einerseits die Formulierung und Realisierung von Strategien. Diese Überwachung und Steuerung findet in Form des strategischen Performance Managements (bestehend aus strategischer Prämissenkontrolle, strategischer Durchführungskontrolle und strategischer Überwachung) statt Strategie-umsetzung unter Berücksichtigung von Sicherheitsaspekten bedeutet, über eine Einschätzung der Geschäftsprozesse hinsichtlich ihrer Sicherheitsziele die an den Geschäftsrisiken der Organisation orientierten Sicherheitsanforderungen mit entsprechenden Maßnahmen abzu-decken.. Im strategischen Teil des strategisch-operativen IT-Security-Managements über-wacht und steuert das strategische Performance Management die Formulierung und Realisierung der Strategie. In Form des operativen Performance Managements hat das strategisch-operative Risiko-Controlling außerdem die Unternehmensziele und den IT-Security-Prozess aufeinander abzustimmen. Dies ist Aufgabe des operativen Teils des strategisch-operativen IT-Security-Managements.

Eine entsprechend ausgestaltete Effektivität und Effizienz des durch Integration des klassischen IT-Security-Managements/des IT-Security-Prozesses in das entwickelte strategische Risiko-Controlling ausgebauten strategisch-operativen IT-Security-Managements ist Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security. Diese Be-dingungen werden über das entsprechend auszugestaltende strategische und operative Per-formance Management in das auf die strategisch-operative Beweglich-keit/Handlungsbefähigung abzielende Modell zum strategisch-operativen Risiko-Controlling integriert. Diese strategische Sicht auf die IT und die damit verbundene Informationssicher-heit bildet den Ansatz für ein konzernweites, ganzheitliches Sicherheitsmanagementkonzept und damit einen effektiven Schutz der digitalen Geschäftsprozesse.

Dieses IT-Security-Management kommt der Forderung des „management control“ nach, zum Zweck der Überwachung aller Sicherheitsprojekte des Unternehmens geforderten Systeme zur Unterstützung der Strategieformulierung und -umsetzung in ein zu implementierendes oder bestehendes Informationssicherheits-Managementsystem zu integrieren. Zudem werden damit geeignete (Kontroll- und Überwachungs-) Strukturen zur kontinuierlichen, evolutionären Weiterentwicklung des Risikomanagements/IT-Security-Managements und Anpassung der

Sicherheitsmaßnahmen an die sich verändernden Anforderungen der Geschäftsmodelle und Geschäftsprozesse/Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander geschaffen.

Die operative Überprüfung findet in Form von SOLL/IST-Vergleichen – der auf Basis der aktuellen Sicherheitslücken der IT-Systeme konzeptionierten – mit den realisierten Sicherheitsmaßnahmen statt. Hierbei ist auch zu prüfen, ob Systeme oder Prozesse geändert wurden, was gegebenenfalls eine Rückkehr zur Analysephase erfordert.

Zur Kompensation der Selektionsrisiken bei der Fokussierung auf die wichtigsten Prämissen dienen die (strategische und operative) Durchführungskontrolle und die (strategische und operative) Überwachung. Auswirkungen unvorhergesehener Störungen in der zukünftigen Entwicklung sollen als Abweichungen sichtbar gemacht werden. Dabei sind Informationen zu sammeln, die auf zukünftige Umsetzungsgefahren hindeuten. Umsetzungsrisiken resultieren aus unzureichender Handlungsbefähigung bei der Umsetzung der Unternehmensstrategie/Abstimmung der Unternehmensziele und der Geschäftsprozesse aufeinander.

Die Komponenten (strategische und operative) Prämissenkontrolle, (strategische und operative) Durchführungskontrolle und (strategische und operative) Überwachung sollen die korrekte Bestimmung der Anwendbarkeit und die konsequente Umsetzung bestehender Methoden, Standards, Tools und Best Practices zur Umsetzung der Unternehmensstrategie und Abstimmung der Unternehmensziele und der Geschäftsprozesse aufeinander sicherstellen.

Es geht um die zur Durchsetzung/Umsetzung der Strategie erforderliche IT-Security der von der Durchsetzung/Umsetzung/Implementierung der Strategie betroffenen IT-Systeme bzw. um die zur Unterstützung der Durchsetzung/Umsetzung/Implementierung von IT-gestützten Geschäftsmodellen erforderliche IT-Security der für die entsprechenden Geschäftsmöglichkeiten notwendigen IT-Systeme. Die Sicht des IT-Systems auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen – der Kontext Verlässlichkeit (beurteilt nach den Kriterien Verfügbarkeit, Integrität und Vertraulichkeit) – und die Sicht der Betroffenen (Anwender/Benutzer) auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen – der Kontext Beherrschbarkeit des Systems (mit den Aspekten Komplexitätsreduktion und Kontrollierbarkeit beurteilt z. B. nach den Kriterien Nachprüfbarkeit und Rechtssicherheit) – bezieht sich dann auf die bei IT-gestützten Geschäftsmodellen erforderliche IT-Security der diese unterstützenden IT-Systeme.

Im Folgenden werden die Phasen des in ein solches IT-Security-Management integrierten IT-Security-Prozesses beschrieben. Die Einteilung orientiert sich an der Erhebung und dem Vergleich von Soll- und Ist-(Prüfungs)Objekten.

8.1 Erstellen einer IT-Security Policy

Prozesse dienen der Umsetzung strategischer Ziele und sind immer an langfristige, strategische Vorgaben angebunden. Mit diesen Vorgaben werden die „Leitplanken“ zur Orientierung und zum „Andocken“ an die Unternehmensstrategie für die Prozesse gelegt, innerhalb derer dann die Prozesse gestaltet und umgesetzt werden können. Diese Vorgaben sind mit Prämissen, also Grundannahmen z. B. über die Entwicklung des Umfelds unterlegt. Bei jeder Initiative bezüglich Prozessmanagements sind die Anknüpfungspunkte der Prozesse zur Strategie festzulegen.[1] Diese Leitplanken sind die Vision/das Leitbild.

Eine Strategie besteht aus einer Vision und Aktionen. Die Vision beschreibt ein mehrdimensionales Zielgebäude mit den zentralen Elementen Leitbild sowie strategische Kompetenzen und strategische Positionen. Aktionen beschreiben die Visionsumsetzung mit den Bausteinen Konsequenzen, Maßnahmen, strategische Programme und Projekte.[2] Die im Leitbild enthaltenen Grundwerte werden auch als „policies“ oder „practices“ bezeichnet. Sie charakterisieren grundsätzliche Verhaltensweisen.[3]

Die Sicherheitsrichtlinien eines Systems oder einer organisatorischen Einheit legen die „Menge von technischen und organisatorischen Regeln, Verhaltensrichtlinien, Verantwortlichkeiten, Rollen und Maßnahmen fest, um die angestrebten Schutzziele zu erreichen“.[4] In der Sicherheitsrichtlinie sind Vorgehensweisen, Standards und Best Practices festzulegen. Die entsprechenden internen Ordnungsmäßigkeitsvorgaben sollten auf die der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume abzielen. Sie beziehen sich auf die Relevanz und Anwendbarkeit der festgelegten Methoden, Standards, Tools und Best Practices zur Erreichung des Ziels der Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit (bei der Realisierung/Umsetzung der Unternehmensstrategie bzw. die Abstimmung der Unternehmensziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander), sowie die Kritikalität/Sensitivität entsprechender Sachwerte und Prozesse. Durch Integration der Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security wird die

[1] vgl. Stöger, Roman (2005), S.45,49
[2] vgl. Fink, Alexander (2001), S.162
[3] vgl. Fink, Alexander (2001), S.166
[4] vgl. Eckert, Claudia (2003), S.20

Realisierung/Umsetzung der Unternehmensstrategie bzw. Abstimmung der Unternehmensziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander auf die Realisierung/Umsetzung der IT-Security-Strategie bzw. Abstimmung der Unternehmensziele und des IT-Security-Prozesses bzw. Abstimmung der IT-Security-Ziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander spezialisiert. Die Ordnungsmäßigkeitsvorgaben stehen in Verbindung mit Aufbau- und Ablauforganisation und/oder dem Einsatz von Technologien, Methoden und Anwendungen zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse. Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse zielt ab auf – mit Nutzenpotenzialen der IT in Verbindung stehende – aufbau- und ablauforganisatorische Optimierung der Aufgabenerfüllung und/oder optimalen Einsatz und Implementierung/Umsetzung der entsprechenden Technologien, Methoden und Anwendungen.

Vor dem Einsatz von Policies und Regelwerken ist dabei eine umfassende Risikoanalyse durchzuführen, um die schützenswerten Elemente zu identifizieren. Dabei sind auch die Anforderungen zu analysieren, die zur Erreichung der strategischen Zielsetzung notwendig sind. Das Audit ist dabei die erste Wahl zur Feststellung von Schwachstellen und bildet die Grundlage, um die Schwachstellen eines IT-Systems zu beseitigen. Audits haben jedoch den Nachteil, dass sie Situationen punktuell betrachten: wenn z. B. heute nur die notwendigen Ports an einem System offen sind, so ist nicht garantiert, dass in wenigen Stunden nicht auch sicherheitskritische Ports offen sind. Es ist eigentlich ein permanentes Auditing System notwendig, das eine permanente Überwachung aller sicherheitskritischen Parameter/Zustände gewährleistet.[1] Ein solches System ist im Übrigen jedoch im Allgemeinen nicht realisierbar, wenn man bedenkt, dass Risiken der IT-Sicherheit nicht vorhersehbar sind.

Die Bedingung, dass die Anforderungen an die IT-Security der von der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander betroffenen IT-Systeme unabhängig von der eventuellen Ausübung entsprechender Realoptionen durch das Unternehmen erfüllt sein sollen, können in die Security Policy aufgenommen werden. Zwecks regelmäßiger bzw. permanenter Überprüfung der Security Policy ist bezüglich der Prämissen eine (strategische und operative) Prämissenkontrolle einzurichten, welche die bei der Formulierung der Strategie/für die Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander gesetzten Prämissen (die An-

[1] vgl. Perdich, Peter (2004)

nahmen, wie kritisch die Konformität mit entsprechenden Ordnungsmäßigkeitsvorgaben ist) auf ihre auch zukünftige Gültigkeit prüfen soll. Die Kritikalität/Sensitivität der Sachwerte und Prozesse bezieht sich (entsprechend den Überlegungen zur Anpassung an das organisatorische Umfeld bzw. Anpassung der Organisation an das Umfeld sowie zur Anpassung an das technische Umfeld bzw. Anpassung der technisch-organisatorischen Konzepte an das Umfeld), auf die Konformität mit den Ordnungsmäßigkeitsvorgaben. Diese Prämissenkontrolle ist Voraussetzung, um die auf diesen Prämissen basierenden Vorgaben zur Legung der „Leitplanken“ zur Orientierung und zum „Andocken“ an die Unternehmensstrategie für die Prozesse (und den IT-Security-Prozess), innerhalb derer dann die Prozesse (und der IT-Security-Prozess) gestaltet und umgesetzt werden können, ständig anpassen und aktuell halten zu können.

Als Voraussetzung für die Implementierung der unternehmensweiten IT-Sicherheit muss das Management den Stellenwert der IT-Sicherheit für den Geschäftsbetrieb feststellen und in Leitlinien und Regelungen für die tägliche Arbeit festschreiben. Die Leitlinie legt als sog. Sicherheitspolitik die Sicherheitsziele und damit das angestrebte ganzheitliche Sicherheitsniveau fest. Sie stellt damit auf der obersten Ebene der Regelungspyramide eine zentrale Richtlinie für den Umgang mit IT-Systemen und Daten dar. Konkretisiert in allgemeinen sicherheitsorientierten Verhaltensweisen stellen sie verbindliche Vorgaben für die übrigen Geschäftsprozesse dar, sie formulieren die für alle Prozesse des Unternehmens gültigen Eckpfeiler der IT-Sicherheit. Sie werden vom IT-Sicherheitsmanagement ausgearbeitet und von der Unternehmensführung als verbindliches Dokument erlassen. Typisches Beispiel ist eine Richtlinie zur Verschlüsselung: Es wird vorgegeben, wann und wie Daten zu verschlüsseln sind. Die übrigen Prozesse müssen diese Richtlinie in ihre Abläufe in der jeweiligen Ausprägung integrieren.[1] Zur Prüfung der unternehmensweiten Sicherheitspolitik muss zunächst festgestellt werden, ob die unternehmensweite Policy zentral definiert und in den Teilsystemen umgesetzt wurde. Dabei sind Teilsicherheitskonzepte entsprechend der Risikoanalyse der Geschäftsprozesse zu bewerten.[2]

Nach IT-Grundschutzhandbuch des BSI dokumentiert eine Information Security Policy/Sicherheitspolitik, welche strategische Position die Unternehmensleitung zur Erstellung und Umsetzung des Sicherheitskonzepts und zur Erreichung der IT-Sicherheitsziele

[1] vgl. Rieger, Holger (2005b), S.65-72
[2] vgl. Ferre, David (2003), S.38

einnimmt. Diese IT-Sicherheitsziele sollen bei der Erstellung der Information Security Policy bestimmt werden.

Eine IT Security Policy ist das Dokument, in dem das Management einer Organisation die wesentlichen Leitlinien und Regelungen festlegt, die die IT-Sicherheit über den gesamten Verantwortungsbereich gewährleisten. Sie enthält Regeln, Prüfvorschriften und Reaktionsverfahren, eingefasst in Audit- oder Prüfvorgängen z. B. mit Checklisten für Mitarbeiterbefragungen.[1]

Nach ISO TR 13335-1 wird zwischen drei Arten der Sicherheitspolitik unterschieden: unternehmensweite Sicherheitspolitik (Corporate Security Policy), unternehmensweite IT-Sicherheitspolitik (Corporate IT-Security Policy) und Sicherheitspolitik des IT-Systems (IT System Security Policy).

Die Corporate IT-Security Policy soll die grundlegenden Sicherheitsprinzipien und -direktiven, die sich aus der unternehmensweiten Sicherheitspolitik ergeben, als auch für den generellen Einsatz der IT-Systeme widerspiegeln. Die unternehmensweite Sicherheitspolitik enthält dabei die Sicherheitsprinzipien und -direktiven für die Organisation als Ganzes und adressiert auch Persönlichkeitsrechte, gesetzliche Anforderungen und Standards. Der Umfang einer Corporate IT-Security Policy ist abhängig von Unternehmensgröße und -komplexität. Dieses zentrale Dokument enthält Aussagen zu den Sicherheitsanforderungen der Organisation und der Informationswerte, zu rechtlichen Aspekten und weitere wesentliche Rahmenbedingungen zur Etablierung und Erhaltung eines angemessenen Niveaus der Informationssicherheit.

Auf Basis der von der Geschäftsleitung verabschiedeten IT-Security Policy sollte die Auseinandersetzung mit bestandsgefährdenden Risiken aus dem IT-Umfeld und die Formulierung detaillierter Maßnahmen zur IT-Sicherheit in einem unternehmensspezifischen IT-Sicherheitskonzept erfolgen. Teilbereiche dabei sind das Datensicherungskonzept, Intra-/Inter-/Extranet-Sicherheitskonzept und die Notfallplanung.

Im Zusammenhang mit der Sicherheit von Informationssystemen geht es um IT-System Security Policies, die aus der Corporate IT-Security Policy auf das einzelne IT-System herunterzubrechen sind. Im Allgemeinen ist also eine unternehmensweite Sicht auf die gesamte IT-Landschaft notwendig. Das IT-Sicherheitsmanagement ist im Zusammenhang mit Revision und Controlling der IT-Security unternehmensweit zu sehen.

[1] vgl. Ferre, David.(2003), S.38

8.2 Bestimmung des Schutzbedarfs der IT-Prozesse, -Systeme, der verarbeiteten Daten und Informationen

Dies ist die Phase „Analyse und Planung“ des obigen IT-Sicherheitsmanagements, in der alle relevanten IT-Systeme zu identifizieren und auf Sicherheitslücken zu prüfen sind. Ferner sind die Risiken bzw. Anforderungen zu bewerten, die durch diese Sicherheitslücken bzw. Kritikalität/Sensitivität entstehen. Auf dieser Grundlage kann dann festgelegt werden, welche Sicherheitslücken bzw. Anforderungslücken zu schließen sind und welche Sicherheitsprojekte begonnen werden müssen.

Diese Phase ist zusammen mit der Erstellung eines Dokuments, in dem das Management einer Organisation die wesentlichen Leitlinien und Regelungen festlegt, die die IT-Sicherheit über den gesamten Verantwortungsbereich gewährleistet, die Phase Plan des ISO 27001.

Ausgangsbasis zur Konkretisierung und Umsetzung der generellen Anforderungen und die Ausrichtung des Unternehmens im Hinblick auf Sicherheit (d. h. die Sicherheitspolitik) ist ein Überblick über die Geschäfts- und Supportprozesse des Unternehmens, z. B. in Form einer Prozessarchitektur. In dieser sind alle Prozesse, ihre Bedeutung für das Unternehmen sowie ihr Zusammenspiel darzustellen. Basis dafür ist eine sog. Business Impact Analyse, mit der alle kritischen Prozesse identifiziert werden, z. B. anhand folgender Fragestellungen: [1]

- Wie ist der Prozess aufgebaut, wer ist daran beteiligt und was wird mit ihm bezweckt
- Welche Ressourcen werden zu seiner Durchführung benötigt
- Welche internen oder externen Unterstützungsleistungen sind zu erbringen
- Welche Parallel-Prozesse sind für die Durchführung zusätzlich bedeutend
- Wie hoch könnte bei seinem Ausfall der finanzielle bzw. Reputationsschaden sein

Entsprechend den Sicherheitsanforderungen, Folgen von Sicherheitsverletzungen, rechtlichen Rahmendaten (Gesetze, Vorschriften, Ausführungsbestimmungen), Schnittstellen (vorgelagert, nachgelagert, unterstützend)), Stammdaten (Kapazität, Umsatz, Deckungsbeitrag, strategische Bedeutung) erfolgt eine Zuordnung der Prozesse in Kritikalitätsklassen. In einer Detaillierungsebene werden die Geschäftsprozesse in Prozessschritte unterteilt und die Informationssysteme und sonstigen Hilfsmittel angegeben, die sie unterstützen. Anschließend wird eine Schutzbedarfsanalyse für jedes Informationssystem erstellt. Die Bestimmung des Schutzbedarfs ist Grundlage für den Einsatz von IT-Sicherheitsmaßnahmen. Um IT-Sicherheit wirtschaftlich einzusetzen, muss sich dabei der Aufwand des Schutzes immer am

[1] vgl. Schneider, Oliver/Giefer, Katrin (2006), S.47

Wert der zu schützenden Daten und Informationen orientieren. Die Ergebnisse der Schutzbedarfsanalyse können in einer zentralen Prozessinformations-/Schutzbedarfsdatenbank abgelegt werden, auf die berechtigte Personen über ein Portal zugreifen können. Bei Ausfall eines Servers oder einer anderen Komponente kann so festgestellt werden, welche Informationssysteme und Geschäftsprozesse davon betroffen sind.[1]

Zunächst sind über eine Einschätzung der Geschäftsprozesse hinsichtlich ihrer Sicherheitsziele die an den Geschäftsrisiken der Organisation orientierten Sicherheitsanforderungen zu identifizieren. Sind die wesentlichen Geschäftsprozesse bekannt und priorisiert, ist die Zuordnung zu den Applikationen und der IT-Infrastruktur vorzunehmen. Für die so identifizierten Applikationen mit höherem Schutzbedarf erfolgen eine Bedrohungs- und eine anschließende Risikoanalyse. Dies sog. Risk Identification und Assessment kann sich z. B. an folgenden Fragestellungen orientieren: [2]

- Welche Risiken können die zugrunde liegenden Geschäftsprozesse beeinträchtigen?

Es sind auch Risiken zu identifizieren, die in der Vergangenheit noch nicht aufgetreten sind aber dennoch vorhanden sein können. Risiko-Awareness ist hier der Schlüssel.

Des Weiteren ist im Rahmen des Assessments zu untersuchen

- welche risikovermeidenden, -minimierenden bzw. –transferierenden Maßnahmen wurden eingeleitet bzw. welche wären wünschenswert

8.3 Ist-Analyse der technischen und organisatorischen Sicherheitsmaßnahmen, Analyse der Anforderungen, Auswahl geeigneter Maßnahmen zur Erfüllung des Schutzbedarfs

Dies ist die als „Realisierung“ bezeichneten Phasen des obigen IT-Sicherheitsmanagements, in der die Sicherheitsmaßnahmen zu erarbeiten sind, um die in der Analysephase festgestellten Sicherheitslücken zu schließen. Das können auch organisatorische Maßnahmen wie Richtlinien, Verfahrens- und Arbeitsanweisungen sein. In modernen ganzheitlich orientierten Sicherheitssystemen werden so auch die konkreten Personen mit ihren Rollen und Aufgaben im Unternehmen geprüft.[3]

Diese Phase entspricht der Phase Do des ISO 27001.

[1] vgl. Müller, Klaus-Rainer (2003) , S.47-50
[2] vgl. Schneider, Oliver/Giefer, Katrin (2006), S.47,48
[3] vgl. Ferre, David (2003), S.39

Um die in der Analysephase festgestellten Sicherheitslücken zu schließen, kann man (wenn die auf die strategische Zielsetzung einwirkenden und deren Erreichung gefährdenden Risiken nicht vorhersehbar/abschätzbar sind), präventiv alle Anforderungen abdecken, die entsprechend der Kritikalität/Sensitivität der betreffenden IT-Objekte relevant sind. In der Analysephase werden dann die das Erreichen der strategischen Zielsetzung beeinflussenden Anforderungen analysiert. Daraus leitet man Maßnahmen ab, die anstatt den ex-ante nicht identifizierbaren Risiken entgegen zu wirken, die identifizierten Anforderungen abdecken.

Häufig sind es neue Gesetze oder sonstige Auflagen, die geänderte betriebliche Abläufe notwendig machen. Um diese Änderungen mit einer durchgängigen Prozesskontrolle für ein hohes Maß an Effizienz in zentralen Geschäftsabläufen zu realisieren, bietet sich eine Business Process Management (BPM) -Lösung an. Damit wird eine Implementierung vollständiger Prozessmodelle über alle Abteilungen hinweg möglich. Das technische Fundament für schlanke Prozesse und kurze Reaktionszeiten bilden dabei Service-orientierte Architekturen (SOA), womit Unternehmen flexibel konfigurierbare Prozessbausteine realisieren.

SOA zielt darauf ab, Geschäftsprozesse schnell und einfach an neue Anforderungen anpassen zu können. SOA bietet hierfür das Konzept der Services, die über eine Service-Middelware unternehmensweit aber auch unternehmensübergreifend benutzt werden können. Es werden Mechanismen für die Interaktion zwischen Anwendungen bzw. den verwendeten und bereitgestellten Services geliefert. SOAs gewinnen immer mehr an Bedeutung, da insbesondere mit Web-Services die Integration von Diensten innerhalb und außerhalb des Unternehmens erheblich erleichtert wird. Mithilfe solcher Dienste wird die Umsetzung von Geschäftsprozessen durch die Abstraktion der Schritte des Geschäftsprozesses als Services vereinfacht.

Das SOA-Konzept will vor allem die Transformation vom „eng gekoppelten“ zu „lose gekoppelten“ Anwendungen durchführen. Lose gekoppelte Anwendungen enthalten sozusagen pure Geschäftslogik-Abläufe und trennen die Service-Schnittstelle von der zugrunde liegenden Architektur. Es wird eine lose Kopplung zwischen Anbieter und Abnehmer ermöglicht.[1] In der Anwendungslandschaft aus Anwendungsbausteinen mit klar modellierten Schnittstellen, die über wohl definierte Services miteinander kommunizieren, wird somit die Komplexität von Abhängigkeiten reduziert. Dies wiederum unterstützt die Aufgabe des IT-Risikomanagements als wichtigem Bestandteil des IT-Security-Managements, Abhängigkeiten zwischen verschiedenen Bedrohungen, Kausalketten sowie potenzielle Angriffsziele zu

[1] vgl. Dampf, Manfred (2006)

reduzieren, da der zugrunde liegenden Architektur und somit auch Angriffspunkte prinzipiell nicht erkennbar sind.

Um die Geschäftslogik rasch an veränderte Anforderungen anpassen zu können, müssen die Geschäftsregeln unabhängig von den technischen Rahmenbedingungen entwickelt werden. Dazu sorgt der Business-Rules Ansatz für die Kapselung der Geschäftslogik innerhalb von Services. Vermeintlich kleine Änderungen in der Geschäftslogik sollen so keine umfangreichen Änderungen der entsprechenden Anwendungen mehr erforderlich machen. Die Geschäftslogik soll in den Business-Rules leicht verständlich abgebildet und von den Fachexperten, den Business-Rules Ownern unabhängig von den Anwendungen gepflegt werden.[1]

Die Prozessbausteine werden über eine BPM-Lösung orchestriert. BPM steuert und verwaltet die Geschäftslogik und abstrahiert die darunter liegenden Technologien. Das von SOA extrahierte Prozesswissen wird auf technischer Ebene über einen Enterprise Service Bus oder eine vergleichbare Middelware gesteuert. Einzelne oder neue Prozesse sind so schnell in übergreifende Abläufe einbindbar und – da Regeln für die Prozessabläufe getrennt von der Technologie bearbeitet werden – sind Änderungen recht einfach umzusetzen. Der Nutzen der integrierten Arbeitsabläufe kann durch die Integration zusätzlicher Informationssysteme erhöht werden. Um dem Optimierungspotenzial im Einzelnen auf die Spur zu kommen, erfolgt eine strukturelle Analyse der vorhandenen Abläufe mit anschließender Gegenüberstellung des Soll-Prozesses.[2]

Mit Business-IT-Alignment wird eine konsequente Ausrichtung der IT an den Geschäftsprozessen des Unternehmens gefordert. Hierzu müssen neben den Abhängigkeiten in der Infrastruktur auch die Zusammenhänge von Geschäftsanforderungen, Service-Nutzung und Service-Inhalt bekannt sein. Dabei nehmen mit der laufenden Standardisierung und Schichtentrennung durchgeführten Umsetzung von Plattformstrategien in der IT-Architektur die Abhängigkeiten in der IT-Infrastruktur zu. Andererseits treiben auch Service-orientierte Softwarearchitekturen die Abhängigkeiten in den IT-Komponenten.[3]

Im Mittelpunkt steht die Unterstützung/Herstellung der strategisch-operativen Beweglichkeit (bei der Formulierung und Umsetzung der Unternehmensstrategie und Abstimmung der Unternehmensziele und der Geschäftsprozesse (und auch des IT-Security-Prozesses) aufeinander) im Mittelpunkt. Um diese zu unterstützen, ist nach den Ergebnissen aus Kap. 6.3 zu gewährleisten, dass folgende Anforderungen erfüllt sind:

[1] vgl. Schärtel, Markus/Peitzker, Stefanie (2006)
[2] vgl. Rother, Tobias (2006)
[3] vgl. Heinrich, Torsten (2006):, S.39

- Verlässlichkeit (und auch Beherrschbarkeit) der betreffenden Systeme bzw. zu implementierenden Maßnahmen unabhängig von einem Betriebszustandswechsel der Ressourcen, der Verbreiterung der Ressourcenbasis und der damit eventuell einhergehenden Variation des Outputs der IT-Projekte
- Verlässlichkeit und Beherrschbarkeit der betreffenden Systeme bzw. zu implementierenden Maßnahmen unabhängig von einer Erweiterung oder Zusammenführung der IT-Projekte
- Verlässlichkeit und Beherrschbarkeit der betreffenden Systeme bzw. zu implementierenden Maßnahmen unabhängig von einer kooperativen Zusammenführung von IT-Projekten/gemeinsamen Nutzung von IT-Prozessen
- Beherrschbarkeit (und auch Verlässlichkeit) der betreffenden Systeme bzw. zu implementierenden Maßnahmen unabhängig von der eventuellen Umsetzung neuer Geschäftsprozesse/Geschäftsmodelle
- Beherrschbarkeit der betreffenden Systeme bzw. zu implementierenden Maßnahmen unabhängig von einer vorübergehenden Neugestaltung der IT-Prozesse

Diese Forderungen sind von einem entsprechend ausgestalteten strategischen und operativen Performance Management abzudecken. Damit soll gewährleistet werden, dass ex-ante die Erreichung der strategisch-operativen Ziele des Unternehmens durch eine mangelnde IT-Security nicht (negativ) beeinflusst wird.

Um zu evaluieren, welche Sicherheitselemente zur Absicherung der Informations- und Kommunikationstechnik (IuK) zur Vermeidung von Notfällen und Katastrophen durch Prävention eingesetzt werden können, sind die Komponenten der IuK, ihre Infrastruktur und ihr Umfeld zu analysieren.[1]

Zur Überprüfung der vorhandenen Strukturen im Unternehmen gehört die Bestandsaufnahme der vorhandenen Hard- und Software sowie des Status der Geschäftsprozesse, eine Risiko-(Schwachstellen- und Bedrohungs-) -analyse, eine Überprüfung der bisherigen Maßnahmen auf Vollständigkeit, Widerspruchsfreiheit, Angemessenheit und Beurteilung hinsichtlich „Stand der Technik“.

Das Ergebnis der Risikoanalyse zeigt Handlungsfelder auf, die durch geeignete Maßnahmen zur Risikominderung abzudecken sind. Diese Maßnahmen sollen wirtschaftlich (angemessen) sein.

[1] vgl. Müller, Klaus-Rainer (2003), S.108-111

Traditionellen Sicherheitssystemen mangelt es oft an ausreichendem Schutz speziell für Webapplikationen. Eine Maßnahme zur zusätzlichen Absicherung dieser Applikationen stellen WebShields/Web Application Firewalls (WAF) dar. Diese sollen Web-Anwendungen vor Angriffen über das im Internet verwendete Protokoll HTTP schützen. Gegenüber klassischen Firewalls und Intrusion Detection Systemen (IDS) überwacht eine WAF dazu die Kommunikation auf der Dienstebene. Damit sollen die Anforderungen der Ebene Sieben des OSI.-Modells (Open Systems Interconnection Reference Model) sichere Datenübertragung, E-Mail Verkehr und Remote Log-in abgedeckt werden.

Die Umsetzung der Maßnahmen erfolgt als internes Projekt. Die Überwachung aller Sicherheitsprojekte und Teilschritte (z. B. Richtlinienerstellung, Basisschutzanalyse, Applikationsanalyse) sowie die Überwachung aller zeitnahen Bedrohungen (z. B. Policy-Verstöße, Zugriffsschutzverletzungen, erkannte Intrusion-Versuche, erkannte Firewall-Angriffe, Virus-/Wurmbefall) soll sowohl während der Maßnahmenumsetzung als auch fortlaufend im IT-Sicherheitsmanagement erfolgen. Die Sicherheitselemente beziehen sich auf einzelne Phasen bzw. Teilschritte der Geschäftsprozesse oder den gesamten Ablauf. Dementsprechend werden phasenspezifische und phasenübergreifende Elemente unterschieden. Des Weiteren gibt es Sicherheitselemente, die sich auf die als Betriebssicherheit bezeichnete Safety und solche, die auf die als Schutz vor Angriffen und die (im Zusammenhang mit der gegebenen Thematik im Mittelpunkt stehende) Gewährleistung der Handlungsfähigkeit bezeichnete Security abzielen.

Um die korrekte Umsetzung zu gewährleisten, ist eine (strategische und operative) Durchführungskontrolle einzurichten. Diese hat im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen zu gewährleisten, dass die notwendige Verlässlichkeit und Beherrschbarkeit der von der Umsetzung der Strategie/Abstimmung der Unternehmensziele und der Geschäftsprozesse (auch des IT-Security-Prozesses) aufeinander betroffenen Systeme bzw. zu implementierenden Maßnahmen gegeben sind. So sollen Strategie-Umsetzungsgefahren/Gefahren bei der Abstimmung der Unternehmensziele und der Geschäftsprozesse (des IT-Security-Prozesses) aufeinander, aufgedeckt werden. Diese Beherrschbarkeit und Verlässlichkeit kann entsprechend den Überlegungen zur Anpassung an das organisatorische Umfeld bzw. Anpassung der Organisation an das Umfeld als gefährdet angesehen werden bei

- Nichterfüllung der Anforderungen an die Konformität mit internen Ordnungsmäßigkeitsvorgaben in Verbindung mit Aufbau- und Ablauforganisation und
- aufbau- und ablauforganisatorisch nicht-optimaler Aufgabenerfüllung in Verbindung mit Nutzenpotenzialen der IT.

Strategie-Umsetzungsgefahren und Gefahren bei der Abstimmung der Unternehmensziele und der Geschäftsprozesse (des IT-Security-Prozesses) aufeinander ergeben sich andererseits aus Überlegungen zur Anpassung an das technische Umfeld bzw. Anpassung der technisch-organisatorischen Konzepte an das Umfeld bei

- nicht optimalem Einsatz und Implementierung/Umsetzung der Technologien, Methoden und Anwendungen zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse in Verbindung mit Nutzenpotenzialen der IT.

Um Betriebssicherheit zu erreichen, genügt es nicht, nur den Betrieb als solchen abzusichern. Im Vorfeld müssen bereits eine Vielzahl von Maßnahmen geplant/ergriffen werden, um die Betriebssicherheit zu ermöglichen. Die Gestaltung eines ausfallsicheren Betriebs ist bereits bei der Systemarchitektur zu berücksichtigen.[1]

Die Sicherheitsarchitektur gibt einen Rahmen vor und stellt einen Überblick der notwendigen, der möglichen und der vorhandenen Sicherheitselemente dar. Diese Sicherheitselemente sind auf einem hohen Abstraktionsniveau dargestellte Bereiche von Sicherheitsmaßnahmen, z. B. Datensicherung, Katastrophenvorsorge, Identifizierung und Authentifizierung. Diese Elemente ergeben sich z. B. aus Lebenszyklus-Betrachtungen der Geschäftsprozesse bzw. sie unterstützenden Informationssystemen von der Planung über Spezifikation, Entwicklung, Test und Betrieb bis hin zur Außerbetriebnahme.

Aus solchen Betrachtungen sollen sich insbesondere die auf die Gewährleistung der Handlungsfähigkeit abzielenden Sicherheitselemente ergeben.

8.4 Schaffung geeigneter Kontroll- und Überwachungs-Strukturen

KonTraG, Sarbanes-Oxley-Act und im weitesten Sinne auch Basel II sind Regelungen zur Corporate Governance (Regeln, die zwischen den Eigentümern des Unternehmens (z. B. Aktionären) und den Verantwortlichen für die Geschäftstätigkeit des Unternehmens vereinbart werden). Sie fordern, abgeleitet aus dem Interesse der Eigentümer in eine Sicherung des Unternehmenserfolgs, einen verantwortungsvollen Umgang der Geschäftsführung mit den der Geschäftstätigkeit inhärenten Risiken. Die genannten Regelungen haben – zumindest wo IT-Risiken Einfluss auf die ordnungsgemäße Abwicklung der Geschäftsprozesse des Unternehmens haben – starken Einfluss auf den Betrieb der IT-Infrastruktur und der IT-Applikationen. Das Management wird durch KonTraG und Sarbanes-Oxley-Act mit erheb-

[1] vgl. Müller, Klaus-Rainer (2003), S.14

lichen Konsequenzen bezüglich deren Haftung in die Pflicht genommen. Es muss beweisen können, dass das Unternehmen alles unternimmt, um die operativen Risiken zu erkennen und zu begrenzen. Damit verbunden ist ein „Paradigmenwechsel“ in der IT-Sicherheit: Die Anstrengungen bezüglich IT-Sicherheit enden nicht mit der Einführung neuer Sicherheitsmaßnahmen, sondern beginnen mit der Implementation nachhaltiger IT-Risk Management Prozesse. Dazu gehört etwa auch das IT-Risk Management im Netzwerkbereich.[1]

Basel II setzt implizit Anreize, das von KonTraG geforderte Risiko-Früherkennungssystem zu einem Risikomanagement-System auszubauen. Die Unternehmen müssen ihre potenziellen Risiken nun auch steuern und kontrollieren. Dies entspricht auch den Anforderungen des Public Company Oversight Board (PCAOB) zur Auslegung des Sarbanes-Oxley-Act, wenn zum Aufbau eines Internen Kontrollsystems (IKS) das COSO-Modell empfohlen wird. Das Committee of Sponsoring Organizations of the Treadway Commission (COSO)-Modell stellt ein erstes Konzept zur Risikosteuerung und -kontrolle dar.

Es ist unzureichend, erkannte Sicherheitsrisikobewältigungsmaßnahmen nur zu implementieren. Ihre Befolgung muss regelmäßig überwacht werden. Das Sicherheitsmanagement hat dies zu initiieren. Wenn während eines Sicherheitschecks Unzulänglichkeiten aufgedeckt werden, sollten nicht bloß die Symptome beseitigt werden. Wichtiger ist die Erkennung des Grundes für das Problem und das Entwickeln von Lösungen. Spezifische IT-Sicherheitsmaßnahmen sind durch ein ganzheitliches IV-Sicherheitsmanagement zu koordinieren, in ein unternehmensweites Sicherheitskonzept und eine Sicherheitsarchitektur zusammenzuführen.

Die Unternehmensarchitektur beschreibt das System der IT-Ressourcen von Unternehmen und erstellt Leitstandards für seine Erstellung und Anpassung.

Zur Erstellung einer sicheren IT-Landschaft sind die einzelnen Merkmale der IT-Sicherheit jeweils angemessen zu gewichten. So ist bei der IT-Infrastruktur hauptsächlich die Verfügbarkeit abzusichern, während bei IT-Anwendungen neben der Verfügbarkeit auch die Integrität ein wichtiges Kriterium ist. Aus dieser Erkenntnis heraus lassen sich Strukturen beschreiben, auf deren Basis ein störungsfreier Ablauf der geschäftskritischen Geschäftsprozesse im Unternehmen garantiert werden muss.[2]

[1] vgl. Grünenfelder, Reto (2006)
[2] vgl. Coester, Ursula/Hein, Matthias (2005), S.30

Dies ist die Phase „Aufrechterhaltung“ des obigen IT-Sicherheitsmanagements. Sie entspricht den Phasen Check (Einhaltung der Anforderungen überwachen/prüfen, Ermittlung der Wirksamkeit der Maßnahmen durch Neubewertung der verbliebenen Risiken und Erarbeitung von Alternativen zur Risikobehandlung) und Act (Umsetzung der Alternativen zur Risikobehandlung und Anpassung von internen Richtlinien und Standards) des ISO 27001.

Die Überwachung der zielorientierten Umsetzung wurde als wichtige Verbesserungsmöglichkeit von Risikomanagement-Systemen angegeben.[1]

Die (strategische und operative) Überwachung hat dabei die Relevanz und Anwendbarkeit der festgelegten Methoden, Standards, Tools und Best Practices unter Berücksichtigung der Kritikalität/Sensitivität der Sachwerte und Prozesse zu bestimmen und Fehleinschätzungen der Kritikalität/Sensitivität der Sachwerte und Prozesse, wie kritisch die Konformität mit entsprechenden Ordnungsmäßigkeitsvorgaben ist, aufzudecken. Sie hat zu gewährleisten, dass Fehleinschätzung vor allem der Relevanz und Anwendbarkeit der festgelegten Methoden, Standards, Tools und Best Practices aufgedeckt werden. Denn aufgrund dieser Nichtaufdeckung der Fehleinschätzungen der Kritikalität/Sensitivität wird kein Anpassungsbedarf der implementierten Maßnahmen festgestellt und vom (operativen) Informationssicherheitsmanagementsystem werden auch die implementierten Maßnahmen nicht angepasst.

Grundvoraussetzung für einen sicheren IT-Betrieb ist eine geschützte Infrastruktur. Das fängt mit Sicherheitsmaßnahmen

- auf der physikalischen Ebene an, z. B. Zugangskontrolle in Verteilerräumen oder einer hoch verfügbaren, mit unterbrechungsfreien Stromversorgungen ausgestatteten IT-Infrastruktur.
- auf der logischen Ebene schließen sich Maßnahmen im Netzwerk an, z. B. Firewalls, Access Control am Netzwerkport (um einen unkontrollierten Zugriff von nicht autorisierten Systemen/Personen auf die IT-Ressourcen zu verhindern), Intrusion Prevention Systeme (um z. B. Flooding-Attacken oder auf Schwachstellen in den Applikationen zielende Angriffe zu erkennen und zu blocken) oder der Schutz der im Netzwerk notwendigen Namensdienste (Domain Name System (DNS)) oder Konfigurations-Services (Dynamic Host Configuration Protocol (DHCP), sowie
- auf Betriebssystemebene, auf die die Komponenten der Applikation aufsetzen, mit der Sicherstellung, dass zeitnah die aktuellen Patches zu bekannt gewordenen Schwachstellen eingespielt werden. Zusätzlich können Verschlüsselungstechnologien (z. B. auf

[1] vgl. Wolf, Klaus (2003b), S.8

Infrastrukturebene IPsec für die Verschlüsselung der Kommunikation im Netzwerk) zur Gewährleistung der Vertraulichkeit und Integrität der Kommunikation eingesetzt werden.

Bezogen auf durchgängige Sicherheitsmechanismen ist die Anforderung, dass der Benutzer sich nicht nur gegenüber dem Geschäftsprozess authentifiziert und in dieser Identität über den gesamten Prozess hinweg arbeitet; jeder Zugriff auf Dienste muss im Kontext dieser Identität erfolgen. Dabei erfolgt der Zugriff nicht über das individuelle Benutzerkonto, sondern über eine Rolle. Ohne eine entsprechende Identitäts-Management-Infrastruktur (welche die Zuordnung von Benutzern zu Rollen übernimmt, Rollen, Gruppen von Rollen und Identitäten verwaltet, und gewährleistet, dass Identitäten flexibel zwischen der SOA basierten Anwendung und den Diensten ausgetauscht werden) lassen sich keine sicheren, wartbaren und revisionsfähigen Geschäftsprozesse realisieren.[1]

Ein qualifiziertes Security-Management bezüglich der Zuweisung und Verwaltung von Rollen in Nutzerverwaltungssystemen erfordert leistungsfähige Kontrollmechanismen. Die Objekte des Systems (Nutzer, Rollen, Applikationen …) müssen mit einer Sicherheits-Klassifizierung versehen werden können, sodass z. B. bestimmte Rollen nur internen Mitarbeitern zugewiesen werden können, oder der Zugang zu vertraulichen Informationen nur der Geschäftsführung möglich ist. Diese Klassifizierung bildet auch die Basis für das Interne Kontrollsystem, um die Prozesse auf Zulässigkeit zu überwachen und beispielsweise auffällige Einzelvorgänge zu ermitteln. Eine möglichst umfassende, automatische Kopplung der Nutzer- und Organisationsdaten (Personal-, Finanz-, Gebäude- und Geräteverwaltung) mit vorgelagerten Systemen verringert die Möglichkeit der bewussten und unbewussten Datenmanipulation. Je nach Ausrichtung des Unternehmens kommen aus verschieden gesetzlichen Regularien (SOX, Basel II, KonTraG etc.) externe Zwänge zu einer eindeutigen Nachvollziehbarkeit der Prozesse in der Nutzeradministration hinzu. Die Zielsysteme, in denen die Berechtigungen aus dem Zentralsystem gesteuert werden, dürfen keine eigene Administration durchführen, um das Rollenmodell mit einem strengen Top-down Fluss nicht zu unterlaufen. Die Überprüfung der Übereinstimmung der Berechtigungen der Nutzer zwischen Zentralsystem und Zielsystemen ist ein Prüfziel der Internen Revision. Ein Revisor überprüft dabei nicht direkt die Zuordnung der Systemberechtigungen zum Nutzer, sondern zweistufig die Zuordnung der Berechtigungen zu den Rollen und die Zuordnung der Nutzer zu den Rollen.[2]

[1] vgl. Kuppinger, Martin (2006)
[2] vgl. Rossa, Gerd (2006)

Die den Geschäftsprozessen zugrunde liegenden Daten liegen meist in den unterschiedlichsten Formaten auf heterogenen Systemen vor. Historisch gewachsene Strukturen, die nicht für eine gemeinsame Nutzung vorgesehen sind, behindern die schnelle und vor allem verlässliche Nutzung dieser Ressourcen in einem einheitlichen Informationskonzept. Um den „Rohstoff“ Information optimal nutzen zu können, können Datenintegrationsplattformen eingesetzt werden, die den Austausch von Informationen zwischen den verschiedenen Systemen automatisieren und vordefinierte Schnittstellen zur Verfügung stellen. Über diese „Datendrehscheiben“ werden Daten, welche in verschiedenen Transaktionsanwendungen, -systemen, Datawarehouses, unstrukturierten Dateisystemen etc. gespeichert sind, zusammengeführt und gemeinsam nutzbar. Darauf aufbauend ist ein großes Stück an Flexibilität gewährleistet, sodass auch weltweit agierende Entwicklerteams produktiv zusammenarbeiten können.[1]

Allgemein führt eine historisch gewachsene IT-Infrastruktur mit zahlreichen Lösungen für gleichartige Probleme (z. B. Nutzung unterschiedlicher ERP-Systeme, E-Mail-Programme oder Betriebssysteme) zu hohen Kosten für die Aufrechterhaltung der Betriebsbereitschaft. Im Rahmen der IT-Strategieentwicklung sind unternehmensinterne IT-Standards zu entwickeln, fortlaufend zu verbessern und im operativen Controlling-Konzept bzw. bei Revisionen auf deren Einhaltung zu überprüfen. Nutzt ein Unternehmen z. B. die Möglichkeiten der Verschlüsselung beim Austausch von E-Mails und anderen elektronischen Dokumenten, so sind einheitliche Verschlüsselungstechniken zu benutzen[2] und ein adäquates Schlüsselmanagement zu installieren.

Wenn die IT-Systeme in einem Unternehmen umfangreicher und verzweigter werden, kann dabei ein zentrales Register (in Form eines Authentification-Gateway) als Voraussetzung für die Automatisierung der Zugangsprivilegien bei den einzelnen Anwendungen eingerichtet werden. Diese Rechte- und Nutzerverwaltung sollte der erste Schritt auf dem Weg zur Einführung eines Universal-Passworts (Single Sign-on) und eventuell auch eines rollenbasierten Rechtemanagements sein. Durch das Arbeiten mit Gruppenrechten wird dabei die gesamte Rechtelandschaft für die Administratoren wie für die Geschäftsverantwortlichen transparenter, auch mit Hinblick auf interne Revisionsanforderungen (z. B. um alle Zugriffe lückenlos mitzuschneiden und anschließend gezielt auszuwerten) und externer rechtlicher Auflagen.

Den wirtschaftlichen Einsatz des Single Sign-on garantiert ein integrierter Self-Service. Dieser weist automatisch den Teilnehmern alle notwendigen Zugriffsprivilegien für die Zielsysteme zu. Bei einem universellen Passwort bedient sich ein entsprechender Automatismus

[1] vgl. Hackett, Christopher (2006)
[2] vgl. Gadatsch, Andreas (2006), S.75-79

nach Zuweisung des Authentisierungsprivilegs für die generelle Netzeingangskontrolle der zentral hinterlegten Identitäten und Rechte. So können im Hintergrund automatisch alle Autorisierungsprivilegien für die berechtigten Zielsysteme zugewiesen werden. Die automatische Freischaltung der berechtigten Zielsysteme/Anwendungen mit der erfolgreichen Authentisierung erfordert aber weitere Sicherheitsvorkehrungen. Neben hinreichend sicheren Passwörtern sind dazu Anmeldeverfahren z. B. mit (biometrischen) Chipkarten erforderlich. Zusätzlich kann die Identitäts- und Zugangsmanagement-Lösung zu einer kartenbasierten Public-Key-Infrastruktur Lösung ausgebaut werden.[1]

Zur Erzielung einer ganzheitlichen Betrachtung und Behandlung der IT-Sicherheit sollte eine integrierte, kooperative und offene IT-Sicherheitsarchitektur angestrebt werden. Sicherheitstechnologien und -werkzeuge müssen in einem Netz auch für die Endgeräte entwickelt werden. Die Vertrauenswürdigkeit, Integrität (Richtlinienkonformität) jedes Endgeräts muss überprüft werden, bevor das Gerät ins Netz eingebunden wird. An jeder Stelle im Netz müssen so Schutzmaßnahmen getroffen und Informationen über den Sicherheitszustand des Netzes gesammelt werden können. Die eingesetzten Technologien und Werkzeuge müssen zusammenarbeiten, um in Abhängigkeit von Ereignissen an einer beliebigen Stelle Maßnahmen an einer anderen Stelle einleiten zu können. Und schließlich müssen die Schnittstellen der Sicherheitsarchitektur offen spezifiziert und standardisiert sein, um eine herstellerübergreifende Kommunikation zu ermöglichen.[2]

Protokolldaten der IT-Systeme und deren Auswertung müssen Aufschluss über sicherheitskritische Ereignisse geben können. Diese Informationen müssen direkt an die zentrale Security-Event-Konsole und den zuständigen IT-Sicherheitsverantwortlichen gemeldet werden.[3]

Eine Service-orientierte Infrastruktur soll die jeweiligen Geschäftsprozesse unterstützen und sich am aktuellen Ressourcenbedarf orientieren. Zudem wird Flexibilität gefordert zur schnellen Anpassung an sich ändernde Anforderungen. Selbst eventuelle Erweiterungen der Infrastruktur sollen den laufenden Geschäftsbetrieb weitestgehend nicht beeinträchtigen. Dies erfordert ein Netzmanagement, das die zur Verfügung stehenden Ressourcen überwacht und entsprechend dem jeweiligen Bedarf zuordnet.[4]

[1] vgl. Drecker, Norbert (2006)
[2] vgl. Helden von, Josef (2006)
[3] vgl. Ferre, David (2003), S.39
[4] vgl. Jahn, Elke (2004)

Dabei ist die IT-Sicherheit ein Teilaspekt der ganzheitlichen Unternehmenssicherheit und in Komponenten der physikalischen Sicherheit wie Gebäudesicherheit inklusive Zutrittskontrolle oder organisatorische Komponenten wie Personalschutz und Datenschutz und -sicherheit sowie Prozesssicherheit zu integrieren. Die Auswahl jeder einzelnen Sicherheitsmaßnahme muss unter Berücksichtigung der globalen Sicherheitsarchitektur erfolgen. Dabei sind die einzelnen Bestandteile im Rahmen der Sicherheitsstrategie zu bewerten.[1]

[1] vgl. Coester, Ursula/Hein, Matthias (2005), S.30,31

C Schlussbetrachtung

Die in einer Unternehmung vorkommenden Problemstellungen sind meist komplexer Art und deren Lösung muss auf einer eher abstrakten Ebene analysiert und diskutiert werden; so auch die Revision und das Controlling der IT-Security.

Die Kenntnis und Akzeptanz der Komplexität lässt bei der Verwendung entsprechender Problemlösungsmethoden dabei den absoluten Wahrheits- und Vollständigkeitsanspruch relativieren.[1] Da die Realität nie vollständig abgebildet werden kann, ist die Modellentwicklung ein selektives und teilweise subjektives Verfahren.[2] In diesem Sinn beansprucht das im Verlauf dieser Ausarbeitung entwickelte Modell keinen Vollständigkeitsanspruch, stellt aber für bestimmte Aspekte eine sinnvolle, Komplexität reduzierende Abbildung dar: Beim Management und Controlling von strategischen Risiken (Risiken, die auf der Ungewissheit der zukünftigen Entwicklungen im Umfeld des Unternehmens und daraus resultierender Ungewissheit über die konkreten Zielvorgaben des IT-Security-Prozesses basieren) wurden die konkreten Zielvorgaben des IT-Security-Prozesses ersetzt durch die angestrebte strategisch-operative Beweglichkeit/Handlungsbefähigung im Kontext der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse. Es wurde versucht, die im Verlauf dieser Arbeit herausgearbeiteten Konzepte zum Management und Controlling von strategischen und operativen Risiken für den Aufbau eines auf die strategisch-operative Beweglichkeit/Handlungsbefähigung abzielenden Modells heranzuziehen. „auf die strategisch-operative Beweglichkeit/Handlungsbefähigung abzielend“ meint, dass in den durch permanente Variation der Umweltbedingungen und damit die Notwendigkeit zur permanenten Handlungsfähigkeit gekennzeichneten unternehmerischen Entscheidungssituationen die Entscheidungsfreiheit (bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und der Geschäftsprozess/des IT-Security-Prozesses aufeinander) zu unterstützen ist. Dabei wurde angenommen, dass die Erreichung der Unternehmensziele/strategisch-operativen Zielsetzungen des Unternehmens und die Abstimmung der Unternehmensziele und Geschäftsprozesse/des IT-Security-Prozesses aufeinander eine entsprechende Handlungsbefähigung/Flexibilität/strategisch-operative Beweglichkeit voraussetzt. Die in das strategisch-operative Risiko-Controlling integrierten Komponenten des strategischen und operativen Performance Managements bilden die (im technisch-organisatorischen Kontext zu analysierende) IT-Sicherheit der die Prozesse des Unternehmens unterstützenden IT-Systeme in eine adäquate IT-Security ab. Diese IT-Security hat die Strategie-konforme und IT-Nutzenpotenzial absichernde Gestaltung der organisatorischen

[1] vgl. Gomez, Peter (2002), S.152
[2] vgl. Gomez, Peter (2002), S.130

Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume so weit möglich zu gewährleisten. Die Strategie-Konformität und Absicherung der IT-Nutzenpotenziale wird dadurch unterstützt, dass adäquate Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security in das strategische und operative Performance Management integriert werden. Insgesamt dient dies der Modellierung entsprechender Steuerungs- und Kontrollprozesse zur Strategieformulierung und -durchsetzung/-umsetzung bezüglich der IT-Security.

1 Zusammenfassung

IT-Sicherheit ist ein Zustand, dessen Stabilität/Dauerhaftigkeit angestrebt wird. Stabilität/Dauerhaftigkeit bedeutet, dass dieser Zustand im Idealfall durch kein Ereignis (als Realisierung eines Risikos), d. h. nur durch ein Ereignis, welches nie eintreten soll, verlassen werden kann. Ein nie eintretendes Ereignis kann aber nicht beobachtet werden, sodass nicht objektiv beurteilt werden kann, ob Stabilität/Dauerhaftigkeit erreicht ist. Notwendige Bedingung zur Erreichung der Stabilität/Dauerhaftigkeit ist aber, dass Sicherheitsanforderungen aufgestellt und diese mit entsprechenden Sicherheitsmaßnahmen abgedeckt werden. Ob ein System in einer bestimmten Hinsicht als sicher gelten kann, hängt u. a. von den zu erfüllenden Anforderungen (z. B. bezüglich der Verfügbarkeit) ab.

IT-Sicherheit ist eine wichtige Voraussetzung für den effektiven und effizienten Einsatz von IT-Systemen. Die IT-Sicherheit eines Systems kann aus zwei komplementären, sich einander ergänzenden Sichten betrachtet werden: Sicherheit des Systems (bezeichnet als Verlässlichkeit) und Sicherheit vor dem System (bezeichnet als Beherrschbarkeit). Die Ziele, mit denen Sicherheit erreicht werden soll (Schutzziele) sind Vertraulichkeit, Integrität, Verfügbarkeit, Verbindlichkeit, Authentizität, Möglichkeit zur Anonym-/Pseudonymisierung und Betriebssicherheit als Voraussetzung für Integrität und Verbindlichkeit. Die Verlässlichkeit eines Systems gewährleistet grundsätzlich aber noch nicht, dass das System/die Anwendung im Sinne der Betroffenen/Anwender funktioniert, ihre Belange berücksichtigt und für sie nachvollziehbar ist. Dem Anwender/Betroffenen fehlt zumeist die Möglichkeit zur unmittelbaren Wahrnehmung dessen, was in einem IT-System passiert. Daher müssen auch Eigenschaften angestrebt werden, um ein IT-System aus Sicht des Betroffenen sicher/beherrschbar zu machen:

Die IT-Sicherheit von Informationssystemen soll Auswirkungen möglicher Ausfälle der Systeme in Form von Unterbrechungen in der Versorgung mit (auf den entsprechenden Informationssystemen basierenden/durch diese zur Verfügung gestellten) Leistungen bzw. Services vermeiden. Im Mittelpunkt steht weniger, wenn z. B. die dahinter stehenden kritischen Infrastrukturen angegriffen oder sensible Geschäftsinformationen ausgespäht werden (was durch noch so starke Schutzvorrichtungen kaum zu verhindern ist). Übergeordnetes Ziel ist die Gewährleistung der Versorgungssicherheit; es ist die Fähigkeit von Geschäftsvorgängen, Organisationen und technischen Systemen zu unterstützten, bei unvorhergesehenen Ereignissen das Geschäft fortzuführen und vor Schaden zu bewahren.

Security bildet einen Zusatzwert eines Informationssystems. Sie ermöglicht die revisionssichere und verantwortungsvolle Ausführung von Applikationen auf diesem IT-System. IT-Sicherheit soll zudem neue Möglichkeiten für computer- bzw. internetbasierte Geschäftsprozesse eröffnen, indem z. B. der flexible und komfortable elektronische Informationsaustausch abgesichert wird. Bezogen auf die IT-Security sind des Weiteren externe und interne Ordnungsmäßigkeitsvorgaben sowie Korrektheitsbedürfnisse bezüglich der im Unternehmen durchlaufenden Daten/Informationen zu erfüllen.

Security wird dabei als strategisches Unternehmensziel und als unternehmensweite Managementaufgabe gesehen, die die Erarbeitung klarer Sicherheitskonzepte erfordert, welche auf der IT-Sicherheits-/IT-Security-Strategie basieren. Mit IT-sicherheitsstrategischen Konzepten sind z. B. Vorgehensmodelle, Systementwicklungsmethoden, Richtlinien für den Werkzeugeinsatz gemeint, die über die Sicherheitsschutzziele definierte Konzepte darstellen. Die Einordnung der IT-Ressourcen und IT-Objekte in diese Konzepte kann über die funktionale Sicht auf die IT-Systeme erfolgen, welche die entsprechenden IT-Ressourcen benutzen, bzw. mit den entsprechenden IT-Objekten modelliert werden können.

Die IT-Sicherheits-/IT-Security-Strategie und der IT-Security-Prozess geben strategische bzw. strategisch-operative Ziele vor allem in der Performance- und in der infrastrukturellen Perspektive vor. Durch Etablierung entsprechender Führungskreisläufe, Organisationsstrukturen und Prozesse müssen die Revision und das Controlling erreichen, dass die IT-Strategie und auch die IT-Security-Strategie die übergeordnete Unternehmensstrategie unterstützt.

Es wurde davon ausgegangen, dass die IT-Security-Strategie aus der IT-Strategie abgleitet wird. Dies bedeutet, dass einer der wichtigsten Zielgegenstände des strategischen IT-Security-Managements mit dem Gegenstand des strategischen IT-Managements übereinstimmt, nämlich den mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozessen und Geschäftsmodellen des Unternehmens. Zur Erreichung seiner Ziele hat das Management ein Managementsystem zu entwickeln. Dieses ist durch ein Informationssystem zu unterstützen, das dem Managementsystem die Durchführung seiner Aufgaben ermöglicht. Vor allem wenn Geschäftsprozesse internetbasiert ablaufen, sind „sichere“ IT-Systeme dabei Voraussetzung für den Erfolg der entsprechenden Geschäftsmodelle.

Gemanagte IT-Sicherheit muss dies mit gesetzlichen Bestimmungen, internationalen Standards, wirtschaftlichen IT-Lösungen sowie der Sicherung des Unternehmenserfolgs verknüpfen.

Externe Ordnungsmäßigkeitsanforderungen in Form von gesetzlichen Vorgaben verfolgen das Ziel, dass Gefahren für das Unternehmen minimiert bzw. frühzeitig erkannt werden sollen. Interne Ordnungsmäßigkeitsanforderungen für den IT-Bereich zielen darauf ab, Effizienz und Effektivität bei der Nutzung moderner Informations- und Kommunikationstechnik zu gewährleisten. Im Zusammenhang mit der enormen Abhängigkeit der Unternehmen von ihrer IT geht es um eine entsprechend optimierte Qualität und Verfügbarkeit der IT-Prozesse. Dieses verlangt ein auf die Anforderungen aus der Umgebung abgestimmtes Maß an IT-Sicherheit.

Die prozessualen und organisatorischen Maßnahmen, die die Führung und Steuerung der IT unterstützen, sollen den zweckgerichteten Einsatz der IT (und zugehöriger IT-Security-Maßnahmen) (d. h. das Verständnis der strategischen Bedeutung von IT (und der IT-Security), um so bessere Strategien für die zukünftige Erweiterung des Geschäftsbetriebs zu schaffen) ermöglichen. Die Prozessabläufe müssen verlässlich ineinandergreifen und ein verlässlicher Datenaustausch mit unterschiedlichen Kommunikationspartnern (Kunden, Lieferanten und Geschäftspartnern) entlang gemeinsamer, zielgerichteter Prozessketten garantieret werden. IT-Sicherheit nimmt dabei eine wichtige Rolle ein: Die meisten Unternehmensprozesse sind mit der IT-Sicherheit eng verzahnt, z. B. Prozesse, welche erfordern, dass alle entscheidungsrelevanten Informationen zeitnah und in hoher Qualität verfügbar sind.

Entscheidungsträger im Unternehmen müssen darüber hinaus über Ablauf und Effizienz ihrer Geschäftsprozesse ständig Bescheid wissen. Dies erfordert, dass alle entscheidungsrelevanten Informationen zeitnah und in hoher Qualität verfügbar sind. Aufgrund der Bedeutung von Informationen für das Überleben und den wirtschaftlichen Erfolg von Unternehmen muss ein strategisches Informationsmanagement dabei auch Regelungen zu den Strukturen, Verantwortlichkeiten und Verfahren der IT-/IV-Sicherheit beinhalten. Das sog. Informationsversorgungssystem soll der Unternehmensführung alle für die Planung, Durchführung und Kontrolle erforderlichen Ergebnisziel-orientierten Informationen bereitstellen. Aufgabe im Zusammenhang mit der IT-Sicherheit ist es, den laufenden Betrieb dieses IV-Systems sicherzustellen.

Mit Internetanbindungen und Einführung mobiler Technologien werden bidirektionale Zugangstüren geöffnet. Aus dem organisatorisch-technischen Zusammenspiel von Mitarbeitern, Partnern und Kunden, beruhend auf der Nutzung dieser Zugangstüren, entstehen über alle geschäftlichen Kernprozesse hinweg Sicherheitsrisiken. Neben den einzelnen konkret gefährdeten Prozessbestandteilen ergeben sich Bedrohungen aus dem Zusammenspiel von Menschen, Soft-/Hardware und Netzen.

Spezielle gesetzliche Sicherheitsanforderungen bezüglich der IT müssen aus den vorhandenen Gesetzen und allgemeineren Normen (z. B. Haftungsnormen oder Verlautbarungen anerkannter Organisationen) abgeleitet werden. Zur Einbindung von technischen Sicherheitsstandards (welche die materiell rechtlichen Anforderungen umschreiben und praktisch handhabbar machen, die zum Schutz der IT-Sicherheit eingehalten werden müssen) in die Gesetze macht der Gesetzgeber abstrakte Vorgaben in Form der unbestimmten Rechtsbegriffe „allgemein anerkannte Regeln der Technik“, „Stand der Technik“ oder „Stand von Technik und Wissenschaft“.

Das deutsche KonTraG und internationale Regelungen wie Basel II oder der amerikanische Sarbanes-Oxley-Act (SOX) sollen für mehr Transparenz in den Unternehmen sorgen und fordern ein aktives Risikomanagement. Zentrale Aufgabe bezogen auf die IT ist der Aufbau, die Überwachung und Steuerung transparenter IT-Strukturen für definierte und kontrollierte Prozesse zur Gewährleistung eines wirksamen internen Kontrollsystems. Ein angemessenes und wirksames IT-Kontrollsystem soll die Umsetzung der IT-Strategie überwachen. Für das Ziel des KonTraG, mehr Transparenz im Unternehmen durch Risikoüberwachung und -steuerung zu erreichen, sind qualitativ hochwertige Informationen und vor allem ein schneller, sicherer Informationsfluss notwendige Voraussetzung. Nur dann haben die Verantwortlichen einen Zeitgewinn, um Maßnahmen zur Risikobekämpfung einzuleiten. Gesetzen wie KonTraG und SOX kann diesbezüglich nur entsprochen werden, wenn ein angemessener IT-Sicherheitsprozess mit Schnittpunkten zu den Risikomanagementprozessen im Tagesgeschäft des Unternehmens verankert ist.

Die Regelungen, Vorschriften und Bestimmungen im Bereich der Erarbeitung und Gestaltung eines umfassenden ganzheitlichen Risikomanagements gewähren der Praxis einen größtmöglichen Freiraum bei der Umsetzung. Der deutsche Gesetzgeber schreibt nicht vor, wie ein Überwachungssystem im Rahmen des Risikomanagements zu gestalten ist. Maßgeblich sind betriebswirtschaftliche Aspekte und das Gebot der Zweckmäßigkeit. Der Gesetzgeber vertraut auf die Selbstorganisation der Unternehmen, die so eine höhere Flexibilität erreichen. Hier kann auf internationale Verlautbarungen wie den COSO-Report, die Grundsätze Risikoorientierter Unternehmensüberwachung (GoÜ) und den deutschen Corporate Governance Kodex zurückgegriffen werden.

Das unternehmensweite Risikomanagement umfasst auch ein IT-Risikomanagement. Die rechtliche Verantwortlichkeit der Vorstände bzw. Aufsichtsräte zur Gewährleistung der IT-Sicherheit ergibt sich daraus, dass sie dem Unternehmen aufgrund ihres Vertrages und gesetzlicher Regelungen verpflichtet sind, Schaden und erkennbare Risiken abzuwenden. Im Falle einer Unternehmenskrise hat der Vorstand basierend auf § 93 Abs. 2 AktG nachzuweisen,

Maßnahmen zur Risikofrüherkennung und zur Risikoabwehr getroffen zu haben. Es gilt die sog. Beweislastumkehr, d. h., kann das Vorstandsmitglied im Schadensfall nicht beweisen, dass es seine gesamten Pflichten erfüllt hat, wird quasi automatisch eine Pflichtverletzung angenommen.

Gesetzliche Grundlagen, die explizit Maßnahmen zur Sicherung von IT-Systemen fordern, müssen in eigenen Sicherheitsprozessen und -richtlinien spezifiziert werden. Dabei kann man sich an IT-Sicherheitsstandards orientieren, mit deren Hilfe sich ein entsprechendes Sicherheits-Managementsystem sowie detaillierte Sicherheitsrichtlinien entwickeln lassen. Für die IT-Systeme werden so Sicherheitsrichtlinien mit konkreten Umsetzungsvorgaben entwickelt mit dem Ziel, einen vorab in einer Schutzbedarfsanalyse festgestellten Schutzbedarf zu erreichen. Die für die erforderliche IT-Sicherheit zu ergreifenden IT-Sicherheitsmaßnahmen werden klassischerweise auf Basis der Ergebnisse einer Risikoanalyse bestimmt. Diese untersucht IT-Systeme auf Schwachstellen und auf Bedrohungen hin, die zu Gefährdungen für die IT-Sicherheit führen könnten. Diese Risikoanalyse setzt zunächst eine Schutzbedarfsanalyse voraus, welche die verwendeten IT-Systeme und Datenbestände nach ihrer Bedeutung für das Unternehmen klassifiziert.

Der Grad der notwendigen Informationssicherheit muss der Wichtigkeit der zu schützenden Informationen und der Priorität entsprechender Anwendungen angemessen sein. Objektiviertes Kriterium zur Beurteilung der Wichtigkeit/Kritikalität der für das Unternehmen relevanten Schutzobjekte bzw. der als besonders sensitiv/risikobehaftet erachteten Anwendungen ist im Zusammenhang mit dem strategischen Ansatz der Grad des Einflusses für das Erreichen der Zieldimensionen des IT-Security-Prozesses. Diese Einflussfaktoren sind auch die notwendige Verlässlichkeit und Beherrschbarkeit entsprechender Systeme und Anwendungen, sofern von diesen die korrekte Umsetzung der IT-Security-Strategie abhängt.

Zur Umsetzung von gemanagter IT-Sicherheit sind entsprechende Prozesse im Bereich der Informationssicherheit zu implementieren (etwa Incident Handling, Reporting oder Change Management). Die notwendige Bedingung zur Erreichung der Stabilität/Dauerhaftigkeit des Zustands IT-Sicherheit erfordert ein geeignetes operatives Sicherheitsmanagement auf Basis der Analyse der potenziellen IT-Bedrohungen. Auch im Bereich der IT-Security sind in einem kontinuierlichen Prozess die einzuleitenden Maßnahmen zu planen, zu analysieren und im Rahmen einer Erfolgskontrolle auf ihre Zielerreichung zu messen.

Mit zunehmender Beschleunigung von Veränderungen und der Notwendigkeit zur Risikobewältigung wird dabei die unternehmerische Flexibilität und Anpassungsfähigkeit zur Wahrung der Handlungsfreiheit und Entscheidungsfreiheit bei der Umsetzung der strategisch-operativen Zielsetzung/alternativ möglicher Strategien/Konzepte immer wichtiger.

Die Umsetzung der IT-Sicherheitsstrategie in Form angemessener Ausführungsschritte setzt die Evaluierung geeigneter Sicherheitsmaßnahmen voraus. Dies ist zentrale Aufgabe des Risikomanagements.

Die Forderung nach Adaptivität bedeutet, vorausschauend agieren sowie schnell und flexibel interne Strukturen und Abläufe ändern zu können. Als strategischer Aspekt kam in dieser Arbeit daher die organisatorische Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume bei der Umsetzung der strategisch-operativen Zielsetzung hinzu. Für diesen Aspekt wurde das IT-Sicherheitsmanagement zu einem strategisch-operativen IT-Security-Management erweitert. Im Kontext der gegebenen Thematik wurde untersucht, wie das erhöhte Risikopotenzial bei der Formulierung und Umsetzung von Zielen und Strategien im Zusammenhang mit IT-Projekten, welche die Geschäftsprojekte und Geschäftsmodelle des Unternehmens unterstützen bzw. ermöglichen sollen, durch die Zuverlässigkeit und Beherrschbarkeit entsprechender IT-Systeme beeinflusst wird.

Handlungsspielräume in Abhängigkeit von möglichen Risiken zu unterstützen ist Aufgabe des hierfür entwickelten strategisch-operativen Risiko-Controllings, welches auf einer adäquaten Risikoüberwachung, und Risikosteuerung basiert. Durch Integration der Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security in dieses Modell wird dieses als Rahmen zur Strategie konformen und IT-Nutzenpotenzial absichernden Formulierung und Umsetzung der IT-Security-Strategie und zur Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander ausgerichtet.

Als Ergebnis des Zyklus im Regelkreis strategische Vorgaben – Konzeptionierung – Umsetzung – Überwachung – Anpassung der Vorgaben kann ein gegebenenfalls. optimiertes Richtlinienwerk vorliegen. Es wird der gesamte Managementzyklus von der Strategiefindung und entsprechenden Zielableitung (Planung) bis hin zur Überwachung der Umsetzung betrachtet.

Zur Umsetzung der Anforderungen z. B. des KonTraG ist eine Risikokontrollstruktur auf allen Konzern- bzw. Unternehmensebenen zu etablieren. Als Pendant dazu ist in Zusammen-

hang mit der gegebenen Thematik eine Risikosteuerungsstruktur auf allen Unternehmensplanungsebenen zu etablieren.

Die Planung in der Unternehmung hängt weitgehend auch von der Entwicklung ihres Umfelds ab. Die Formulierung der Ziele in der Unternehmung unterliegt einem umweltbedingten Wandel. In diesem Zusammenhang ist die Anpassungsfunktion des Risiko-Controllings wichtig, welches Prämissen bei der Geschäftsprozess-bezogenen Risikoerfassung, -selektion und -bewertung sowie Konzepte der Risikosteuerung an sich ändernde Gegebenheiten im Umfeld des Unternehmens anpassen soll. Erforderlich ist die Ausgestaltung der aus der Koordinationsfunktion des Controllings als Koordination der Führungsaufgabe mit der Umwelt abgeleiteten Anpassungsfunktion. Der optimale, am besten auf das Umfeld angepasste (best adapted) Einsatz der IT-Technologie wird immer mehr zum Hauptüberlebenskriterium eines Unternehmens. Neue Systeme sind (auf Grundlage einer konsistenten, unternehmensweiten Sicherheitsarchitektur) so anzupassen, dass sie dem definierten Sicherheitsniveau des Unternehmens entsprechen.

Das strategische IT-Security-Management (der strategische Teil des strategisch-operativen IT-Security-Managements), welches sich auf die Anpassung an das Umfeld sowie der Begründung und Erhaltung der Handlungsfähigkeit des Unternehmens mit seiner Umwelt konzentriert, ist eine Ausprägung des strategischen Risikomanagements, für das eine genaue Identifizierung und Analyse von Potenzialen bzw. Strategien zur Ausnutzung operativer Flexibilität und zur Steigerung von Managementflexibilität erforderlich ist. Ziel des strategischen IT-Security-Managements ist es, neue Geschäftsmöglichkeiten und entsprechende Geschäftsmodelle mit zugehörigen Erfolgspotenzialen zu ermöglichen bzw. abzusichern, das bewusste Aufbauen und Sichern von Erfolgspotenzialen zu unterstützen. Eigentliche Aufgabe ist dabei das Management des Risikos, dass der IT-Sicherheits-/IT-Security-Prozess nicht die benötigte Effektivität (und Effizienz) aufweist. Dabei geht es um das Risiko ungültiger oder falscher Zielvorgaben aufgrund falscher Annahmen (und das Risiko mangelnder Umsetzung).

Für das IT-Security-Management ist also ein kontinuierlicher Verbesserungsprozess zu initiieren, der auf die Anpassung vom Ist ans Soll abzielt. Dazu sollen Systeme zur Unterstützung der Strategieformulierung und -umsetzung bezüglich der IT-Sicherheits-//IT-Security-Managements in ein entsprechendes Lösungsmodell integriert werden. Unterstützung der Strategieformulierung betrifft den Aspekt der Veränderung der Vorstellung des Wirtschaftssubjekts über den Soll-Zustand, Unterstützung der Strategieumsetzung betrifft den Aspekt der Veränderung des Ist-Zustands.

Bezüglich des strategischen Risikomanagements können in Anlehnung an das Konzept des strategischen Performance-Managements als Risiken für den IT-Security-Prozess die Prämissen- bzw. Selektionsrisiken der Planung (Irrtumsrisiken der Selektions- und Filterkriterien bei der Fokussierung auf die wichtigsten Prämissen der Security-Strategie) und zukünftige Security-Strategie-Umsetzungsgefahren analysiert werden.

Irrtumsrisiken der Selektions- und Filterkriterien bei der Fokussierung auf die wichtigsten Prämissen der Security-Strategie resultieren aus einer Fehleinschätzung, wie kritisch und sensitiv gewisse Sachwerte (vorhandene Systeme, Netzwerke, Applikationen und Informationen) sind.

Security-Strategie-Umsetzungsgefahren bestehen potenziell bei mangelnder Flexibilität. Auch hier sind die beeinflussbaren Größen wie organisatorische, managementspezifische oder technische und personelle Fragestellungen von großer Bedeutung. Technische Fragestellungen betreffen die Verlässlichkeit und Beherrschbarkeit der für die Umsetzung relevanten Systeme.

Ein Ziel des (sich mit Ungewissheitssituationen befassenden) Risikomanagements ist es, die Anteile an Ungewissheit zu mindern, indem sie messbar und handhabbar gemacht werden. Ein Ansatz zur Auflösung der Ungewissheit bezüglich Umfeldentwicklungen kann darauf abzielen, Strategieoptionen zu untersuchen: Die Ungewissheit bezüglich Umfeldentwicklungen kann in zwei Richtungen getrennt voneinander untersucht werden: eigene Handlungsmöglichkeiten und mögliche Randbedingungen des Umfelds. Bei der Untersuchung der Ungewissheit bezüglich Umfeldentwicklungen in Richtung eigener Handlungsmöglichkeiten sind Entscheidungsfreiheiten/Flexibilitätspotenziale zu analysieren, um wandelnden Konstellationen im Umfeld entsprechen zu können. Zur Abbildung und Beurteilung strategischer und operativer Handlungsmöglichkeiten wurden Realoptionen angesetzt.

Die auf die Umwelt bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse (mögliche Randbedingungen des Umfelds) wurden mit den Rahmenbedingungen für das Management identifiziert. Diese Rahmenbedingungen für das Management beziehen sich (im Zusammenhang mit der Anpassung an das organisatorische und das technische Umfeld des Unternehmens) wiederum auf den technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen. Dieser ist aus Sicht des IT-Systems der Kontext Verlässlichkeit (beurteilt nach den Kriterien Verfügbarkeit, Integrität und Vertraulichkeit), und aus Sicht der Betroffenen (Anwender/Benutzer) der Kontext Beherrschbarkeit des Systems (mit den Aspekten Komplexitätsreduktion und Kontrollierbarkeit, beurteilt z. B. nach

den Kriterien Nachprüfbarkeit und Rechtssicherheit). Der technisch-organisatorische Kontext für die IT-Sicherheit von Systemen umfasst die Sichten der Beurteilung der Sicherheit des Systems, wobei die IT-Infrastruktur die zentrale Rolle spielt. Die IT-Infrastruktur wiederum ist das zentrale Element eines IT-Security-Frameworks, welches die Ebene der IT-Sicherheit/IT-Security mit der Strategieebene verbindet.

Das IT-Security-Framework, welches die Aufgabenstellung eines Risiko-orientierten zukunftsbezogenen IT-Security-Managements abbildet, hat unter Berücksichtigung möglicher Randbedingungen des Umfelds IT-Security bezogene Aktivitäten zur Sicherung der Koordinations-, Reaktions- und Adaptionsfähigkeit der Führung auf den Planungsebenen für eine geschäftsübergreifende Unternehmensstrategie festzulegen.

Das IT-Security-Framework, ausgehend von der Geschäftspolitik sowie von Geschäftsregeln und Weisungen, die IT-Sicherheitsmechanismen mit Geschäftsrisiken in Verbindung bringen, verbindet die Strategieebene direkt mit der Ebene der IT-Security/IT-Sicherheit:

Dieses IT-Security-Framework hat die aus der Koordinationsfunktion des Controllings abgeleitete Anpassungsfunktion als Koordination der Führungsaufgabe mit der Umwelt auszufüllen. Konzepte zur Ausgestaltung dieses IT-Security-Frameworks ergeben sich folglich aus Überlegungen zum Anpassungsprozess an das Umfeld des Unternehmens.

Die Ausgestaltung dieses IT-Security-Frameworks basiert auf einem auf die Sicherstellung von Potenzialen bzw. Strategien zur Ausnutzung operativer Flexibilität und zur Steigerung von Managementflexibilität abzielendem, als strategisch-operatives Risiko Controlling bezeichneten Konzept. Dieses strategisch-operative Risiko Controlling soll die Effektivität und Effizienz des IT-Sicherheitsmanagements überwachen, dieses koordinieren/steuern und auf die Herstellung/Unterstützung der strategisch-operativen Beweglichkeit/Handlungsbefähigung bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens ausrichten.

Der technisch-organisatorische Kontext für die IT-Sicherheit von Systemen wird innerhalb des strategisch-operativen Risiko-Controllings in die auf das System bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume, also eigene Handlungsmöglichkeiten (Flexibilität und Entscheidungsfreiheit) (bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens) transformiert. Auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen stehende Kriterien werden so in diesen Kontext projiziert.

Das strategisch-operative IT-Security-Management muss Gefahren/externe Ungewissheit und Risiken/interne Ungewissheit für den IT-Security-Prozess (wobei sich Ungewissheit auf Zielvorgabe und -erreichung bezieht) identifizieren, bewerten und steuern. Zielvorgabe und -erreichung wiederum bezieht sich auf die Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse. In diesem Kontext soll das strategisch-operative IT-Security-Management strategische Handlungsspielräume unterstützen/absichern. Um sich in einer an Komplexität und „externer Ungewissheit“ zunehmenden Umwelt an die aus der Unternehmensumwelt auf das Unternehmen einwirkenden Gefahren, wenn diese gewisser werden, mit einer entsprechenden Alternative aus einem strategischen Handlungsspielraum anpassen zu können, muss das strategisch-operative IT-Security-Management die Möglichkeiten in diesem strategischen Handlungsspielraum unterstützen/absichern. Dieser strategische Handlungsspielraum bezieht sich auf den Gegenstand des strategischen IT-Managements, die mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens. Diese IT-Projekte wiederum werden mittels der physischen Objekte Hardware, Software, Netze und Personal und logischen Objekte wie Informationssysteme, Datenbanken, Kommunikationsbeziehungen sowie Konzepte wie Vorgehensmodelle, Systementwicklungsmethoden und Richtlinien für den Werkzeugeinsatz umgesetzt. Auf diese physischen und logischen Objekte beziehen sich auch die operativen Bestandteile einer ganzheitlichen IT-Security-Strategie, welche auf den Ebenen der Gründe für die Unbestimmtheit der Zielvorgabe und Zielerreichung des IT-Security-Prozesses identifiziert wurden.

So kann auch die IT-Security als „Enabler“ von Geschäftsmodellen/Geschäftsmöglichkeiten betrachtet werden (z. B. bezüglich der Möglichkeiten des Internets). Andererseits ist die IT-Security ein Managementprozess. Bezüglich des IT-Security-Managements ist ein Anpassungsprozess zu initiieren, um sich an die aus dem Umfeld des Unternehmens entspringenden IT-Risiken anzupassen.

Risiko wird bestimmt durch Ungewissheit, geprägt von Unbestimmtheit und Unvollständigkeit. Entscheidungen sind das handlungsbestimmende Element, rationale Entscheidungen von einem gewissen Informationsstand der Akteure abhängig, und Handlungen wiederum rufen Risiken hervor. Es stehen die Ursache-Wirkungs-Beziehungen, die Zusammenhänge und Abhängigkeiten zwischen den Erfolgsfaktoren und den strategischen Zielen im Vordergrund. Im Modell zum strategisch-operativen (Risiko-)Controlling der IT-Security sind die operativen Ergebnisse im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen die

optimierte Verlässlichkeit und die optimierte Beherrschbarkeit der von der Umsetzung der strategischen Ziele betroffenen IT-Systeme bzw. zu implementierenden Maßnahmen. Diese kritischen Erfolgsfaktoren (Verlässlichkeit und Beherrschbarkeit) können auch als Frühwarnindikatoren aufgefasst werden.

Die Risikoanalyse von IT-Security-Risiken im operativen IT-Security-Management erfolgt auf Basis der Schwachstellenanalyse und der Bedrohungsanalyse. Der Erfolg des (operativen) Risikomanagements hängt aber nicht davon ab, jedes Risiko exakt zu berechnen. Im Rahmen der Analyse werden wichtige Erkenntnisse zur strategischen Bedeutung bestimmter Risiken gewonnen. In der Business-Perspektive der Sicherheitserfordernisse soll die strategische Risikoanalyse dem Management ermöglichen, sich auf eine Strategie zum Umgang mit Risiken festzulegen. Die Unternehmung muss die Fähigkeit aufbauen, das Nichtvorhersehbare erfolgreich und effizient zu meistern. Auch angesichts zunehmender Beschleunigung der Veränderung kommt dabei der unternehmerischen Flexibilität, der Wahrung der Handlungsbefähigung wesentliche Bedeutung zu.

Wichtig ist das Management des Risikos, dass nicht die vom IT-Risikomanagement evaluierten (der Wichtigkeit der zu schützenden Informationen und der Wichtigkeit der Geschäftsprozesse angemessenen) Maßnahmen/Schutzvorrichtungen der IT-Sicherheit/IT-Security implementiert werden. Für das IT-Risikomanagement sind Schutzkonzepte für die IT-Komponenten und IT-sicherheitsstrategische Konzepte, in der die IT-Komponenten eingeordnet werden können, zu entwickeln.

In dieser Arbeit ging es hauptsächlich um Risiken, dessen Ursachen außerhalb der unternehmerischen Entscheidungsgewalt, d. h. im Umfeld des Unternehmens liegen. Die Wirkung des Risikos ist die Zielgefährdung. Ein die IT-Sicherheit betreffendes bzw. gefährdendes Ereignis ist immer unsicher bzw. in der Regel nicht prognostizierbar. Ob es ein Risiko für das Unternehmen darstellt, hängt davon ab, ob sein Eintreten Auswirkungen auf das Erreichen der Unternehmensziele hat. In diesem Sinn lag der Schwerpunkt auf strategischen Risiken, welche die Gefahr beinhalten, dass der Rahmen für das unternehmerische Handeln nicht so ausgerichtet ist, dass z. B. die Verschwendung von Ressourcen aufgrund von nicht mehr gültigen Prämissen und damit einer ungültigen Strategie vermieden wird.

Die ungenauen gegenwärtigen und ungewissen zukünftigen Anforderungen an die IT-Sicherheit/IT-Security können als Grund für die Unbestimmtheit der Zielvorgabe und Zielerreichung des IT-Security-Prozesses auf den Planungsebenen für eine geschäftsübergreifende Unternehmensstrategie (Ressourcenebene, sozio-technische Ebene, Organisationsebene, Ge-

schäftsebene und Unternehmensebene) untersucht werden. Dabei ist der IT-Sicherheitsprozess kein konkreter Kernprozess eines Unternehmens. Vielmehr soll er das grundsätzliche unternehmensweite Vorgehen beschreiben, um für alle Prozesse und IT-Systeme geeignete IT-Sicherheitskonzepte zu entwickeln, zielgerichtet umzusetzen und regelmäßig zu überprüfen. Er muss dazu alle relevanten IT-gestützten Abläufe im Unternehmen durchdringen.

Zum Management dieser strategischen Risiken wurde das strategische Performance Management als wichtigstes Konzept der strategischen Unternehmensführung auf die Planungs- und Lenkungsaufgabe bezüglich des IT-Security-Prozesses/IT-Security-Management übertragen. Unter einer Sicherheitsstrategie werden dabei Konzepte zur Führung der Sicherheitssysteme des Unternehmens verstanden.

Die Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security wurden in das, auf die strategisch-operative Beweglichkeit/Handlungsbefähigung abzielende Modell zum strategisch-operativen Risiko-Controlling integriert. Somit wird über die entsprechenden Komponenten ein Anpassungsprozess an die „Umgebung“ bezüglich der IT-Security modelliert und in das Modell zum strategisch-operativen Risiko-Controlling integriert, das die Formulierung und Realisierung der IT-Security-Strategie steuert, die angestrebte IT-Security und die Geschäftsprozesse/Geschäftsmodelle aufeinander. abstimmt, und auf die Unterstützung/Herstellung der strategisch-operativen Beweglichkeit/Handlungsbefähigung bei der IT-Nutzenpotenzial absichernden Umsetzung der strategisch-operativen Zielsetzung des Unternehmens abzielt.

Einen wichtigen Teil der „Umgebung“ des Unternehmens stellen die externen Compliance-Anforderungen dar. Der andere Teil dieser „Umgebung“ ist das IT-Umfeld. Dieses ist durch die Infrastruktur, die Applikationen und Business-Prozesse beschrieben. Dieses Umfeld wird in rechtliches, organisatorisches und technisches Umfeld unterteilt. Zur Anpassung an das rechtliche Umfeld muss das Unternehmen sich an den „Rechtsorganismus“ der IT-Sicherheit anpassen. Anpassung an das organisatorische und technische Umfeld ist in dem Sinne gemeint, dass Unternehmen ihre IT-Ressourcen, Systeme und Geschäftsprozesse ständig anpassen und neu konfigurieren müssen, um einen optimalen, am besten auf das Umfeld angepassten Einsatz der IT-Technologie zu erreichen. Zur Anpassung an das technisch-organisatorische Umfeld ist etwa die ständige Verbesserung und Anpassung von Schutzvorrichtungen und -mechanismen an neue Angriffsszenarien und -möglichkeiten erforderlich.

Die Anpassung an das rechtliche Umfeld liefert mit der Compliance einen Teil der notwendigen Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security. Der

andere ergibt sich aus Überlegungen zur Anpassung an das organisatorische und das technische Umfeld. Überlegungen zur Anpassung an das organisatorische und das technische Umfeld müssen darüber hinaus die hinreichende Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security ableiten. Der aus den Überlegungen zur Anpassung an das organisatorische Umfeld bzw. Anpassung der Organisation an das Umfeld abgeleitete Teil der notwendigen Bedingung sowie die hinreichende Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security beziehen sich auf Aufbauorganisation und Ablauforganisation.

Einen Beitrag für die notwendige Bedingung für die Anpassung an die „Umgebung“ liefern die mit Aufbauorganisation und Ablauforganisation in Verbindung stehenden internen Ordnungsmäßigkeitsvorgaben. Die hinreichende Bedingung für die Anpassung an die „Umgebung“ kann an die, ebenfalls mit Aufbauorganisation und Ablauforganisation in Verbindung stehende Optimierung der Aufgabenerfüllung geknüpft werden, die mit entsprechenden Nutzenpotenzialen der IT in Verbindung steht.

Einen Beitrag für die notwendige Bedingung für die Anpassung an die „Umgebung“ liefern weiterhin die mit dem Einsatz von Technologien, Methoden und Anwendungen zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse in Verbindung stehenden internen Ordnungsmäßigkeitsvorgaben z. B. in Form der zu verwendenden Standards. Die hinreichende Bedingung für die Anpassung an die „Umgebung“ kann an den optimalen Einsatz und die optimale Implementierung/Umsetzung der Technologien, Methoden und Anwendungen zur Ausrichtung der IT-Prozesse an die Anforderungen der Geschäftsprozesse geknüpft werden, welcher mit entsprechenden Nutzenpotenzialen der IT in Verbindung stehen.

Der Prozess zur Formulierung und Umsetzung der strategisch-operativen Zielsetzungen des Unternehmens ist ständig an das Unternehmensumfeld anzupassen. Die Bedeutung der IT-Security für Formulierung und Umsetzung der strategisch-operativen Zielsetzungen des Unternehmens liegt einerseits darin begründet, dass der entsprechende Anpassungsprozess auch einen Anpassungsprozess an die Umgebung bezüglich der IT-Security umfasst.

Der IT-Security-Prozess ist mit den Unternehmenszielen abzustimmen. Bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander, benötigt das Unternehmen eine entsprechende strategisch-operative Beweglichkeit/Handlungsbefähigung. Die Bedeutung der IT-Security für Formulierung und Umsetzung der strategisch-operativen Zielsetzungen des Unternehmens liegt also andererseits

darin begründet, dass die als Voraussetzung zum Erreichen der strategisch-operativen Zielsetzungen des Unternehmens angesehene strategisch-operative Beweglichkeit/Handlungsbefähigung auch von der IT-Sicherheit entsprechender IT-Systeme abhängt.

Das strategische Performance Management steuert die Formulierung und Realisierung von Strategien, das operative Performance Management stimmt die Unternehmensziele und die Geschäftsprozesse aufeinander ab. Die Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security wurden auf die Unterstützung/Herstellung der strategisch-operativen Beweglichkeit/Handlungsbefähigung bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens bezogen. Strategisch-operative Beweglichkeit/Handlungsbefähigung wird im Modell zum strategisch-operativen Risiko-Controlling als durch Realoptionen abzubildende Entscheidungsfreiheit modelliert. Bei der Formulierung und Umsetzung von Strategien sowie der Abstimmung der Unternehmensziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander muss das Management des Unternehmens entsprechende Entscheidungsfreiheiten haben. Indem die Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security in das strategische und das operative Performance Management im Modell zum strategisch-operativen Risiko-Controlling integriert werden, bildet das strategische und das operative Performance Management einen Anpassungsprozess an die „Umgebung“ bezüglich der IT-Security und einen PDCA-Zyklus im Sinne der ISO 270001 ab.

Aus den Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security ergeben sich so Anforderungen zur Gestaltung der Komponenten des strategischen Performance Managements (strategische Prämissenkontrolle, strategische Überwachung und strategische Durchführungskontrolle) und des operativen Performance Managements (operative Prämissenkontrolle, operative Überwachung und operative Durchführungskontrolle).

Der strategische Teil des strategisch-operativen IT-Security-Managements zielt auf die Optimierung der Effektivität des IT-Security-Managements, und der operative Teil des strategisch-operativen IT-Security-Managements auf die Optimierung der Effizienz des IT-Security-Managements.

Das strategisch-operative Risiko-Controlling (mit der Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in die auf das System bezogene Kontextseite der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse) entwickelt sich so zum organisatorischen Rahmen für den gesamten IT-Security-

Management-Prozess zur strategiekonformen Zielausrichtung und Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander.

Über die Betrachtung von durch die IT-Security beeinflussbaren Nutzenpotenzialen der IT kann die ex-ante Bewertung der IT-Security konkretisiert werden.

Der Nutzen der IT liegt darin, die Prozesse/Anwendungen des Unternehmens effizienter zu gestalten, etwa durch Konsolidierung von dezentralen Anwendungen mit überlappenden Anforderungen auf eine zentrale Plattform (z. B. Portal). Es ist jedoch schwer monetär darzustellen, wenn eine Anwendung „schneller“, „besser“ oder „effizienter“ ausgeführt wird, und daraus ertragswirksame Potenziale abzuleiten. IT-Sicherheit liefert ihren Nutzen über die Anwendungen und Applikationen, die diesen Zustand voraussetzen und die Geschäftsprozesse des Unternehmens unterstützen: Im Zusammenhang mit dem Controlling der IT-Security geht es vor allem um strategische Nutzenpotenziale. Der ex-ante Nutzen eines strategischen IT-Security-Managements wurde als Absicherung der Umsetzung von IT-Projekten identifiziert. Das strategische IT-Security-Management hat die in Optionen ausgedrückte Handlungsbefähigung bei der Umsetzung eines IT-Projekts abzusichern. Dies kann dadurch erfolgen, die für den IT-Security-Prozess zur Absicherung der Priorisierung und Umsetzung von IT-Projekten definierten Risikokomponenten Prämissenrisiko, Umsetzungsrisiken, Überwachungsrisiko zu analysieren, entsprechend zu bewerten und zu steuern. Die Effizienz eines solchen strategischen IT-Security-Managements liegt darin, inwieweit die Absicherung der Priorisierung und Umsetzung von IT-Projekten gelingt. Die Absicherung der Priorisierung und Umsetzung von IT-Projekten wurde gleichzeitig als der ex-ante Nutzen eines solchen strategischen IT-Security-Managements definiert.

Die hinreichende Bedingung für die Anpassung an die „Umgebung“ bezüglich der IT-Security (im Kontext des technisch-organisatorischen Umfelds des Unternehmens) wurde mit der Optimierung der durch die IT-Security beeinflussbaren Nutzenpotenziale/der Effizienz der IT in Verbindung gebracht. Diese Optimierung kann in der Form geschehen, die Maximierung, die Nutzenpotenziale der IT durch geeignete Eskalations- und Risikobewältigungsstrategien sowie ein geeignetes Business Continuity Planning (Notfallplanung/Incident-Management) organisatorisch abzusichern. Diese zielen auf die Unterstützung/Herstellung der Handlungsbefähigung ab. Ein strategisches IT-Security-Management hat also die Unterstützung/Herstellung der Handlungsbefähigung zur Absicherung von Nutzenpotenzialen der IT/zur Absicherung der Effizienz der IT zu gewährleisten. Die ex-ante Absicherung von Nutzenpotenzialen der IT/Absicherung der Effizienz der IT erfolgt durch die Absicherung der Priorisierung und Umsetzung von IT-Projekten.

Zur Analyse der Bedeutung der IT-Security für das Erreichen der Unternehmensziele/Unternehmensstrategie/strategisch-operativen Zielsetzungen des Unternehmens wurde der Einfluss der IT-Security auf Handlungsbefähigung/Flexibilität/strategisch-operative Beweglichkeit (bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander) untersucht.

Die Analyse und Bewertung der strategischen, zukunftsorientierten Bedeutung der Sicherheit von Informationssystemen auf Basis des IT-Security-Frameworks zielt nicht auf die Bewertung der Effektivität oder Effizienz des operativen IT-Security-Managements ab, sondern auf die Beurteilung der Bedeutung der Anforderungen an die IT-Security für die Handlungsfähigkeit/Flexibilität/strategisch-operative Beweglichkeit bei der Umsetzung der strategisch-operativen Zielsetzung des Unternehmens und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander

Die Ausgestaltung der IT-Security geschieht über den IT-Security-Prozess. Eine strategische Bewertung der IT-Security wird innerhalb der Transformation des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen in die auf das System bezogene Seite des Kontexts Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume über die Analyse der drei Risikokomponenten Planungs-, Umsetzungs- und Überwachungsrisiko ermöglicht. Im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen wurden mögliche Auswirkungen auf das Erreichen der Ziele des Unternehmens auf den Ebenen der Unternehmensplanung untersucht. Die ex-ante Bewertung der IT-Security läuft dabei auf die Beurteilung der Unterstützung/Herstellung der Handlungsbefähigung zur Absicherung von Nutzenpotenzialen der IT hinaus.

Anhaltspunkte zur Abschätzung der Gefährdung der Unterstützung/Herstellung der Handlungsbefähigung zur Absicherung von Nutzenpotenzialen der IT aufgrund mangelnder IT-Security sind die Risiken für einen adäquaten IT-Security-Prozess. Diese Risiken sind neben den Prämissen- bzw. Selektionsrisiken der Planung (Irrtumsrisiken der Selektions- und Filterkriterien bei der Fokussierung auf die wichtigsten Prämissen der Security-Strategie), zukünftige Security-Strategie-Umsetzungsgefahren. Als sinnvolles Kriterium für Sicherheit bleibt also die Bewertung der korrekten Bestimmung der Anwendbarkeit und der konsequenten Umsetzung bestehender Methoden, Standards, Tools und Best Practices. (d. h., wie die Richtlinien und die dazu verwendeten Technologien implementiert und umgesetzt werden).

Die Bewertungsdimensionen der Erreichung der Unternehmensziele/strategisch-operativen Zielsetzungen des Unternehmens sind in diesem Zusammenhang dann die der entsprechenden Handlungsbefähigung/Flexibilität/strategisch-operativen Beweglichkeit.

Auf den Planungsebenen für eine Geschäftsfeld-übergreifende Unternehmensstrategie und in den Zieldimensionen der Handlungsbefähigung erfolgt so die Analyse der Zielerreichung als abhängig von den im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen relevanten Aspekten/den Anforderungskriterien an die IT-Security. Diese für die IT-Sicherheit von Systemen relevanten Aspekte/die Anforderungskriterien an die IT-Security beziehen sich auf die von Formulierung und Umsetzung der Strategie und Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander betroffenen Systeme bzw. zu implementierenden Maßnahmen. Die Zieldimensionen der Handlungsbefähigung (Realoptionen) beziehen sich auf die (zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse) eingesetzten Technologien, Methoden und Anwendungen der IT-Projekte (zur Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle des Unternehmens).

Die Zieldimensionen der Handlungsbefähigung/strategisch-operativen Beweglichkeit wurden in Realoptionen ausgedrückt. Es wird so analysiert, welche grundlegenden strategischen Optionen mit welcher IT-Security-Unterstützung gewählt werden können. Die auf den Planungsebenen für eine Geschäftsfeld-übergreifende Unternehmensstrategie untersuchten Zieldimensionen der Handlungsbefähigung können im Prinzip mit den Dimensionen der Erfolgsfaktoren des E-Business (E-Readiness) identifiziert werden:

Wenn das Unternehmen (bei der Umsetzung und Optimierung der Geschäftsprozesse und Geschäftsmodelle zur Ausrichtung der IT-Prozesse an den Anforderungen der Geschäftsprozesse) Realoptionen (bezüglich der eingesetzten Technologien, Methoden und Anwendungen der IT-Projekte sowie der entsprechenden Aufbau- und Ablauforganisation) ausübt, so müssen die Anforderungen der Beherrschbarkeit und Verlässlichkeit der von der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander betroffenen IT-Systeme weiterhin erfüllt sein.

Hierbei unterstützt das strategisch-operative Risiko-Controlling/Controlling der IT-Security den Prozess des strategischen Managements bei der Strategieentwicklung und bei der Strategieumsetzung insofern, dass es die (als Voraussetzung zur Erreichung der Unternehmensziele/strategisch-operativen Zielsetzungen des Unternehmens angenommene) Handlungsbefähigung/Flexibilität/strategisch-operative Beweglichkeit (bei der Umsetzung der

Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander), so weit diese durch die IT-Sicherheit von Systemen beeinflusst wird, überwacht und steuert. Dieses strategisch-operative Risiko-Controlling/Controlling der IT-Security wurde mithilfe der Komponenten (strategische und operative) Prämissenkontrolle, (strategische und operative) Durchführungskontrolle und (strategische und operative) Überwachung eines entsprechenden Performance-Managements als dem klassischen Risikomanagement-/IT-Security-Managementprozess übergeordneter Baustein konzipiert.

Es wurden Anforderungen an die Komponenten des strategischen und des operativen Performance Managements gesucht, die den Bedingungen zur Anpassung an die „Umgebung“ bezüglich der IT-Security genügen. Es wurden somit Bedingungen gesucht, mit denen das entwickelte strategisch-operative IT-Security-Management einen Anpassungsprozess an die „Umgebung“ bezüglich der IT-Security implementiert, der die Formulierung und Realisierung der IT-Security-Strategie steuert, und die Unternehmensziele und den IT-Security-Prozess aufeinander abstimmen soll.

2 Würdigung

Der Business Value der IT-Sicherheit ergibt sich aus Anwendersicht aus der Beherrschbarkeit und damit der Akzeptanz der die IT-gestützten Geschäftsprozesse unterstützenden IT-Systeme und -Prozesse. Dabei ist Compliance als „negativer Treiber“ zu sehen: Der Nutzen entsteht hier dadurch, dass es keine rechtlichen Risiken in Form drohender Sanktionen gibt. Für das Unternehmensmanagement stehen die Optimierung der vorhandenen, und die Ermöglichung neuer, sicherer Geschäftsprozesse im Vordergrund.

Die im Rahmen der Risikominimierung (z. B. nach KonTraG) abgeleitete Pflicht zum Ergreifen von Maßnahmen zum Schutz gegen IT-Sicherheitsrisiken macht sehr unpräzise Vorgaben für Art und Umfang der Maßnahmen. Eine persönliche Haftung des Unternehmers ist daher bei mangelnder Umsetzung diesbezüglich kaum anzunehmen. Sie betrifft eher das Vorhandensein eines angemessenen IT-Sicherheitskonzepts.[1] In diesem Fall kann sogar eine zivilrechtliche (z. B. gegenüber Anteilseignern) deliktische Haftung für durch einen fahrlässig verursachten Fehler entstandene Schäden in Betracht kommen.

Hier kann das entwickelnde Modell für ein Framework, abgebildet als strategisch-operatives Controlling der IT-Security einen Beitrag für ein solches IT-Sicherheitskonzept bilden.

Um zu analysieren, welche relative Bedeutung Einzelrisiken für die Gesamtrisikolage bzw. für einzelne Unternehmens-Kenngrößen haben (Sensitivitätsanalyse), können die Wirkungen von ereignisorientierten Einzelrisiken, z. B. Umsatzschwankungen aus Leistungsrisiken in einem Rechenmodell des Unternehmens beispielsweise den entsprechenden Posten der GuV oder Bilanz zugeordnet werden. In unabhängigen Simulationsläufen kann mit Hilfe von Zufallszahlen ein Geschäftsjahr mehrere tausend Mal durchgespielt und jeweils eine Ausprägung der GuV oder Bilanz berechnet werden. Damit erhält man in jedem Simulationslauf einen Wert für die betrachtete Zielgröße (z. B. Gewinn, Cash-Flow oder Unternehmenswert). Daraus kann theoretisch der Erwartungswert und die Standardabweichung der betrachteten Zielgröße bestimmt werden. Durch Sensitivitätsanalysen ist es weiterhin möglich, die wesentlichen Einflussfaktoren (Einzelrisiken) auf die Zielvariablen zu bestimmen ("Varianzanalyse").[2] Eine klassische Risikoeinschätzung in Verbindung mit der Auswirkung auf die Gewinn- und Verlustrechnung stellt einen Ansatz dar, das Risiko zu quantifizieren, welches durch Sicherheitsmaßnahmen reduziert wird. So werden z. B. durch Risikoeinstufung die als

[1] vgl. Schröder, Georg F. (2006), S.10-12
[2] vgl. Rubenschuh, Marcus (2003)

besonders gefährdet eingestuften Komponenten eines Systems aufgelistet und die Auswirkungen ihres Ausfalls auf die betrachteten Zielgrößen ermittelt. Beispielsweise kann ein technischer Defekt, der zu einem irreparablen Ausfall einer Produktionsanlage führt, den Wert des Anlagevermögens mindern, aber auch den geplanten Bestand an Halb- und Fertigprodukten und damit das Umlaufvermögen sowie die Anzahl absetzbarer Produkte und damit Erträge und Aufwendungen beeinflussen.[1]

Dies war aber kein Untersuchungsgegenstand dieser Arbeit. Die Bedeutung der IT-Security für die Erreichung der Unternehmensziele wurde in ein weniger aufwendigeres Konzept, nämlich den Einfluss der IT-Security auf Handlungsbefähigung/Flexibilität/strategisch-operative Beweglichkeit (bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander), zurückgeführt. Für eine mögliche Gefährdung der in Realoptionen ausgedrückten Handlungsbefähigung (im Sinne der Wahrnehmung von, als Frühindikator für Gefahren verstandenen Risiken) wurden im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen mögliche Ursachen aufgezeigt.

Dieser Ansatz geht in die Richtung einer quantitativen Bewertung der IT-Security auf strategischer (Planungs-)Ebene. Auf dieser Basis könnte z. B. auch untersucht werden, ob und welchen Einfluss die IT-Security auf den Unternehmenswert hat. Es werden so Risiken aus strategischen Werttreibern[2] identifiziert, die Gegenstand der Geschäftssteuerung sind, und sich aus einer Verfehlung der für die Strategieerreichung relevanten Faktoren ergeben.

Der Wert eines Unternehmens kann im Wesentlichen anhand der Parameter Rentabilität, Wachstum und Risiko ausgemacht werden, die direkt miteinander verknüpft sind. Neben dem Umsatzwachstum und der Rentabilität ist das Risiko ein primärer Werttreiber im Unternehmen. Bei steigendem Risiko und gleich bleibender Rentabilität sinkt der Unternehmenswert. Damit hat eine dauerhafte, nachhaltige IT-Sicherheit, die Risiken der IT-Sicherheit vermeidet oder begrenzt bei gleich bleibender Rentabilität einen direkt Unternehmenswert-steigernden Effekt.

Eine Erhöhung des Unternehmenswerts ist nicht alleine durch eine Verbesserung der Ertragsaussichten möglich: Ein proaktives Risikomanagement ist zur Sicherung des Fortbestands des Unternehmens unverzichtbar. Aber auch im Zusammenhang mit einem Rating nach Basel II

[1] vgl. Hölscher, Reinhold (2002), S.268
[2] vgl. Wolf, Klaus (2003b), S.177

können sich durch ein dokumentiertes Risikomanagement beim Unternehmen direkte finanzielle Vorteile in Form besserer Kreditkonditionen ergeben.

Die gezielte Steigerung des Unternehmenswerts ist durch die Nutzung realwirtschaftlicher Flexibilität (Realoptionen) möglich. Auf die Nutzung von Realoptionen bezüglich der mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens bei der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse zielt das in dieser Arbeit entwickelte Modell ab.

Vor allem im Rahmen dieses Ratings nach Basel II ist das „organisationale Kapital“ (Finanzielles Kapital, Soziales Kapital und Humankapital) der entscheidende Faktor für die Beurteilung der Zukunftsfähigkeit des Unternehmens. Das „Kapital“ der IT-Security ist die Effektivität und Effizienz des IT-Security-Managements und soll dem organisatorisch-technischen Strukturkapital zugeordnet werden. Das organisatorisch-technische Strukturkapital sei als Teil des internen intellektuellen Kapitals angesehen. Die Effektivität und Effizienz des IT-Security-Managements ist als Teil des organisatorisch-technischen Strukturkapitals Teil des internen intellektuellen Kapitals und somit des Humankapitals also ein Faktor im Rahmen eines Ratings nach Basel II.

Basel II veranlasst die Unternehmen, sich intensiver mit ihren Risiken, ihrer Identifikation und Analyse als Voraussetzung für deren Steuerung, im Hinblick auf den Fortbestand des Unternehmens, auseinanderzusetzen. Das KonTraG gibt mit der Identifikation und Bewertung direkt nur einen Teil des Risikomanagementprozesses als Pflicht für Unternehmen vor. Um diesen Risikomanagementprozess als einen notwendigen Prozess zur erfolgreichen Unternehmensentwicklung zu verstehen, ist der Prozess mit Risikosteuerung und -kontrolle zu einem Kreislauf auszuweiten. An diesem Punkt setzt (wie z. B. auch COSO (2.2.1)) Basel II an[1], indem hier bei dem Rating zur Festlegung der Kreditkonditionen auch Risikosteuerung und -kontrolle beim Kredit suchenden Unternehmen in die Beurteilung durch die Bank einbezogen wird. So werden implizit Anreize gesetzt, das von KonTraG geforderte Risiko-Früherkennungssystem zu einem Risikomanagement-System auszubauen.[2] Die Unternehmen müssen ihre potenziellen Risiken nun auch steuern und kontrollieren, um im Kontext von Basel II ihre Finanzierungskosten zu senken und ihre Bonität durch ein dauerhaftes Risikomanagement zu sichern.

[1] vgl. Reichling, Peter (2003), S-29,2 9
[2] vgl. Reichling, Peter (2003), S.111

Als Aufgabe für das IT-Risikomanagement als wichtigem Bestandteil des operativen IT-Security-Managements wurde identifiziert

- der Wichtigkeit der zu schützenden Informationen und der Priorität entsprechender Anwendungen angemessene Sicherheitsmaßnahmen zu evaluieren,
- Abhängigkeiten zwischen verschiedenen Bedrohungen, Kausalketten sowie die Attraktivität des Unternehmens als potenzielles Angriffsziel für Angreifer zu reduzieren. Die Komplexität dieser Abhängigkeiten kann durch die sog. lose Kopplung reduziert werden. Diese lose Kopplung wird bezüglich der Integration der im Unternehmen eingesetzten IT-Lösungen und der unternehmensübergreifenden Datenintegration mittels einer Service-orientierten Architektur (SOA) unterstützt, wo die Anwendungslandschaft aus lose gekoppelten Anwendungsbausteinen mit klar modellierten Schnittstellen besteht, die über wohl definierte Services miteinander kommunizieren.

Allgemein kann die Fähigkeit von Geschäftsvorgängen, Organisationen und technischen Systemen, bei unvorhergesehenen Ereignissen das Geschäft fortzuführen und vor Schaden zu bewahren, durch die lose Kopplung unterstützt werden.

Ein Geschäftsmodell wird als kurze Beschreibung der Strukturierung einer neuen geschäftlichen Aktivität verstanden. Es erfüllt im Kontext eines Geschäftsplans die Rolle, (strategische) Szenarien und Handlungsmöglichkeiten zu beschreiben und soll mit Innovationen und Unsicherheit (Ungewissheit) umgehen. Es soll erklären, wie gedachte (Wettbewerbs-)Vorteile strukturiert sind und umgesetzt werden können.[1] In diesem Sinne könnte man das hier entwickelte Modell als Geschäftsmodell bezeichnen.

Das entwickelte strategisch-operative Risiko-Controlling setzt nicht auf den Phasen Risikoidentifikation und Risikobewertung des klassischen Risikomanagement Prozesses auf. Es bezieht sich wie das generelle Risiko-Controlling[2] auf Planungsrisiken infolge der Ungewissheit. Dieses Risiko-Controlling wird nicht als Teil des Prozesses zur Identifikation, Bewertung, Steuerung und Überwachung von Risiken, sondern (ähnlich der Risikoüberwachung i. w. S., die das Risikomanagement-System überwacht, und nicht als Teil des Prozesses zur Identifikation, Bewertung, Steuerung, Überwachung i. e. S. und Kommunikation von Risiken gesehen wird[3]), als ein übergeordneter/unabhängiger Baustein betrachtet. Die Überwachung

[1] vgl. Ehrmann, Thomas (2006), S.220,221
[2] vgl. Martin, Thomas A. (2002), S.122
[3] vgl. Seidel, Uwe M. (2002), S.70

i. w. S. überwacht die auf den Regelkreislauf Risikomanagement (z. B. in Form personeller oder organisatorischer Risiken) einwirkenden Gefahren, dass die Unternehmensrisiken nicht ausreichend identifiziert und abgewehrt werden. Ähnlich steuert das strategisch-operative Risiko-Controlling, welches das IT-Security-Management zum strategisch-operativen IT-Security-Management erweitert, die auf den das Erreichen der strategisch-operativen Zielsetzung des Unternehmens in Form mangelnder strategisch-operativer Beweglichkeit bei der Umsetzung der Unternehmensziele einwirkenden Gefahren. Der in das strategisch-operative Risiko-Controlling über das strategische und operative Performance-Management integrierte Anpassungsprozess an die Umgebung bezüglich der IT-Security sorgt dafür, dass der Prozess zur Formulierung und Umsetzung der strategisch-operativen Zielsetzungen des Unternehmens, bezüglich der IT-Security ständig an das Unternehmensumfeld angepasst wird. Der Bezug zur IT-Sicherheit von Systemen wurde über deren Bedeutung für die als Voraussetzung zum Erreichen der strategisch-operativen Zielsetzungen des Unternehmens gesehene strategisch-operative Beweglichkeit/Handlungsbefähigung (bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander) hergestellt. Dieser Baustein besteht aus einer Analyse der Bedeutung der Anforderungen an die IT-Sicherheit von Systemen für die Ausübung von Realoptionen durch das Unternehmen.

Die Anforderungen an die IT-Security sollen unabhängig von der Wahl möglicher Strategieoptionen durch das Unternehmen erfüllt sein. Das Grundprinzip z. B. auf der Ressourcenebene besteht darin, mit einer für den normalen Bedarf überdimensionierten Hardware-Ausstattung bei Bedarf Ressourcen zu- oder abschalten zu können. Außerdem kann als spezieller Aspekt der IT-Governance die Aufgabe des Top-Managements zur Steuerung der IT-Funktionen [1] unterstützt werden. Dazu muss die IT-Security an den ex-ante möglichen Optionen des Geschäfts ausgerichtet werden.

Die Strategie zur Risikosteuerung ähnelt dann am ehesten der Risikokompensation (Risikoakzeptanz), denn im Bereich der IT-Security greifen die Risikosteuerungsstrategien Risikovermeidung, -vermindeung, -überwälzung typischerweise nicht. Das auf dem strategisch-operativen Risiko-Controlling basierende IT-Security-Management betrachtet über (strategische und operative) Prämissenkontrolle, (strategische und operative) Überwachung und (strategische und operative) Durchführungskontrolle Effektivität und Effizienz des IT-Security-Managements quasi gleichzeitig. Während das Unternehmen strategisch in Geschäftsprozessen denkt, handelt die Organisation in Abläufen innerhalb funktional aus-

[1] Krupp, Thomas (2006)

gerichteter Abteilungen. Eine ganze Reihe anderer Managementthemen, wie das Projektmanagement, Qualitätsmanagement oder das Risikomanagement soll sich über Business Process Management (BPM) besser darstellen lassen. So haben das Risikomanagement und das IT-Security-Management ebenfalls eine strategische Dimension, eine Geschäftsprozessdimension, eine Architekturdimension und eine Umsetzungsdimension.

Auf dem klassischen „Pfad“ von der Strategieebene (strategische Sichtweise, Geschäftsfelder und ihre Erfolgsfaktoren) über die Ebene der Organisation (Effizienz) und der Geschäftsprozesse zur Ebene der IT-Sicherheit/IT-Security (der das Business Process Management (BPM) und das Corporate Performance Management (CPM) einschließt), würde ein so definiertes IT-Security-Management Effektivität und Effizienz nacheinander betrachten.. Mit dem strategisch-operativen IT-Security-Management wurde im Sinne des. „Launch & Learn“–Ansatzes ein IT-Security-Management entwickelt, bei dem die IT-Security-Strategie in einem dynamischen Prozess während der Implementierung laufend angepasst, erweitert und verfeinert werden kann. BPM passt die Geschäftsprozesse an die Unternehmensstrategie an. CPM „synchronisiert“ die Unternehmensstrategie mit der IT-Strategie. Bei dem entwickelten strategisch-operativen IT-Security-Management steht die Abstimmung der Unternehmensziele mit dem IT-Security-Prozess im Mittelpunkt; die strategisch-operative Beweglichkeit einerseits bei der Formulierung und Umsetzung der Unternehmensstrategie und andererseits der Abstimmung der Unternehmensziele mit dem IT-Security-Prozess sollen unterstützt werden. Dies gelingt dem auf die strategisch-operative Handlungsbefähigung abzielenden strategisch-operativen Risiko-Controlling dadurch, dass es über das strategische und operative Performance-Management die Bedingungen zur Anpassung an die Umgebung bezüglich der IT-Security in das Modell integriert, um so die Strategie konforme und IT-Nutzenpotenzial absichernde Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume so weit möglich zu gewährleisten,

Allerdings stellt die Abbildung des IT-Security-Frameworks in Form des strategisch-operativen IT-Security-Managements auf Basis des strategisch-operativen Risiko-Controllings, das auf die Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit (bei der Durchsetzung/Umsetzung/Implementierung der Unternehmensstrategie und Abstimmung der Unternehmensziele und der Geschäftsprozesse/Geschäftsmodelle aufeinander) abzielt, keinen 1:1-Ersatz für den klassischen „Pfad“ von der Strategieebene (strategische Sichtweise, Geschäftsfelder und ihre Erfolgsfaktoren) über die Ebene der Organisation (Effizienz) und der Geschäftsprozesse zur Ebene der IT-Sicherheit/IT-Security dar. Denn die Gewährleistung der Handlungsbefähigung/strategisch-

operativen Beweglichkeit ist eigentlich kein direkter Erfolgsfaktor auf der Strategieebene. Die Gewährleistung der Handlungsbefähigung/strategisch-operativen Beweglichkeit abzusichern/zu unterstützen steht aber im Zusammenhang mit der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume im Mittelpunkt.

.

In Anlehnung an die Unterscheidung zwischen Problem-, Wirkungs-, Eingriffs- und Lösungsbereich im Systems Engineering können in der Risikoanalyse die drei Bereiche Ursachen-, Wirkungs- und Eingriffsbereich unterschieden werden. Dem Eingriffsbereich werden diejenigen Prozesse bzw. Schritte zugeordnet, in denen die Möglichkeit risikopolitischer Maßnahmen besteht. Für die Erfassung und die anschließende Beurteilung von Risiken ist ein klares Bild über die strategischen und operativen Zielvorgaben des Unternehmens unabdingbar. Gegebenenfalls hat vor der Risikoerfassung eine umfassende Analyse der Unternehmensstrategie, des Unternehmensumfelds sowie der Risiken und Chancen zu erfolgen. Ohne eine regelmäßige, systematische Analyse auf allen Ebenen ist ein effektives Management nicht möglich.[1]

Die Bewertung auf den Ebenen der Unternehmensplanung/zukünftige Bedeutung der IT-Security hat einerseits die inhärenten Risiken des Prüffelds „Beurteilung z. B. des Managements, inwieweit das Erreichen der Unternehmensziele trotz Risiken der IT-Security gewährleistet ist“ (ex-ante IT-Security) zu beurteilen. Anhaltspunkte dafür sind die Relevanz, Anwendbarkeit und konsequente Umsetzung der Methoden, Standards, Tools und Best Practices zur Erreichung der aus den Unternehmenszielen abgeleiteten IT-Security-Ziele. Andererseits ist das entsprechende Kontrollrisiko zu beurteilen. Anhaltspunkte dafür sind Unzulänglichkeiten bei der Bestimmung der Relevanz, Anwendbarkeit sowie der konsequenten Umsetzung der Methoden, Standards, Tools und Best Practices zur Erreichung der aus den Unternehmenszielen abgeleiteten IT-Security-Ziele. Die Steuerung dieses Kontrollrisikos (im Rahmen des IT-Security-Managements) besteht aus (in den PDCA-Zyklus des Informationssicherheitsmanagementprozesses integrierter) Prämissenkontrolle, strategischer Durchführungskontrolle und strategischer Überwachung. So wurden im Zusammenhang mit den inhärenten Risiken die Anforderungen analysiert, die zur Erreichung der strategischen Zielsetzung notwendig sind. Im Zusammenhang mit dem Kontrollrisiko kann zur Bewertung der zukünftigen Bedeutung der IT-Security die Unterstützung/Herstellung der Handlungsbefähigung zur Absicherung von Nutzenpotenzialen/der Effizienz der IT bzw. der Ab-

[1] vgl. Hölscher, Reinhold (2002), S.101

sicherung der Priorisierung und Umsetzung von (diese Nutzenpotenziale generierenden) IT-Projekten analysiert werden.

Die Anforderungskriterien an die IT-Sicherheit können in den Kontext der Handlungsbefähigung trotz Unsicherheit projiziert werden, wenn man als Umwelt das technisch-soziale Umfeld betrachtet. Dies führt neben der Verlässlichkeit (beurteilt nach den Kriterien Verfügbarkeit, Integrität und Vertraulichkeit) und Beherrschbarkeit (beurteilt nach den Kriterien Nachprüfbarkeit, Rechtssicherheit) zu einer dritten Sicht der Beurteilung/Bewertung der IT-Security, nämlich der Handlungsbefähigung.

Aufgabe des operativen Controllings der IT-Security, welches auf adäquater Risikoüberwachung und Risikosteuerung basiert ist, Eskalations- und Risikobewältigungsstrategien sowie das Business Continuity Planning (Notfallplanung/Incident -Management) zu unterstützen.

Man befindet sich bei Eskalations-, Risikobewältigungsstrategien, Business Continuity Planning (Notfallplanung/Incident Management) also auf Ebene von IT-Risiken. Wenn die auf die strategische Zielsetzung einwirkenden und deren Erreichung gefährdenden Risiken nicht vorhersehbar/abschätzbar sind, ist es sinnvoller, die Anforderungen zu analysieren, die zur Erreichung der strategischen Zielsetzung notwendig sind. Hierzu hat das strategische Controlling der IT-Security zu untersuchen, welche Aspekte der IT-Security (unabhängig von bestehenden IT-Security Methoden, Standards, Tools und Best Practices) bezüglich möglicher Auswirkungen auf die Erreichung der Unternehmensziele relevant sind. Damit werden Einflussfaktoren für das Erreichen der Zieldimensionen des IT-Security-Prozesses ermittelt, welche auch Beurteilungshinweise für die strukturiert-strategische ex-ante Bewertung der IT-Security darstellen. Diese Einflussfaktoren wurden mit der Kritikalität/Sensitivität entsprechender Sachwerte und Prozesse sowie der notwendigen Beherrschbarkeit der von der Umsetzung der IT-Security-Strategie betroffenen Systeme bzw. zu implementierenden Maßnahmen angesetzt.

Die auf die auf das System bezogene Kontextseite der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse bezogenen Ziele (bezüglich der Unterstützung strategisch-operativer Handlungsspielräume) sollen in entsprechende Anforderungen auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen projiziert werden. Diese Vorgehensweise stellt die Alternative zur Antizipation von Risiken (Voraussehen negativer Ereignisse und ihrer Folgen) auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen dar. Aus den identifizierten Anforderungen werden dann

Maßnahmen abgeleitet, die, anstatt den ex-ante nicht antizipierbaren Risiken entgegenzuwirken, die Anforderungen abdecken.

Somit ist ein Konzept für die ex-ante Revision der IT-Security in der Einsatzumgebung des IT-Systems erstellt: Dieses gibt vor, die durch die IT-Security beeinflussbaren Bedingungen zur Gewährleistung des Erreichens der Unternehmensziele/strategisch-operativen Zielsetzungen des Unternehmens herzustellen. Zur Untersuchung der durch die IT-Security beeinflussbaren Bedingungen zur Gewährleistung des Erreichens der Unternehmensziele/strategisch-operativen Zielsetzungen des Unternehmens kann der Einfluss der IT-Security auf Handlungsbefähigung/Flexibilität/strategisch-operative Beweglichkeit (bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander) analysiert werden.

Diese ex-ante Revision kann als „Managed Security Service“ z. B. auch als externe Dienstleistung erbracht werden. Managed Security Service – Anbieter unterstützen den Kunden beim Umgang mit sicherheitsrelevanten Daten, aber auch dem vollständigen Management der Sicherheitssysteme.[1] Im Kontext der behandelten Problematik geht es um die Ausgestaltung der IT-Sicherheitsinfrastruktur:

Das Aufzeigen von Handlungs-/Gestaltungsoptionen[2] gehört zu den wesentlichen Inhalten der IT-Strategie; die Analyse des Einflusses der IT-Security für diese Handlungs-/Gestaltungsoptionen ist Aufgabe des strategischen Controllings der IT-Security. Eingebettet in das strategisch-operative Risiko-Controlling wird das IT-Security-Management also auf die Unterstützung der IT-Strategie, in Form des Aufzeigens und der Analyse der Bedeutung der IT-Security für diese Handlungs-/Gestaltungsoptionen ausgerichtet: In das entwickelte Modell zum strategisch-operativen Risiko-Controlling integriert, zielt das IT-Security-Management auf die Unterstützung/Herstellung der strategisch-operativen Beweglichkeit/Handlungsbefähigung und damit auf einen sog. „Flexibilitätswert“[3] ab.

Als Dimensionen der Handlungsbefähigung/Flexibilität/strategisch-operative Beweglichkeit wurden Realoptionen angesetzt und der Einfluss der IT-Security auf Handlungsbefähigung/Flexibilität/strategisch-operative Beweglichkeit (bei der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander) auf den Planungsebenen für eine Geschäftsfeld übergreifende Unternehmens-

[1] vgl. Nedon, Jens (2003)
[2] vgl. Gadatsch, Andreas (2006), S.41
[3] vgl. Niemann, Rainer (2001), S.39

strategie betrachtet. Ziel der ex-ante Revision der IT-Security in der Einsatzumgebung des IT-Systems ist es, dass die Anforderungen an die IT-Security der von der Umsetzung der Unternehmensstrategie und der Abstimmung der Unternehmensziele und des IT-Security-Prozesses aufeinander betroffenen IT-Systeme unabhängig von der eventuellen Ausübung entsprechender Realoptionen durch das Unternehmen erfüllt sind. Diese Anforderungen sind es, die - wenn die auf die strategische Zielsetzung einwirkenden und deren Erreichung gefährdenden Risiken nicht vorhersehbar/abschätzbar sind - zur Umsetzung der strategischen Zielsetzung notwendig sind und sich auf die Objekte beziehen, für die man eigentlich eine Risikoanalyse durchführen müsste. Diese Anforderungen sind die mit der strategischen und operativen Durchführungskontrolle aufzudeckenden Umsetzungsrisiken, nämlich die notwendige Verlässlichkeit und Beherrschbarkeit der von der Abstimmung der Unternehmensziele und Geschäftsprozesse/des IT-Security-Prozesses aufeinander betroffenen Systeme bzw. zu implementierenden Maßnahmen. Aus diesen Anforderungen können dann Maßnahmen abgeleitet werden, die, anstatt den ex-ante nicht identifizierbaren Risiken entgegenzuwirken, die entsprechend der Kritikalität der betreffenden IT-Objekte relevanten Anforderungen präventiv abdecken. So wird die Alternative zur Antizipation von Risiken auf Ebene des technisch-organisatorischen Kontexts für die IT-Sicherheit von Systemen operationalisiert.

Wird diese Bedingung in die Security Policy aufgenommen, so kann das entwickelte Modell als Security Model[1] im Sinne einer Darstellung der Security Policy des Unternehmens aufgefasst werden.

Die Vorgehensweise zur Ableitung von Beurteilungshinweisen für die strategische ex-ante Bewertung entspricht der an den Geschäftsrisiken der Organisation orientierten Einschätzung der Geschäftsprozesse hinsichtlich der Sicherheitsziele über das Kriterium „Einfluss auf Managemententscheidungen“, angelehnt an Information Security Forum - Business Impact Analysis.

Diese Vorgehensweise ist im Prinzip in Analogie mit dem Ziel der Risikobewertung zu sehen, nämlich welche Risiken bei der vorgegebenen Zielsetzung relevant und wesentlich sind, wie stark der Risikofaktor auf das Unternehmen einwirkt. Letzteres ist auch der erste Schritt bei der Bestimmung eines sog. Absicherungsprofils, mit dessen Hilfe dargestellt wird, „inwiefern die bei der Risikoidentifikation ermittelten Risiken auf das Unternehmen einwirken und in welchem Umfang Gegenmaßnahmen bereits ergriffen wurden, um diese Risikoposition zu

[1] vgl. Fischer-Hübner, Simone (2001), S.38

optimieren“.[1] „Wie stark der Risikofaktor auf das Unternehmen einwirkt“ bezieht sich auf die strategisch-operative Beweglichkeit und die Unterstützung/Herstellung der Handlungsbefähigung. Risikofaktoren sind Planungs-, Umsetzungs- und Überwachungsrisiko bezüglich der mittels geeigneter IT-Projekte angestrebten strategisch-operativen Ziele. Dieses Planungs-, Umsetzungs- und Überwachungsrisiko bezieht sich im Gegensatz zum inhärenten Risiko oder zum Kontrollrisiko des Prüffelds „Beurteilung z. B. des Managements, inwieweit das Erreichen der Unternehmensziele trotz Risiken der IT-Security gewährleistet ist“ nicht auf IT-Risiken selber, sondern auf die Anforderungen, die im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen zur Erreichung der strategischen Zielsetzung notwendig sind.

Wie bei der erfolgreichen Umsetzung des Value Based Management sind für die Bestimmung der notwendigen Steuerungsinformationen und die Implementierung des Zielbildungs- und Zielverfolgungsprozesses adäquate Controllingprozesse unentbehrlich.[2] Ähnlich einem Kreditrisikocontrolling, das für Einrichtung und Qualitätssicherung des internen Ratings verantwortlich ist,[3] dient das durch die drei Komponenten (strategische und operative) Prämissenkontrolle, (strategische und operative) Durchführungskontrolle und (strategische und operative) Überwachung definierte Controllingsystem sozusagen der Qualitätssicherung dieser Bewertung.

In der Tat macht es einen Unterschied in der Bewertung, ob man ein Risiko selber steuern kann, oder ob man es passiv hinnehmen muss.[4] Auf diesen „Flexibilitätswert“ wird in Form der Unterstützung/Herstellung der strategisch-operativen Beweglichkeit/Handlungsbefähigung durch das entsprechend aufgebaute Modell zum strategisch-operativen Risiko-Controlling fokussiert. Die Sicherheit von Informationssystemen ist dahin gehend auszugestalten, dass ex-ante die Strategie konforme und IT-Nutzenpotenzial maximierende organisatorische Abwicklung der Geschäftsprozesse des Unternehmens unterstützt werden soll. Dazu ist der erwähnte Flexibilitätswert zu generieren, wobei ein Anpassungsprozess an die Umgebung bezüglich der IT-Security zu integrieren ist.

[1] Reichling, Peter (2003), S.225
[2] vgl. Wolf, Klaus (2003b, S.25
[3] vgl. Töpfer, Armin (2003), S.30
[4] vgl. Hölscher, Reinhold (2002), S.75

3 Ausblick

Mit dem Fortschritt in Wissenschaft und Technik steigt das Ausmaß potenzieller Schäden aufgrund immer komplexerer technischer Systeme. Insbesondere für strategische Werttreiber, die bestandsgefährdende Risiken der künftigen Entwicklung zur Folge haben können, nimmt die Wichtigkeit der aus weichen Faktoren in Form qualitativer Risiken resultierender Gefährdungspotenziale zu.[1]

Die technische Entwicklung in zahlreichen Bereichen kann vom Einzelnen kaum mehr nachvollzogen werden. Daher wird der technischen Entwicklung oftmals mit irrationaler Angst begegnet, welche wiederum zu Schadensvermutungen verbunden mit Kausalitätsbehauptungen führt. Diese münden häufig in Ansprüchen gegenüber dem vermeintlichen Schadensverursacher. Gleichzeitig steigen mit dem Rückgang der Risikoakzeptanz der Öffentlichkeit aufgrund der öffentlichen und politischen Meinung die in Schadenersatzprozessen zuerkannten Entschädigungssummen.[2] Dieser Trend wird noch zunehmen, sodass eine nachvollziehbare Revision/ein nachvollziehbares Controlling von Konzepten und Maßnahmen zur Risikosteuerung immer wichtiger wird.

In gewisser Weise trägt die Unterscheidung des ISO TR 13335-1 zwischen drei Arten der Sicherheitspolitik diesen Tendenzen Rechnung: Unterschieden werden Unternehmensweite Sicherheitspolitik (Corporate Security Policy), Unternehmensweite IT-Sicherheitspolitik (Corporate IT Security Policy) und Sicherheitspolitik des IT-Systems (IT System Security Policy). Die Sicherheitspolitik des Unternehmens wird so transparenter und nachvollziehbarer. Die Überlegungen in dieser Arbeit betrafen die Ebenen IT System Security Policy und (da das IT-Sicherheitsmanagement im Zusammenhang mit Revision und Controlling der IT-Security unternehmensweit zu sehen ist) die Ebene Corporate IT Security Policy. Die Bedeutung dieser Unterscheidung zwischen drei Arten der Sicherheitspolitik wird in Zukunft zunehmen.

[1] vgl. Wolf, Klaus (2003b, S.179
[2] vgl. Dahmen, Jörn (2002), S.16-17

Literaturverzeichnis

Allenspach, Marco (2001):

Integriertes Risiko-Management, Institut für Versicherungswirtschaft der Universität St. Gallen

Amann, Marion (2006):

Reif für den Paradigmenwechsel, in: IT Fokus Ausg.9/10 S.34-35, IT Verlag

Armbruster, Marcus J. (2005):

Prozesse im geordneten Fluss, in: IT Fokus Ausg.9/10 S.48-51, IT Verlag

Armbruster, Marcus/Niegel, Andreas /2006):

Gestaltung von Geschäftsprozessen aus Sicht der Anwender, in: IT Fokus Ausg.9/10 S.30-33, IT Verlag

Arnold, Jörg/Frisch, Wolfgang (2005):

Die erweiterte Revision, Beck Verlag

ASTRUM IT (2005):

Gemeinsame Nutzung von COBIT, ITIL und BS7799, in: IT Management Ausg.5 S.55, IT Verlag

Baker, Sean (2005):

Zusammenarbeit über Dienste, in: IT Management Ausg.11 S.56-58, IT Verlag

Bascurov, Oleg (2005):

Federated Identity Management, in: IT Fokus Ausg.1/2 S.46-50, IT Verlag

Becker, Thomas (2005):

Netzwerkmanagement, Springer

Berens, Wolfgang (2004):

Controlling im E-Business, Lang Verlag

Bernhard, Martin G. (2005):

IT-Security-Management nach ITIL, in: Schoolmann Jürgen/Rieger Holger: Praxis-handbuch IT-Sicherheit, S.93-138, Symposium Publishing

Berninghaus, Siegfried (2002)

Strategische Spiele, Springer Verlag

Besemann, Martin (2005):

Nicht schätzen, sondern wissen, in: IT Management Ausg.9, S.30-33, IT Verlag

Betz, Martin (2006):

Über Grenzen hinweg, in: IT Management, Ausg. 1 S.8-15, IT Verlag

Bieberstein, Norbert (2006):

Das Service-orientierte Ökosystem, in IT Management, Ausg.2 S.22-28, IT Verlag

Bieta, Volker/Siebe, Wilfried (1998):

Spieltheorie für Führungskräfte, Wirtschaftsverlag Carl Ueberreuter

Bischof, Jürgen (2002) :

Die Balanced Scorecard als Instrument einer modernen Controlling-Konzeption, Dt. Univ.-Verlag

Bieta, Volker (2004):

Szenarienplanung im Risikomanagement, Wiley Verlag

BITKOM (2005):

Kompass der IT-Sicherheitsstandards, online verfügbar unter: www.bitkom.org/files/documents/BITKOM_Broschuere_Sicherheitsstandard_V1.01f.pdf (30.10.05)

BMJ (2002).

Bekanntmachung des Deutschen Rechnungslegungs-Standards Nr.12, Bundesanzeiger vom 22.10.2002 Nr.197a

Bosse, Richard/Scholz, Wolfgang (2007):

Erkennen und Bekämpfen von Mitarbeiterkriminalität, in: PRev Ausg.I S.5-12, Ottokar Schreiber Verlag

Brewing, Josef (2005):

Der Blick aufs Ganze, in: IT Security Ausg.4 S.32-34, IT Verlag

Brezski, Eberhard (2004):

Finanzmanagement und Rating kompakt, Schäffer-Poeschel

Bruns, Hans-Georg/Thuy, Michael G./Zeimes Markus (2003)::

Die Bilanzierung von immateriellen Vermögenswerten des Anlagevermögens im Konzernabschluss, in: Controlling Heft 3/4 S.137-142, Vahlen

BSI (2003):

Artikel zu Common Crriteria: Evaluation Assurance Level (EAL), online verfügbar unter: www.bsi.de/cc/eal_stufe.htm (3.11.2005)

BSI (2006):

IT-Sicherheitsmanagement und IT-Grundschutz, Bundesanzeiger-Verlag

BSI (2007):

Formale Methoden für mehr Sicherheit, in: IT Security Ausg.2 S.50-51, IT Verlag

BSI & Secure Net GmbH (2007):

Schutz von Web-Anwendungen, in: IT Security Ausg.3 S.24-27, IT Verlag

Buchta, Dirk Uwe (2004):

Strategisches IT Management, Gabler

Burger, Anton/Buchhart, Anton (2002):

Risiko-Controlling, Oldenbourg

Burkhard, Markus (2006):

Wer klopft an meine Tür, in IT Fokus Ausg.1/2 S.42-44, IT Verlag

Bursch, Daniel (2005):

IT-Security im Unternehmen, VDM-Verlag

Cazemier, Jacques A. verbeek Paul L./Peters, Louk M.C. (2004):

Security Management, OGC (Office of Government Commerce)

Chamoni, Peter (2004).

Informationssysteme in Industrie und Handel, Business Intelligence, Knowledge supply and information logistics in enterprises and networked organizations, organisationale Intelligenz, Akad. Verl.-Ges.

Chanliau, Marc (2004):

Secure Federation – Definitionen, Use-Cases, Szenarien, in: IT Fokus Ausg.9/10 S.60-63, IT Verlag

Coester, Ursula/Hein, Matthias (2005):

IT-Sicherheit für den Mittelstand, Datakontext

Collenberg, Thomas/Wolz Matthias (2005):

Zertifizierung und Auditierung von IT- und IV-Sicherheit, Vahlen

Copeland, Thomas E. (2002)

Realoptionen, Wiley

Currle, Michael (2002):

Performance-Management für IT-Services, Dt. Univ.-Verlag

Dahmen, Jörn (2002):

Prozeßorientiertes Risikomanagement zur Handhabung von Produktrisiken, Shaker

Dahmer, Ralf (2006):

Haftungsrisiken in der IT minimieren, in: IT Security Heft 1 S.12-14, IT Verlag

Dahmer, Ralf (2007):

Redundanz und Wirtschaftlichkeit, in: IT Security Heft 2 S.14-15, IT Verlag

Damovo (2006)

Security-Framework von Damovo macht IP-Telefonie sicher, online verfügbar unter: http://www.damovo.de/DE/press/2005/preview_IT-Telefonie%20ist%20sicher.htm (13.9.20006)

Dampf, Manfred (2006):

Service-Kapseln, in: IT Fokus Ausg. 34 S.14-20, IT Verlag

Deininger, Olaf (2005):

Kostbare Informationstechnik, in: IT Security Ausg.3 S.18-21, IT Verlag

Deutsches Institut für Interne Revision (1998):

Grundsätze risikoorientierter Unternehmensüberwachung, in: ZIR Heft 5 S.237-248

Deutsches Rechnungslegungs Standards Committee (2002):

Immaterielle Vermögenswerte des Anlagevermögens, Bundesanzeiger vom 22.10. Nr.197a

Diederichs, Marc (2004)

:Risikomanagement und Risikocontrolling, Vahlen

Dietrich, Lothar (2004):

IT im Unternehmen, Springer

Dolezch, Timm (2003):

Unternehmensbewertung und Wachstum, Bankakademie-Verlag

Dollinger Bernd F./Schmidt Rainer (2004):

Prozesse lernen laufen, in: IT Fokus Ausg.11/12 S.12-16, IT Verlag

Drecker, Norbert (2006):

Digitale Drehkreuz, in: IT Fokus Ausg.7/8 S.18-21, IT Verlag

Eckert, Claudia (2003):

IT-Sicherheit, Oldenbourg

Edelmüller, Martina (2003)

Arten von Optionen in IT-Projekten und ihre Bewertung , online verfügbar unter:

wwwai.wu-wien.ac.at/~koch/lehre/inf-sem-ws-02/edelmueller/9550917.pdf (9.4.2007)

Ehrmann, Thomas (2006) :

Strategische Planung, Springer

Elting, Andreas (2005):

Business Process Management (BPM) im Großen, in: IT Fokus Ausg.3/4 S.32-38, IT Verlag

Elsässer, Wolfgang (2005)

ITIL einführen und umsetzen, Hanser Verlag

Engl, Roland (2006):

ITIL und Cobit: gemeinsamer Einsatz, in: IT Management Ausg.10 S.38-43, IT Verlag

Ernst & Young (2005):

IT Security Workshop „extreme Hacking“, angekündigt z.B. in IT-Fokus Ausg.7/8 S.22-23, IT Verlag

Eschenbach, Rolf (2003):

Strategische Konzepte, Schäffer-Poeschel

Essigke, Andreas (2005):

Aufbruch in neue Dimensionen, in: IT Fokus Ausg.11/12 S.40-43, IT Verlag

Fähnrich, K.P./Grawe, Tonio (2005):

Service-Integration, in: IT Management Ausg.11 S.22-27, IT Verlag

Fassbender, Pantaleon (2001):

Werte und Integritätsmanagement, in: Wieland, Josef: Human capital und Werte, Metropolis-Verlag

Ferre, David (2003):

RAFC unter Kontrolle, Revision Ausg.III S.37-39, Ottokar Schreiber Verlag

Fischer, Bettina (2005):

The Power of Now!, in: IT Management Ausg.11 S.52-55, IT Verlag

Fischer-Hübner, Simone (2001):

IT-security and privacy, Springer

Förschle, Gerhart/Peemöller, Volker H. (2004):

Wirtschaftsprüfung und interne Revision, Verl. Recht und Wirtschaft

Foerster, Udo (2002):

Unternehmen sollten das Ratingverfahren im Rahmen von Basel II, Zeitschrift der Gründerregion Aachen, Ausg.3 online verfügbar unter: www.gruenderregion.de/gzeitung/2002_3/finanzielles.htm, (11.9.2005)

Foth, Michael (2006a):

Mobile Sicherheit – Widerspruch mit Lösungen, in: PRev Ausg.I S.35-39, Ottokar Schreiber Verlag

Foth, Michael (2006b):

Prüfung durch alle Schichten, in: PRev Ausg.III S.40-43, Ottokar Schreiber Verlag

Foth, Michael (2006c):

Im Dschungel der Telegesetze, in: Interne Revision Jahrbuch 2007 S.131-166, Ottokar Schreiber Verlag

Freihube, Klaus (2001) :

Die Bedeutung und die Bewertung von Realoptionen (Handlungsspielräumen) in der wertorientierten Unternehmensführung, Dissertation Freie Universität Berlin

Frohn, Michael/Parthier, Ulrich (2005):

Die Gefahr, die mit dem Internet kam, in: IT Security Ausg. 7/8 S.14-15, IT Verlag

Fink, Alexander (2001):

Erfolg durch Szenario-Management, Campus-Verlag

Finke, Robert (2005)

Grundlagen des Risikomanagements, Wiley-VCH

Funk-Kadir, Thomas (2006):

Ein Weg aus dem Wirtschaftlichkeits-Dilemma, in: IT Management Ausg.4 S.28-32 IT Verlag

Füser, Karsten (2006):

Säulen für die Sicherheit, in: IT Security Ausg.2 S.12-17, IT Verlag

Gadatsch, Andreas (2003):

Grundkurs Geschäftsprozess-Management, Vieweg

Gadatsch, Andreas (2004):

Grundkurs IT-Controlling, Vieweg

Gadatsch, Andreas (2006):

Masterkurs IT-Controlling, Vieweg

Gaulke Markus (2003):

IT-Risk-Framework

Geis, Ivo (2005):

E-Mail und Revision, in: ReVisiion Ausg.II S.14-16, Ottokar Schreiber Verlag

Gerick, Thomas (2004):

IT-Infrastrukturen ordnen, in: IT Management Ausg.9 S.10-15, IT Verlag

Geschonnek, Alexander (2006):

Forensische Tools im Überblick, in: IT Security Ausg.7/8 S.40-45, IT Verlag

Giefer, Katrin (2006):

Risikomanagement in der IT, Berechenbare Risiken, in: IT Security Ausg.2 S.20-24, IT Verlag

Glemser, Tobias (2006):

Penetrationstesta, Schutz vor Hackern, in: IT Security Ausg.3 S.22-30, IT Verlag

Gleißner, Werner/Meier, Günter (2000):

Risikomanagement als integraler Bestandteil der wertorientierten Unternehmens-führung, DSWR 29.Jg Heft 1/2 S.6-10

Goeken, Matthias/Burmester, Lars (2004):

Entwurf und Umsetzung einer Business-Intelligence-Lösung für ein Fakultäts-controlling, in: Chamoni, Peter: Informationssysteme in Industrie und Handel, Business Intelligence, Knowledge supply and information logistics in enterprises and networked organizations, Akad. Verl.-Ges, S.137-166

Gomez, Peter (2002):

Komplexe IT-Projekte ganzheitlich führen, Verlag Paul Haupt

Gössinger, Ralf (2005) :

Dienstleistungen als Problemlösungen, Dt. Univ.-Verlag

Grawe, Tonio (2005a):

„Produktisierung“ prägt den Markt für IT-Services, in: IT Management Ausg.9 S.21-26, IT Verlag

Grawe, Tonio (2005b):

Liberale Modelle für strategische Partnerschaften, in IT Management Ausg.10 S.4, IT Verlag

Grawe, Tonio (2006):

Sicher ist besser, in IT Management Ausg.2 S.12-16, IT Verlag

Grawe, Tonio (2007):

IT wie ein eigenständiges Unternehmen führen, in IT Management Ausg.1/2 S.38-44, IT Verlag

Grimm, Sebastian (2005):

Schnittstelle zwischen Anwendern und Unternehmen, in IT Management Ausg.11 S.16-22, IT Verlag

Grünenfelder, Reto (2006):

IT Risk Management im Netzwerk, in IT Security Ausg. 7/8 S.16-19, IT Verlag

Güth, Werner/Peleg, Bezalel (1997)

When will the fittest survive?, Universität Berlin

Hackett, Christopher (2006):

Datenintegration fast auf Knopfdruck, in: IT Fokus Ausg. 3/4 S.22-25, IT Verlag

Hahn, Dietger (2006):

Strategische Unternehmungsplanung - strategische Unternehmungsführung, Springer

Hanke, Thomas (2006):

Controlling wissensintensiver Strukturen und Prozesse, Lohmar

Harbick, Dierk (2005):

Turnaround-Management in Projekten, in: IT Management Ausg.4 S.45-49, IT Verlag

Hasenkamp, Ulrich (2003):

Ausrichtung der betrieblichen IT in Abhängigkeit von E-Business Strategien, in Mülder, Wilhelm: Informationsmanagement, Eul Verlag

Haug, Andreas (2005):

Flexibles Neben- und Miteinander, in: IT Fokus Ausg.3/4 S.46-51, IT Verlag

Heimann, Holger (2006):

Das Rahmenwerk zum Erfolg, in: IT Security Ausg.7/8 S.20-23, IT Verlag

Heinevetter, Thomas/Schrecklinger, Nicole/Scherf, Alexander (2006):

Adapt or Die, in: IT Management Ausg.6 S.36-41 IT Verlag

Heinrich, Torsten (2006):

Chancen und Hürden in der Umsetzungspraxis, in: IT Management Ausg.8 S.38-43, IT Verlag

Heisel, Frank (2005):

Absicherung der Geschäftsführung durch Zertifizierung der IT, in: Revision Ausg. IV S.16-21, Ottokar Schreiber Verlag

Helden von, Josef (2006):

IT-Security Zukunftsszenario, IT-Sicherheit verteilt, integriert, kooperativ und offen, in: IT-Security Ausg.2 S.26-29, IT Verlag

Henkel, Sven/Schick, Andreas (2004):

Steuerungsinstrumente für die IT-Weiterentwicklung, in: IT Management Ausg.10 S.30-35, IT Verlag

Henze, Detlev/Parthier, Ulrich (2005):

Gratwanderung zwischen Zeit, Kosten und Qualität, in. IT Security Ausg.4 S.16-18, IT Verlag

Hermanns, Arnold (2001):

Management-Handbuch electronic commerce, Vahlen

Herweg, Ralf (2001):

Kosten und Nutzen von IT-Sicherheitsmaßnahmen, in: IT-Sicherheit Ausg.1, Datakontext

Hess, Andreas (2004):

Sie sind es uns wert !, in: IT Management Ausg.8 S.52-57, IT Verlag

Hinterhuber, Hans H. (2004a):

Strategische Unternehmungsführung - Strategisches Handeln, de Gruyter

Hinterhuber, Hans H. (2004b):

Strategische Unternehmungsführung - Strategisches Denken, de Gruyter

Hirch, Axel/Rahmel, Jürgen (2005):

Einführung einer IT-Risikosteuerung, in: ReVision Ausg.III S.5-13, Ottokar Schreiber Verlag

Hofmann, Ralf (2003) :

Aufbau, Transfer und Nutzung von Wissen und dessen Anwendung im Bereich der IT-Unternehmensberatung, Dissertation Uni Essen

Hölscher, Reinhold (2002):

Herausforderung Risikomanagement, Gabler

Holznagel, Bernd (2003):

Recht der IT-Sicherheit, C.H.Beck

Hommel, Ulrich (2001):

Realoptionen in der Unternehmenspraxis, Springer

Horster, Patrick (2002a):

Enterprise Security, IT Verlag

Horster, Patrick (2002b):

Sichere Geschäftsprozesse, IT Verlag

Horváth, Péter (2006):

Controlling, Vahlen

Humpert, Frederik (2005):

IT-Grundschutz umsetzen mit GSTOOL, Hanser

Ibers, Tobias (2005) :

Risikomanagement, Merkur-Verlag.

IDS Scheer AG (2005):

ARIS Plattform Produktbroschüre, online verfügbar unter:

www.ids-scheer.com/sixcms/media.php/2152/PR0905-D-BR.pdf (24.10.05)

IDW (1998):

PS 880 – Erteilung und Verwendung von Softwarebescheinigungen, in: Die Wirtschaftsprüfung, 51.Jg. S.1066-1071

IDW (2000a):

S1 Grundsätze zur Durchführung von Unternehmensbewertungen, in: Die Wirtschaftsprüfung, 53. Jg, S.825-842

IDW (2000b):

PS 230 - Kenntnis über die Geschäftstätigkeit sowie das wirtschaftliche und rechtliche Umfeld des zu prüfenden Unternehmens im Rahmen der Abschlussprüfung, in: Die Wirtschaftsprüfung, 53.Jg, S.842-846

IDW (2001):

PS 260 – Das interne Kontrollsystem im Rahmen der Abschlussprüfung, in: Die Wirtschaftsprüfung, 54.Jg., S.821-831

IDW (2002a):

RS FAIT 1 – Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie, in: Die Wirtschaftsprüfung, 55.Jg., S.1157-1167

IDW (2002b):

PS 330 – Abschlussprüfung bei Einsatz von Informationstechnologie, in: Die Wirtschaftsprüfung, 55.Jg., S.1167-1179

IDW (2002c):

Internationale Arbeit – International Federation of Accountants, in: IDW Fachnachrichten, Heft 5 S.326.

IDW (2002d):

PS 321 – Interne Revision und Abschlussprüfung, in: Die Wirtschaftsprüfung, 55.Jg. S.686-689

IDW (2003):

RS FAIT 2 – Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce, in: Die Wirtschaftsprüfung, 56.Jg. S.1258-1275

IDW (2004):

RS HFA 11 Bilanzierung von Software beim Anwender, in: Die Wirtschaftsprüfung, 57.Jg, S.817-820

IIR (2001):

Revisionsstandard Nr.1 – Zusammenarbeit von Interner Revision und Abschluss-prüfer, in: ZIR Heft 1 S.34-36

IIR (2002):

IT-Revision: - Leitfaden zur Durchführung von Prüfungen der Informationsver-arbeitung, Erich Schmidt Verlag

ILTIS GmbH (2005):

IT-Sicherheit, online verfügbar unter:

www.4managers.de/10-Inhalte/asp/it-sicherheit.asp (2.9.05)

Initiative D21 e.V. (2002):

IT-Sicherheitskriterien im Vergleich, online verfügbar unter:

www.initiatived21.de/druck/news/publikationen2002/doc/22_1053502380.pdf

(30.10.05)

Jahn, Elke (2004).

Dynamische Services sind Trumpf, in: IT Management Ausg.8 S.14-18, IT Verlag

Jansen, Dietmar (2006):

Das Richtige programmieren, in IT Management Ausg.2 S.32-35 IT Verlag

Japp, Klaus Peter (2000):

Risiko, Transcript-Verlag

Jekel, Nicole (2006):

IT-Effizienz: Kontrolle und Messung mit der Balanced Scorcard, in: PRev Ausg.IV S.24-29, Ottokar Schreiber Verlag

JNet Quality Consulting (2007):

Automatisiertes Business Process Discovery, in: IT Fokus Ausg.3/4, S.36-39, IT Ver lag

Kamlah, Bernd (2004a):

IT-Sicherheit und Notfallplanung, in: ReVision, Ausgabe I, S 9-20, Ottokar Schreiber Verlag

Kamlah, Bernd (2004b):

IT-Sicherheitsmanagement: Outsourcing der Aufgaben eines IT-Sicherheitsbeauftragten, in: ReVision, Ausgabe II, S 11-13, Ottokar Schreiber Verlag

Kamlah, Bernd (2004c):

Prüfung des internen Kontrollsystems in der Praxis,, in: ReVision, Ausgabe IV, S 34-38, Ottokar Schreiber Verlag

Kamlah, Bernd (2005):

IT-Sicherheit: Voraussetzung für die Ordnungsmäßigkeit der Rechnungslegung und den Datenschutz im Unternehmen, in: ReVision Ausg.I S.21-26, Ottokar Schreiber Verlag

Kappelhoff, Peter (2002):

Komplexitätstheorie: Neues Paradigma für die Managementforschung ? in: Schreyögg, Georg: Theorien des Managements, Gabler

Kappeller, Wolfgang (2003) :

Management-Konzepte von A - Z , Gabler

Karpinsky, Jörg (2007):

Sicherheit in virtuellen Umgebungen, in: IT Security Ausg.1 S.22-24, IT Verlag

Kearney, A..T. (2005):

IT-Manager müssen umdenken, in: IT Management Ausg.6 S.6-7, IT Verlag

Keuper, Frank (2003):

E-Business, M-Business und T-Business, Gabler

Keuper, Frank (2005):

Integriertes Risiko- und Ertragsmanagement, Gabler

Kemper, Hans-Georg (2006)

Business Intelligence - Grundlagen und praktische Anwendungen, Vieweg

Kimmig, Jens M. (2001):

Risiko-Controlling in der Unternehmung, Dt. Univ.-Verlsg

Knupfer, Jörg (2005):

Rechtliche Grundlagen der IT-Sicherheit, in: Schoolmann Jürgen / Rieger Holger: Praxishandbuch IT-Sicherheit, S.37-52, Symposium Publishing

Kirchner, Michael (2002):

Risikomanagement, Hampp

Kirchhoff, Tobias (2005):

Kennzahlen für die Sicherheit, in: IT Security Ausg.3 S.26-29, IT Verlag

Klaftenegger, Peter (2004):

In sicheren Händen, in: IT Fokus Ausg.9/10 S.64-66, IT Verlag

Klapdor, Martin (2005):

IT-Risiken im virtuellen Netzwerk prüfen, in: IT Security Ausg.3 S.30-34, IT Verlag

Klement, Peter (2006):

Business-Alignment durch Agilität, in: IT Management Ausg.5 S.56-60, IT Verlag

Klindtworth, Holger (2003):

Outsourcing der IT: Chancen und Risiken aus Sicht der Revision, in: Revision Ausg.IV S.40-45, Ottokar Schreiber Verlag

Klindtworth, Holger (2005):

Risikomonitoring mit Unternehmensdaten, in: Revision Ausg.IV S.5-8, Ottokar Schreiber Verlag

Kob, Timo (2005):

Messbare Qualität mit SSE-CMM, in: IT Security Ausg.2 S.54-58, IT Verlag

Kob, Timo/Schumann, Detlef (2005):

Prozesse, Prozesse, Prozesse, in: IT Security Ausg. 6, S.30-35 IT Verlag

Kromschröder, Bernhard/Lück, Wolfgang (1998):

Grundsätze risikoorientierter Unternehmensüberwachung , in: Der Betrieb Heft 32: S. 1573-1576

Krcmar, Helmut/Junginger, Markus (2003):

Risikomanagement im Informationsmanagement, in: Mülder, Wilhelm: Informations-management, Eul Verlag

Kremin-Buch, Beate/Unger, Fritz/Walz, Hartmut (2004):

Wissen, Wissenschaft & Praxis

Krüger, Torsten/Graf, Richard (2005).

Von den Kosten bis zur Wertschöpfung, in: IT Management Ausg. 12, S.38-43

Krupp, Thomas (2006):

Größere Flexibilität durch On-Demand-Modelle, in: IT Management Ausg.10, S.20-22, IT Verlag

Kruth, Wilhelm (2004):

Mission RoSI, in: ReVision, Ausg.III S.5-12, Ottokar Schreiber Verlag

Kullmann, Peter (2005):

Kosten und Nutzen von Notfallkonzepten, in: IT Fokus Ausg.7(8 S.47-50, IT Verlag

Kullmann, Peter (2006):

Bewertung von Wiederherstellungslösungen, in: IT Security Ausg.1 S.24-28, IT Verlag

Kuppinger, Martin (2005a):

Identity Management, in: IT Security Ausg.3/4 S.2-4, IT Verlag

Kuppinger, Martin (2005b):

Reife Anwendungen für reife Unternehmen, in: IT Management Ausg.12 S.12-18, IT Verlag

Kuppinger, Martin (2006):

SOA benötigt einen festen Grund, in: IT Fokus Ausg.3/4 S.10-12, IT Verlag

Kütz, Martin (2005) :

IT-Controlling für die Praxis, dpunkt-Verlag

Küpper, Hans-Ulrich (2005).

Controlling, Schäffer-Poeschel

Kyas, Othmar (2000)

IT crackdown, mitp

Lautenbach, Annette (2005):

Von der Störungsmeldung zum Kosten-Controlling, in: IT Management Ausg.7/8 S.32-37, IT Verlag

Leitch, Robert A. (1992)

Accounting information systems, Prentice-Hal

Lentfer, Thies (2003):

Risikomanagementsystem: Die Aufbauorganisationn und das Interne Überwachungs-system, in: Revision Ausg.IV S.11-16, Ottokar Schreiber Verlag

Lenzen, Manuela (2003):

Evolutionstheorien in den Natur- und Sozialwissenschaften, Campus-Verlag

Löbel, Jürgen (2005):

Nachhaltige Managementsysteme, Erich Schmidt Verlag

Lück, Wolfgang (2000):

Die Zukunft der internen Revision, Erich Schmidt Verlag

Ludwig, Bernd (2004):

Neue Mode oder neuer Standard ?, in: IT Management Ausg.12 S.44-45, IT Verlag

Lüke, Detlef (2005):

Device-Security trifft Systemmanagement, in: IT Fokus Ausg.1/2 S.32-35, IT Verlag

Lutz, Harald (2005):

Dynamik pur, in: IT Management Ausg.7/8 S.60-62, IT Verlag

Mallow, Birgit (2005):

Mit einer Stimme sprechen, in: IT Management Ausg.7/8 S.48-52, IT Verlag

Marten, Kai-Uwe/Köhler, Annette G. (2001):

Entwicklung und gegenwärtiger Stand der Assurance Services in den USA, in: Die Wirtschaftsprüfung, 54. Jg., S. 435-440

Marten, Kai-Uwe/Quick, Reine/Ruhnke, Klaus (2006):

Lexikon der Wirtschaftsprüfung, Schäffer-Poeschel

Martin, Thomas A. (2002):

Grundzüge des Risikomanagements nach KonTraG, Oldenbourg

Martin, Wolfgang (2004):

Business Intelligence trifft Business Integration, in: IT Management Ausg.11 S.10-20, IT Verlag

Mayer, Barbara (2003):

ROSI: Return on Security Investment – eine notwendige Rechnung, in IT-Management Ausg.1, S.26-31, IT Verlag

Mayer, Volker (2003):

Operatives Krisenmanagement, DUV, Gbgler

Meisel, Alexander (2005):

Web Application Security – Teil 1 Die Grundproblematik, in: IT Security Ausg. 6 S.26-29, IT Verlag

Meisel, Alexander (2006):

Web Application Security – Teil 2 Authentifizierung und Session-Handling, in: IT Security Ausg. 1 S.16-19, IT Verlag

Melz, Carsten (2005).

Unterstützung für Projektabläufe, in: IT Management Ausg.6 S.20-25, IT Verlag

Menzies, Christof (2004):

Sarbanes-Oxley-Act, Schäffer-Poeschel

Merbecks, Andreas (2004)

Intelligentes Risikomanagement, Redline Wirtschaft

Meyer, Ulf (2004):

E-Business und Wirtschaftsprüfung, Eul

Mieschke, Lutz (2003):

Strategisches Geschäftsmodell der Informationstechnologieberatung, Dissertation Uni Essen

Mischur, Oliver/Bostelmann, Uwe (2005):

Alle Technik nutzt im Notfall nichts, in: IT Fokus Ausg.7/8 S.43-46, IT Verlag

Miscbur, Oliver (2006):

Business Continuity Management, Das Plus zur Technik, in: IT Security Ausg.2 S.30-33, IT-Veröag

Möller, Thorsten (2007): Risikobewertung in der EDV, in PRev Ausg.I S.32-38, Ottokar Schreiber Verlag

Mühlenbrock, Frank (2003):

IT-Sicherheit – Effektive Richtlinien und Standards im Unternehmens-Netzwerk, SmartBooks

Müller, Klaus-Rainer (2003)

IT-Sicherheit mit System, Vieweg

Nandico, Oliver F. (2004):

Von Monolithen zu lose gekoppelten Sevices, in: IT Fokus Ausg.9/10 S.40-44, IT Verlag

Nedon, Jens (2003):

IT incident management & IT forensics, Gesellschaft für Informatik / Fachgruppe Erkennung und Beherrschung von Vorfällen der Informationssicherheit

Neeb-Bruckner, Barbara (2007):

CMMI und agile Methoden – Widerspruch oder sinnvolle Ergänzung, in: IT Fokus Ausg.1/2 S.13, IT Verlag

Niemann, Rainer (2001) :

Neutrale Steuersysteme unter Unsicherheit, Erich Schmidt Verlag

Nolte, Bernd (2003):

Basel II konkret, Wiley

Nußdorfer, Richard/Martin, Wolfgang (2005a):

Echtzeit-Regelschleifen, in: IT Fokus Ausg.5/6 S.10-16, IT Verlag

Nußdorfer, Richard/Martin, Wolfgang (2005b):

Evolutionsprozess, in: IT Management Ausg.7(8 S.12-19, IT Verlag

O.Nigisch (1998):

Was ist Sozialkompetenz?, Uni Linz, online verfügbar unter: www.stangl-taller.at/4711/SIEB.10/SATIRE/SOZIALEKOMPETENZ/Nigsch98.html (7.1.2006)

Parthier, Ulrich (2005a):

Schadensfälle antizipieren, in: IT Management Ausg.1/2 S.14-17, IT Verlag

Parthier, Ulrich (2005b):

Sesam öffne dich, Chief Security Officerr, in: IT Security Ausg.5 S.40-42, IT Verlag

Parthier, Ulrich/Lamm, Andreas (2006):

Das Internet bietet Chancen: Die Kehrseite sind die Risiken, in: IT Security Ausg. 2 S.16,17, IT Verlag

Pausch, Karl (2005):

IT-Goverance auch für KMUs, in: IT Management Ausg.6 S.50-55, IT Verlag

PC-Welt (2004),

tecCHANNEL-Ccompact Sicherheit für Netzwerk & Server, IDG Interactive

Peemöller, Volker H. (2005) :

Controlling, Verl. Neue Wirtschafts-Briefe

Peemöller, Volker H. (2006):

Sarbanes Oxley Act und Interne Revision, in: Interne Revision Jahrbuch 2007 S.113-130, Ottokar Schreiber Verlag

Peisl, Roland (2006):

BPM & SOA: Ein perfektes Paar, in: IT Fokus Ausg.11/12 S.13-17, IT Verlag

Pepels, Werner (2005) :

Servicemanagement, Merkur-Verlag

Perdich, Peter (2004):

Organisation & Technik im Einklang, in: IT Fokus Ausg.11/12 S.60-63, IT Verlag

Perner, Petra (2004):

Advances in data mining, Springer

Pietsch, Thomas (2003):

Bewertung von Informations- und Kommunikationssystemen, Erich Schmidt Verlag

Pietsch, Thomas (2004)

Strategisches Informationsmanagement, Erich Schmidt Verlag

Piser, Marc (2004)

Strategisches Performance Management, Dt. Univ.-Verl.

Pobbig, Heiko (2005):

Von der Kosten- zur Wertorientierung, in: IT Management Ausg.7/8 S.42-46, IT Verlag

Poels, Torsten (2004a):

Mit Sicherheit unsicher, in: IT Qualifikation Ausg.7/8 S.9-10, IT Verlag

Poels, Torsten (2004b):

IP-Lauschangriff, in: IT Qualifikation Ausg.11/12 S.6, IT Verlag

Poels, Torsten (2005):

Aufwand contra Sicherheit, in: IT Security Ausg.3 S.22-25, IT Verlag

PwC Deutsche Revision Aktiengesellschaft – WPG (2000):

Unternehmensweites Risikomanagement

Redenius, Jens O. (2004):

Die Wirtschaftlichkeit von IP-Konvergenz, in: IT Management Ausg.8 S.10-13, IT Verlag

Redenius, Jens O. (2005):

Im Mittelpunkt steht die Wirtschaftlichkeit, in: IT Management Ausg.3 S.52-57, IT Verlag

Reichling, Peter (2003):

Risikomanagement und Rating, Gabler

Reichmann, Thomas (1993):

DV-gestütztes Unternehmens-Controlling, Vahlen

Reichmann, Thomas/Form, Stephan (2000):

Balanced Chance- and Risk-Management, in: Controlling Heft 4/5, Vahlen

Reichmann, Thomas (2006) :

Controlling mit Kennzahlen und Management-Tools, Vahlen

Rentschler, Peter (2005a):

Kontrolle ist besser, in: IT Management Ausg.1/2 S.22-26, IT Verlag

Rentschler, Peter (2005b):

IT-Goverance mit Cobit, in: IT Management Ausg.4 S.28-32, IT Verlag

Rentschler, Peter (2005c):

Risikomanagement auf normierter Basis, in: IT Management Ausg.6 S.38-43, IT Verlag

Rieger, Holger (2005a):

IT-Sicherheit – Risiken und Gefährdungspotenziale, in: Schoolmann Jürgen / Rieger Holger : Praxishandbuch IT-Sicherheit, S.19-36, Symposium Publishing

Rieger, Holger (2005b):

IT-Sicherheit als Kernelement der Unternehmenssicherheit, in: Schoolmann Jürgen / Rieger Holger : Praxishandbuch IT-Sicherheit, S.53-79, Symposium Publishing

Rieger, Holger/Schoolmann Jürgen (2005):

Wege zu mehr IT-Sicherheit, in: Schoolmann Jürgen / Rieger Holger : Praxishandbuch IT-Sicherheit, S.435-442, Symposium Publishing

Ritter, Michael (2000):

Kapitalkostenermittlung im Shareholder-Value-Konzept mit Hilfe optionspreis-theoretischer Ansätze, Josef Eul Verlag

Romeike, Frank (2003):

Integration von IT-Risiken in das proaktive Risk Management, DuD Heft 4 S.193 ff.

Romeike, Frank (2004):

Erfolgsfaktor Risiko-Management, Gabler

Romeike, Frank (2005):

Modernes Risikomanagement, Wiley-VCH

Rosenkranz, Friedrich (2006) :

Geschäftsprozesse, Springer

Rossa, Gerd (2006):

Automatismen verhindern Fehlentwicklungen, in: IT Fokus Ausg. 5/6 S.30-33, IT Verlag

Rother, Tobias (2006).

IT doesn’t matter, in: IT Management Ausg.6 S.48-53, IT Verlag

Rubenschuh, Marcus (2003):

Measuriing Security and Conformity, Ernst & Young

Rudholzer, Gerhard (2005):

Ein Web-basiertes Informationssicherheitsmanagementsystem : Diplomarbeit am FB Informatik FH Landshut

Rudolph, Heiko (2006):

IT-Sicherheitsinfrastrukturen, in: IT Fokus, Ausg.11/12 S.44-47, IT Verlag

Rumsauer, Klaus (2007):

Auf dem Weg zum Next Generation Data Center, in: IT Fokus Ausg.3/4 S.48-50, IT Verlag

Sabathil, Kurt (1993)

Evolutionäre Strategien der Unternehmensführung, Dt. Univ.-Verlag

Santifaller, Michael (2005):

Feste Beziehung gesucht, in: IT Fokus Ausg.1/2 S.36-40, IT Verlag

Schäfer, Gernot (2006):

Lästige Notwendigkeit oder Chance ?, in: IT Management Ausg.5 S.42-47, IT Verlag

Schärtel, Markus/Peitzker, Stefanie (2006);:

Flexible Architektur für agile Geschäftsprozesse, in: IT Management Ausg.4 S.44-49, IT Verlag

Scheer, August-Wilhelm (2004):

Innovation durch Geschäftsprozessmanagement, Springer

Scheer, August-Wilhelm (2005):

Corporate Performance Management, Springer

Schmitz, Ulrich (2004):

Mit Sicherheit Karriere machen, in: IT Qualifikation Ausg.9/10 S.11-12, IT Verlag

Schmitz, Ulrich (2007):

Sicherheitsleitfaden für das SAP NetWeaver Portal, in: IT Security Ausg.3 S.41, IT Verlag

Schneider, Oliver/Giefer, Katrin (2006):

Schnell und sicher aus der Krise, in: IT Management Ausg.3 S.46-49, IT Verlag

Schreiber, Ottokar (2006):

Notwendigkeit der Internen Revision, in: PRev Ausg.II S.5-7, Ottokar Schreier Verlag

Schreyögg, Georg (2002):

Theorien des Managements, Gabler

Schröder, Christian (2007):

Merkmale effizienter EAI-Lösungen in einer SOA-Landschaft, in: IT Fokus Ausg.1/2 S.28, IT Verlag

Schroff, Joachim (2006):

Risikomanagement nach COSO und Interne Revision, in: Interne Revision Jahrbuch 2007 S.5-46, Ottokar Schreiber Verlag

Schneier, Bruce (2000):

Secrets & Lies, dpunkt Verlag

Schreiber, Ottokar R. (2003):

Interne Revision - Aufgabe und Notwendigkeit, in: Revision Ausg.IV S.5-10, Ottokar Schreiber Verlag

Schröder, Georg F. (2006).

IT-Security - rechtssichere Umsetzung im Unternehmen, Interest Verlag

Schwarze, Lars (2006):

Wichtigste Eckpfeiler einer erfolgreichen IT-Strategie, in: IT Management Ausg.10 S.32-36, IT Verlag

Sehlhorst, Michael (2004):

Managed Security Services, in: IT Management Aug.10 S.73-75, IT Verlag

Seidenschwarz, Werner/Huber, Christian (2002):

Management von Strategien, in: Gleich, Ronald /Becker, Ralph/Horváth, Péter: Controlling Fortschritte, S. 121-148, Vahlen

Seidenschwarz, Werner (2003):

Steuerung unternehmerischen Wandels, Vahlen

Seidel, Uwe M. (2002):

Risikomanagement, Weka Media

Seidl, Matthias (2006):

Wegweiser für das IT-Management, in: IT Management Ausg.1 S.26-30, IT Verlag

Sommer, Jochen (2004):

IT-Servicemanagement mit ITIL und MOF, mitp-Verlag

Sonntag, Matthias (2005):

IT-Sicherheit kritischer Infrastrukturen, C.H.Beck

Stahl, Christoph (2005):

Transparenz und Revisionssicherheit in den Prozessen, in. IT Management Ausg.5 S.12-15, IT Verlag

Stahlknecht, Peter (2003):

Informationsmanagement zwischen Paradigmen, Paradoxien, Phrasen und Prognosen, in Mülder, Wilhelm: Informationsmanagement, Eul Verlag

Stöger, Roman (2005):

Geschäftsprozesse erarbeiten - gestalten – nutzen, Schäffer-Poeschel

Stoi, Roman (2002):

New Economy Controlling, in: Horváth, Péter: Controllingfortschritte, Vahlen

Stoi, Roman (2003):

Controlling von Intagibles, in: Controlling Heft 3/4, S.175-183, Vahlen

Streiblich, Karl-Heinz/Parthier, Ulrich (2005):

SOA Mehr als ein Schlagwort, in: IT Management Ausg.6 S.14-15, IT Verlag

Strobel, Stefan (2003) :

Firewalls und IT-Sicherheit, dpunkt-Verlag

Strobel, Stefan (2005):

Angriffsszenarien simulieren, in: IT Security Ausg.5 S.58-61, IT Verlag

Tiemeyer, Ernst (2005) :

IT-Controlling kompakt, Spektrum Akad. Verl.

Töpfer, Armin (2003):

Forum Unternehmer und Wissenschaft <14, 2002, Dresden> : Risikomanagement, WGMU

Trossmann, Ernst/Baumeister, AlexanderWerkmeister, Clemens (2003):

Management-Fallstudien im Controlling, Vahlen

Tscherwitschke, Hans (2007):

Wer rastet, der rostet, in: IT Management Ausg.1/2 S.19-22, IT Verlag

UIMCert PS 102 (2007):

Standard für die Prüfung der Datenschutzordnungsmäßigkeit von Produkten/Systemen für die Verarbeitung von personenbezogenen Daten, UIMCert

Voß, Antje (2003).

Security – Das Grundlagenbuch, Franzis

Vossbein, Reinhard (2004a):

Höhere IT-Sicherheit durch Auditierung gemäß BS7799 / ISO/IEC 17799-1, in ReVision Ausg.II S.5-10, Ottokar Schreiber Verlag

Vossbein, Reinhard (2004b):

Risikomanagement in der IT-Siccherheit – eine Revisionsaufgabe, in ReVision Ausg.IV S.25-30, Ottokar Schreiber Verlag

Vossbein, Reinhard (2005a):

ITIL/BS 15000 – eine neue Norm und ihre Bedeutung für die Arbeit der IR, in ReVision Ausg.II S.5-11, Ottokar Schreiber Verlag

Vossbein, Reinhard (2005b):

Revision der IT-Notfall und Business Continuity Planung, in ReVision Ausg.III S.19-25, Ottokar Schreiber Verlag

Vossbein, Reinhard/Collenberg, Thomas (2007):

Externe Revision – Interne Revision: Partner bei der Erhöhung der IT-Sicherheit, in PRev Ausg.I S.39-43, Ottokar Schreiber Verlag

Wagner, Siegfried (2005):

Neue Sicht auf alte Daten, in: IT Fokus Ausg. 9/10 S.38-42, IT Verlag

Wähner Gerd W. (2002):

DV-Revision - Handbuch für die Unternehmenspraxis, Kiehl

Wall, Friederike (2003):

Kompatibilität des betriebswirtschaftlichen Risikomanagement mit den gesetzlichen Anforderungen ?, in: Die Wirtschaftsprüfung 56.Jg. S 457-471

Wallmüller, Ernest (2004):

Risikomanagement für IT- und Software-Projekte, Hanser

Warncke, Markus (2006):

Corporate Governance und Interne Revision, in: Interne Revision Jahrbuch 2007 S.47-64, Ottokar Schreiber Verlag

Weber, Jürgen (2006):

Controlling von Intangibles, WILEY-VCH

Weigelt, Lutz (2005):

Das magische Dreieck, in: IT Qualifikation Ausg.1/2 S.14, IT Verlag

Weick, Karl E. (2003):

Das Unerwartete managen, Klett-Cotta

Weiß, Steffen (2005):

Sicherheit dokumentieren, in: IT Security Ausg.3 S.60-63, IT Verlag

Wieczorek, Martin (2003):

Business continuity, Springer

Wikimedia Foundation (2005):

Die freie Enzyklopädie: Realoption, online verfügbar unter:

de.wikipedia.org/wiki/Realoption (17.9.2005)

Wolf, Klaus (2003a):

Risikomanagement und KonTraG,, Gabler

Wolf, Klaus (2003b):

Risikomanagement im Kontext der wertorientierten Unternehmensführung, Dt. Univ.-Verl.

Wulff, Joachim (2006):

Aus dem Vollen schöpfen, in: IT Fokus Ausg.7/8 S.12-17, IT Verlag

Woywode, Michael (1998)

Determinanten der Überlebenswahrscheinlichkeit von Unternehmen, Nomos Verlag

Zarnekow, Rüdiger (2005):

Integriertes Informationsmanagement, Springer

Zarnekow, Rüdiger (2006):

Präzise modellierte IT-Services, in: IT Fokus Ausg.5/6 S.10-15, IT Verlag

Zimmermann, Christian (2005):

Die Zukunft fest im Blick, in: IT Management Ausg.6 S.10-12, IT Verlag