Lernen vom Business Engineering - Ansätze für ein systematisches, modellgestütztes Vorgehensmodell zum Sicherheitsmanagement

Sabrina Sitzberger, Thomas Nowey
Lehrstuhl Management der Informationssicherheit,
Universität Regensburg, D-93040 Regensburg
sabrina.sitzberger@web.de, thomas.nowey@wiwi.uni-regensburg.de

Abstract: Das vorliegende Papier zeigt, wie Erkenntnisse des Business Engineering als Grundlage für ein umfassendes Vorgehensmodell zum IT-Sicherheitsmangement in Organisationen dienen können. Zunächst wird die Notwendigkeit eines systematischen Vorgehens im IT-Sicherheitsmanagement erläutert. Anschließend werden kurz bestehende Vorgehensweisen diskutiert. Ein Vergleich von Business Engineering und Sicherheitsmanagement zeigt Parallelen zwischen den Bereichen auf und bildet die Basis für die weitere Untersuchung. Ausgehend von diesen Parallelen wird in Analogie zu Methoden des Business Engineering ein Ansatz für ein systematisches Vorgehensmodell für das IT-Sicherheitsmanagement entworfen. Es werden Empfehlungen für dessen Anwendung gegeben und Ansätze für weitere Forschungsarbeiten geliefert.

1 Einleitung

Der Unternehmenserfolg wird in Zukunft entscheidend von einem umfassenden IT-Sicherheitsmanagement abhängen. Dies zeigen beispielsweise die aktuellen Bestimmungen zu Basel II (vgl. [GK03], [JR02]). Auch wird das Beherrschen der IT-Sicherheit selbst von Autoren, die in Informationstechnologie nur eine weitere Form von Infrastruktur sehen, als kritischer Erfolgsfaktor bewertet (vgl. [Car03]). Die Notwendigkeit eines strukturierten und systematischen Vorgehens in dieser Managementdiszplin wird damit offensichtlich. Es gibt zahlreiche Ansätze, die ein Vorgehen für einzelne Bereiche und Aspekte des IT-Sicherheitsmanagements darstellen, doch existiert nach Einschätzung der Autoren noch keine allgemein akzeptierte, detaillierte und weit reichende Methodik im Sinne eines Vorgehensmodells, auch wenn bereits verschiedene Unternehmensberatungen ihre Beratungsansätze als solches deklarieren. Zur Entwicklung eines Vorgehensmodells ist zunächst die Frage zu beantworten, welche Anforderungen an ein solches bestehen.

Ganzheitliche Betrachtung. Dass IT-Sicherheit nicht durch rein technische Maßnahmen allein erreicht werden kann ist inzwischen allgemein akzeptiert. Bei einer isolierten Betrachtung würde nur eine selektive Sicherheit und damit ein relativ niedriges Sicherheitsniveau verwirklicht werden können. So steht die IT-Sicherheit in enger Verbindung zu nahezu allen anderen Unternehmensbereichen. Aufgrund wechselseitiger Beziehungen müssen die IT-Sicherheit und somit auch das IT-Sicherheitsmanagement stets einer ganzheitlichen

Betrachtung unterliegen. Um diesem Ansatz gerecht zu werden, muss ein Vorgehensmodell neben technischen Aspekten auch betriebliche Abläufe sowie organisatorische, personelle und baulich-infrastrukturelle Aspekte einbeziehen. Das bedeutet einerseits, dass sich Sicherheitsmaßnahmen auf diese Bereiche erstrecken müssen, andererseits aber auch, dass Wechselwirkungen zwischen diesen Bereichen und der IT-Sicherheit bei Neu- und Umgestaltungen berücksichtigt werden müssen.

Berücksichtigung unternehmensindividueller Gegebenheiten. Unternehmen unterscheiden sich im Gegenstand ihrer Geschäftstätigkeit, in ihrem Aufbau, in ihrer Organisation und damit auch darin, wie Informationstechnologie im Unternehmen eingesetzt wird und zu welchem Grad das Unternehmen von dieser abhängig ist. Ein Vorgehensmodell muss daher unternehmensindividuelle Aspekte beachten. So sind spezifische Gefährdungen zu berücksichtigen und individuell an das Unternehmen angepasste Sicherheitskonzepte und -maßnhamen zu definieren.

Ökonomische Steuerung und Kontrolle. Geht es um Investitionen im Bereich der IT-Sicherheit, so ist eine ökonomische Betrachtung des Sicherheitsmanagements erforderlich. Einerseits sind die Kosten von Sicherheitsmaßnahmen und der Nutzen, der sich daraus ergibt, gegeneinander abzuwägen, um im Idealfall das Bündel aus Sicherheitsmaßnahmen zu identifizieren, bei dem die Summe aus zu erwartenden Schäden und Kosten der Maßnahmen minimal ist. Andererseits benötigen Unternehmen auch zuverlässige Informationen über die Höhe des verbleibenden Restrisikos aus IT-Sicherheitsvorfällen. Aufgrund der Notwendigkeit solcher Berechnungen sollte ein Vorgehensmodell die ökonomische Steuerung und Kontrolle der IT-Sicherheit unterstützen.

Im Vergleich zum IT-Sicherheitsmanagement verfügt die Managementdisziplin des Business Engineering über mehrere strukturierte und erprobte Methoden und Vorgehensmodelle. Bereits auf den ersten Blick lassen sich gewisse Parallelen zwischen dem Business Engineering und dem Sicherheitsmanagement erkennen. So liegt es nahe, Methoden des Business Engineering hinsichtlich einer Adaption auf den Bereich der IT-Sicherheit zu überprüfen. Im Folgenden wird diese Idee verfolgt und ein Ansatz für ein umfassendes und strukturiertes Vorgehen im Sinne eines Vorgehensmodells für das IT-Sicherheitsmanagement dargestellt. Zunächst werden in Kapitel 2 kurz in Deutschland verbreitete Ansätze für das Sicherheitsmanagement thematisiert. Kapitel 3 untersucht die Parallelen zwischen dem Business Engineering und dem Sicherheitsmanagement. Kapitel 4 stellt einen neuen Ansatz einer systematischen Vorgehensweise im Sicherheitsmanagement vor und zeigt seine Anwendung. Offene Fragen und weitere Schritte werden in Kapitel 5 dargestellt.

2 Verbreitete Vorgehensweisen zum Sicherheitsmanagement

IT-Grundschutzhandbuch (GSHB) des BSI. Das GSHB des BSI (siehe [BfSidIB04]) ist eines der von deutschen Unternehmen am häufigsten genutzten Rahmenwerke für Sicherheitsmanagment. Es empfiehlt Standardsicherheitsmaßnahmen für typische IT-Systeme mit normalem Schutzbedarf. Das praxisorientierte Werk bietet eine Zusammenstellung von Umsetzungshinweisen und Hilfsmitteln für zahlreiche IT-Konfigurationen, wobei ne-

ben technischen Maßnahmen auch auf organisatorische, personelle und infrastrukturelle Maßnahmen eingegangen wird. Dadurch weist das GSHB auch Grundzüge einer ganzheitlichen Betrachtung auf.

Es beschränkt sich jedoch auf die Beschreibung von standardmäßigen Gefährdungen und Sicherheitsmaßnahmen. Durch diesen Best-Practice-Ansatz ist nicht sichergestellt, dass auch alle unternehmensspezifischen Bereiche und Prozesse berücksichtigt werden. Als Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von IT-Sicherheitsmaßnahmen sieht das BSI einen so genannten IT-Sicherheitsprozess vor. Dadurch wird eine Vorgehensweise vorgegeben, welche ausgehend von den vorhandenen IT-Systemen Standardsicherheitsmaßnahmen anbietet. Unternehmens-individuelle Gefährdungen werden nicht berücksichtigt. Im Sinne einer ökonomischen Betrachtung der IT-Sicherheit gibt das GSHB einen Hinweis auf die Notwendigkeit einer Wirtschaftlichkeitsbetrachtung. Ein Vorgehen für ökonomische Steuerung und Kontrolle ist allerdings nicht enthalten.

Internationale Rahmenwerke und Normen. Der internationale Standard ISO/IEC-17799 als "Code of practice for information security management", häufig ergänzt durch BS 7799:2, stellt einen weltweit verbreiteten Leitfaden zum Management von Informationssicherheit dar. Der Standard umfasst verschiedene Managementaufgaben, wobei überwiegend nicht-technische Sicherheitsmaßnahmen definiert werden. Dadurch wird das Vorgehen den Anforderungen eines ganzheitlichen Ansatzes nur teilweise gerecht. Für einen solchen müssten weitere Standards oder Rahmenwerke einbezogen werden. Der Standard stellt eine umfassende Auflistung von generischen Maßnahmen dar, ohne aber auf tiefere Zusammenhänge einzugehen. Dabei ist nicht sichergestellt, dass alle unternehmensspezifischen Gegebenheiten berücksichtigt werden. Eine Anleitung zur Anwendung des Standards im Sinne einer Vorgehensweise wird nicht gegeben. Die Bedeutung des Risiko-Managements wird hervorgehoben, die Anforderungen hinsichtlich ökonomischer Steuerung und Kontrolle können jedoch allein auf Basis dieser Rahmenwerke nicht verwirklicht werden.

Fazit. Bei den vorhandenen nationalen sowie internationalen Rahmenwerken handelt es sich jeweils um Best-Practice Ansätze, welche auf Standardsicherheitsmaßnahmen beruhen. Das GSHB enthält dabei relativ konkrete Maßnahmen, während sich ein solcher Detaillierungsgrad in internationalen Rahmenwerken erst aus dem Zusammenspiel verschiedener Normen ergibt. Eine Methodik zur Durchführung eines umfassenden und systematischen IT-Sicherheitsmanagements im Sinne einer Vorgehensweise findet sich nicht. Dies betrifft einerseits das Vorgehen über die verschiedenen Hierarchieebenen hinweg und andererseits die Verknüpfung der Teilbereiche. So erfüllen existierende Vorgehensweisen im IT-Sicherheitsmanagement den Anspruch einer ganzheitlichen Betrachtung der IT-Sicherheit nur unzureichend. Sie orientieren sich eher an technischen Gegebenheiten als an Geschäftsabläufen. Unternehmensindividuelle Gefährdungen bzw. Sicherheitsmaßnahmen werden nur wenig berücksichtigt. Zudem erfolgt das Sicherheitsmanagement in der Regel losgelöst von anderen Managementbereichen. Ein Vorgehen zur Unterstützung einer ökonomischen Betrachtung bieten vorhandene Vorgehensweisen nur ansatzweise.

Insgesamt beschreiben existierende Vorgehensweisen zwar alle relevanten Unternehmensbereiche und schlagen ein mehrstufiges Vorgehen vor, einzelne Schritte und insbesondere deren Abfolge und Verknüpfung im Sinne einer Methode bzw. eines Vorgehensmodells lassen sich jedoch kaum identifizieren.

3 Parallelen zwischen dem Business Engineering und dem IT-Sicherheitsmanagement

Ziel der Fachdisziplin Business Engineering ist es, ein Unternehmen so zu gestalten, dass es den Anforderungen der Kunden entspricht und sich im Wettbewerb behaupten kann. Zur Erreichung dieses Zieles setzt das Business Engineering Methoden, Techniken sowie Vorgehensmodelle ein. Durch eine Methode wird ein Ablauf in Form von Aktivitäten festgelegt. Die Spezifikation des Ablaufs der Aktivitäten hinsichtlich ihrer Reihenfolge und zulässiger Überlappungen wird als Vorgehensmodell bezeichnet. Techniken stellen Vorschriften zur Erstellung der Ergebnisse dar, wobei diese wiederum durch Werkzeuge unterstützt werden [ÖW03]. Die bekanntesten und am weitesten verbreiteten Methoden des Business Engineering stellen die Architektur integrierter Informationssysteme (ARIS) von A.-W. Scheer (vgl. [Sch91], [Sch01a], [Sch01b]), das Semantische Objektmodell (SOM) von O.K. Ferstl und E. J. Sinz (vgl. [FS90], [FS91]) sowie die Methode Business Engineering (BE) von H. Österle und R. Winter (vgl. [Öst95], [ÖW03]) dar. Alle drei Methoden weisen eine Ebenenstruktur mit unterschiedlich ausgeprägter Strategie-, Prozess- und Systemebene auf. Auf Strategieebene werden die Unternehmensaufgaben festgelegt und strategische Planungen vorgenommen. Zur Konkretisierung dieser strategischen Überlegungen sieht das Business Engineering auf Prozessebene die Gestaltung der Abläufe der Prozesse vor. Auf Systemebene findet eine Analyse und Spezifikation der Anwendungssysteme statt, die die Prozesse der Prozessebene unterstützen.

Übergeordnetes Ziel des Sicherheitsmanagements ist der systematische Schutz des Unternehmens gegen beabsichtigte Angriffe und unbeabsichtigte Ereignisse [Kra03]. Die Ziele sowie Aufgaben des Sicherheitsmanagements lassen sich auf die strategische sowie die operative Ebene aufteilen [HP03], wobei sich die letzere noch in einen konzeptionellen Teil und einen Implementierungsteil unterteilen lässt. Andere Autoren verwenden etwas andere Bezeichnungen oder führen weitere Zwischenstufen ein (vgl. z. B. [Mül05]), die sich jedoch ebenfalls auf drei wesentliche verdichten lassen.

Abbildung 1 gibt einen Überblick über eine mögliche Strukturierung. Zur Erreichung der Ziele werden typischerweise eine Sicherheitspolitik, ein Sicherheitskonzept mit Maßnahmen sowie konkrete Mechanismen zu deren Umsetzung definiert. Dabei werden in der Sicherheitspolitik strategische Ziele, Grundsätze und Richtlinien definiert. Das Sicherheitskonzept stellt eine Übersetzung dieser Politik in Maßnahmen dar, welche auf einer nächsten Stufe durch konkrete Mechanismen detailliert beschrieben werden.

Vergleicht man diese Untergliederung nun mit dem Business Engineering, lässt sich in beiden Teilen eine Unterteilung in drei Ebenen finden. Beide Disziplinen definieren auf einer strategischen Ebene strategische Ziele, Grundsätze und Richtlinien. Eine Konkretisierung dieser strategischen Überlegungen findet auf der Prozessebene statt. Eine detaillierte Beschreibung der Prozessebene findet sich wiederum auf Systemebene, zum einen durch Analyse und Spezifikation der Anwendungssysteme (Business Engineering), zum anderen durch konkrete Mechanismen (IT-Sicherheitsmanagement).

Aufgrund derartiger Parallelen liegt es nahe, die Erkenntnisse des Business Engineering für den Bereich des IT-Sicherheitsmanagements nutzbar zu machen. Es soll daher im Fol-

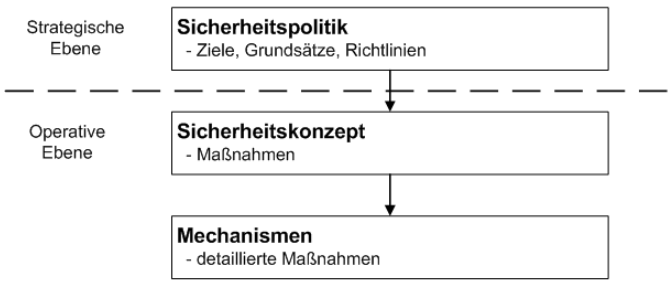

Abbildung 1: Strukturierung des IT-Sicherheitsmanagements

genden versucht werden, etablierte Techniken des Business Engineering auf den Bereich der IT-Sicherheit zu übertragen. Zur Umsetzung einer solchen Vorgehensweise empfiehlt sich eine Orientierung an den Prozessen des Unternehmens. Da Geschäftsprozesse substanziell durch IT-Systeme unterstützt werden, erscheint eine getrennte Betrachtung von Geschäftsprozessen und IT-Systemen heute kaum noch sinnvoll. Zudem bietet ein Vorgehen, welches sich stärker von den Geschäftsprozessen - die ja die Wertschöpfung im Unternehmen abbilden - als von der IT-Infrastruktur leiten lässt, eine bessere Basis für die Analyse und damit für Erweiterung um eine ökonomische Betrachtung (vgl. [RD04]).

Durch die Verbindung von Business Engineering und Sicherheitsmanagement ergeben sich verschiedene Vorteile:

- Bewährte Vorgehensweisen geben ein klares Schema vor und erleichtern die Verknüpfung der verschiedenen Ebenen und Teilbereiche.
- Die erprobten und detaillierten Techniken des Business Engineering, beispielsweise Modellierungstechniken, können für das Sicherheitsmanagement adaptiert werden und so die Konzeption und Implementierung von Sicherheitsmaßnahmen unterstützen.
- Bei der Umsetzung eines prozessorientierten Ansatzes im IT-Sicherheitsmanagement kann auf Ergebnisse des Business Engineering zurückgegriffen werden. Wechselwirkungen zwischen den Bereichen können identifiziert und gesteuert werden. Zwischen zwei bisher getrennten Bereichen werden Austausch und Übergänge ermöglicht.

4 Vorgehensmodell für das IT-Sicherheitsmanagement

4.1 Strategieebene

Ziel des IT-Sicherheitsmanagements auf der strategischen Ebene ist es, das Unternehmen beim Erreichen der unternehmerischen Ziele zu unterstützen und somit den Fortbestand des Unternehmens zu sichern. Zu den wesentlichen Aufgaben der Strategieebene zählen

die *Entwicklung der Sicherheitspolitik* und die *Etablierung einer Sicherheitsideologie und -kultur.*

Die Sicherheitspolitik stellt das zentrale Dokument der Strategieebene dar. Zur Erstellung der Sicherheitspolitik ist zunächst die generelle Bedeutung der IT-Sicherheit für das Unternehmen zu bestimmen. Das angestrebte Gesamtsicherheitsniveau ist zu definieren und zu begründen. Dabei ist das Unternehmen aus verschiedenen Perspektiven im Kontext der IT-Sicherheit zu untersuchen. Hier sind Faktoren wie die IT-Abhängigkeit, das soziales Umfeld, externe Interessenten, die Produkte bzw. Dienstleistungen sowie wirtschaftliche Aspekte zu betrachten. Je nachdem, welche Anforderungen diese Perspektiven an die IT-Sicherheit stellen und wie sehr somit das Unternehmen und insbesondere dessen Aufgaben von der Sicherheit der Informationen und der Informationssysteme abhängen, desto größer ist der Stellenwert der IT-Sicherheit.

Abgeleitet aus den in der Unternehmenspolitik festgelegten Unternehmenszielen werden die Sicherheitsziele formuliert. Für jedes dieser Ziele ist die Fragestellung zu beantworten, inwiefern das jeweilige Schutzziel (Vertraulichkeit, Integrität, Verfügbarkeit etc.) zur Erfüllung des Unternehmensziels beiträgt, bzw. wie groß der Schutzbedarf bzgl. des jeweiligen Schutzzieles ist. Die IT-Sicherheitsziele müssen immer im Zusammenhang mit den entsprechenden Unternehmenszielen gesehen werden. Neben den Sicherheitszielen ist eine IT-Sicherheitsstrategie Teil der Sicherheitspolitik. Diese definiert mittels strategischer Planungen den Soll-Zustand der IT-Sicherheit. Dieser Soll-Zustand ergibt sich aus den Sicherheitszielen und dem gewünschten Gesamtsicherheitsniveau.

In Analogie zum Vorgehen der Methode BE empfehlen sich zur Feststellung des Ist-Zustandes die Verwendung eines geeigneten Fragebogens und die Durchführung von Interviews mit ausgewählten Mitarbeitern, die bisher für IT-Sicherheit zuständig waren. Ebenso wie bei der Definition der Sicherheitsziele, muss die IT-Sicherheitsstrategie in Einklang mit der Unternehmensstrategie stehen und als Teil von dieser gesehen werden. Weiterhin sind in der Sicherheitspolitik Angaben zur periodischen Überprüfung, zur Verpflichtung des Managements sowie zur etablierten Organisationsstruktur der IT-Sicherheit zu machen.

Neben der Entwicklung der IT-Sicherheitspolitik, muss im Unternehmen eine Sicherheitskultur geschaffen werden, welche die Grundsätze und Richtlinien der Sicherheitspolitik verfolgt. Dafür ist es notwendig, dass die IT-Sicherheit als ständiger Prozess des Unternehmens gesehen wird und die Sicherheitspolitik fester Bestandteil der Unternehmenspolitik ist. Damit dies möglich ist, muss sich das Management zur IT-Sicherheit verpflichtet fühlen und diese den Mitarbeitern vorleben. Durch Schulungen zur IT-Sicherheit sollen die Mitarbeiter für die Notwendigkeit der IT-Sicherheit sensibilisiert und motiviert werden. Ziel ist es, dass die Mitarbeiter die sie betreffenden Sicherheitsmaßnahmen als Selbstverständlichkeit ansehen und diese akzeptieren.

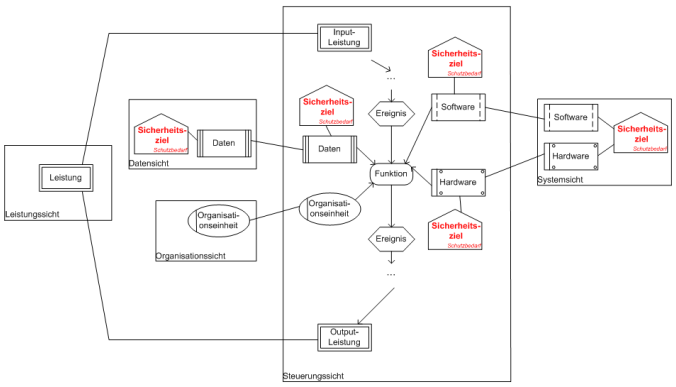

Abbildung 2: Sichten der IT-Sicherheit auf den Geschäftsprozess

4.2 Prozessebene

Ziel der Prozessebene ist es, die Planungen und Ziele der Strategieebene zu konkretisieren und Maßnahmen zu deren Umsetzung zu definieren. Wesentliches Ergebnis dieser Ebene ist das Sicherheitskonzept, welches die konzeptionellen Sicherheitsanforderungen enthält und die daraus resultierenden Maßnahmen systematisch festlegt. Gemäß dem prozessorientierten Ansatz sind zunächst die Geschäftsprozesse des Unternehmens zu identifizieren und in Form von Ereignisgesteuerten Prozessketten (EPKs) zu dokumentieren. Anschließend findet eine Analyse und Modellierung dieser Prozesse bezüglich sicherheitsrelevanter Aspekte statt. Analog dem Business Engineering ist eine Modellierung des Prozesses aus ÏT-Sicherheitssichtßinnvoll. Dazu sind die sicherheitsrelevanten Komponenten des jeweiligen Prozesses zu identifizieren. Zur Reduzierung der Komplexität einer solchen Sicherheitsbetrachtung werden in Anlehnung an die Modellierung in ARIS folgende Sichten modelliert (siehe auch Abbildung 2).

Systemsicht. Die Systemsicht bildet die beteiligten technischen IT-Komponenten ab. Dabei wird auf IT-Systeme (Hardware), IT-Anwendungen (Software), infrastrukturelle Komponenten sowie Datenübertragungs- oder Telekommunikationseinrichtungen eingegangen. Die IT-Komponenten sind hinsichtlich ihres Schutzbedarfes bezüglich der jeweiligen Schutzziele zu analysieren. Bei der Analyse sind die auf Strategieebene durchgeführten Überlegungen zu berücksichtigen. So sind das definierte Gesamtsicherheitsniveau sowie - falls der Prozess oder die Funktion davon betroffen sind - die Sicherheitsziele und die Sicherheitsstrategie in die Analyse zu integrieren. Die identifizierten Schutzziele sind mit ihrem Schutzbedarf zu modellieren und den entsprechenden IT-Komponenten zuzuweisen.

Datensicht. In der Datensicht werden die Daten, welche den Prozess oder die Funktion auslösen, von ihr bearbeitet oder erzeugt werden, abgebildet. Für die Daten ist wiederum der Schutzbedarf bezüglich der Schutzziele zu definieren und zu modellieren. Analog der Systemsicht sind die Überlegungen der Strategieebene einzubeziehen. Für den gesamten Prozess ist es sinnvoll, den Datenfluss des Prozesses in den Netzplan der Systemsicht aufzunehmen. Dadurch wird sichtbar, welche Daten in welcher Reihenfolge mit welcher

IT-Komponente be- bzw. verarbeitet werden. Weiterhin wird dadurch die Ausbreitung der Daten auf die IT-Komponenten sowie die Zusammenhänge und Wechselwirkungen zwischen den Daten ersichtlich.

Organisationssicht. Die Organisationssicht zeigt für jede Funktion die Rollen und Verantwortlichkeiten auf. Bei Identifikation einer Rolle sind der Aufgabenbereich bzw. die Zuständigkeiten der Rolle zu definieren. Ausgehend von diesen Zuständigkeiten ist es in der Risikosteuerung möglich, Berechtigungen zu vergeben. So können ausgehend von dieser Ebene Zugangsberechtigungen zu Bereichen oder Zugriffsberechtigungen auf Daten bestimmt werden.

Leistungssicht. In der Leistungssicht wird der gesamte Prozess ökonomisch bewertet. Dabei werden materielle und immaterielle Input- und Output-Leistungen abgebildet. Diese Sicht dient zur Bewertung des gesamten Prozesses oder einer Funktion des Prozesses.

Steuerungssicht. Die Steuerungssicht fügt die zuvor beschriebenen Sichten zusammen und stellt die Beziehungen zwischen diesen dar. Die wechselseitigen Beziehungen zwischen der System-, Daten-, und Organisationssicht sind dabei zu untersuchen. Die Leistungssicht steht in keiner Beziehung zu den anderen Sichten, sondern wird zur späteren Bewertung der Maßnahmen benötigt. Ausgehend von den Erkenntnissen, die sich aus dem Zusammenwirken der Sichten ergeben, erfolgt im nächsten Schritt die Identifikation möglicher Risiken.

Sind alle Prozesse des Unternehmens modelliert, so sind diese hinsichtlich bestehender Beziehungen und Wechselwirkungen zwischen den einzelnen Prozessen, wie beispielsweise in Form von Datenaustausch, zu untersuchen. Dazu ist ein Prozessmodell zu definieren, welches das Zusammenwirken und die Schnittstellen der einzelnen Prozesse veranschaulicht. Zur Ableitung von konkreten Maßnahmen ist es sinnvoll, einen Netzplan über die IT-Komponenten des Unternehmens zu erstellen. Ausgehend vom Prozessmodell werden nun Risiken identifiziert, analysiert und bewertet. Anschließend findet in der Risikosteuerung die eigentliche Definition der unternehmensindividuellen Sicherheitsmaßnahmen statt. Dies erfolgt unter Angabe des Schutzzieles, des Schutzbedarfs sowie einer ausführlichen Begründung.

4.3 Realisierungsebene

Ausgehend von dem Sicherheitskonzept der Prozessebene bestehen die Aufgaben der Realisierungsebene in der Detaillierung der Maßnahmen und der Überwachung der Umsetzung der Maßnahmen. Die zur Detaillierung der Maßnahmen nötigen Informationen sind in den Beschreibungen der Maßnahmen auf Prozessebene zu finden. Hier sind beispielsweise das verfolgte Schutzziel und der jeweilige Schutzbedarf hinterlegt. Zur Detaillierung sind Angaben wie die genaue Bezeichnung der an der Umsetzung der Maßnahme beteiligten Komponenten (IT-Komponenten, Räume, Daten, Rollen etc.), zeitliche Angaben, sowie Verantwortliche für die Initialisierung und Umsetzung der Maßnahme, nötig. Da auf dieser Ebene eine Konkretisierung der Maßnahmen stattfindet, ist es möglich, dass Wechselwirkungen bekannt werden, welche auf Prozessebene nicht ersichtlich waren. Um die

Maßnahmen dahingehend zu analysieren, sind für die Prozesse detaillierte Maßnahmenmodelle anzufertigen, welche das Zusammenwirken wiedergeben. Ein ähnliches Vorgehen findet sich im Business Engineering bei der Methode BE wieder. Hier werden Applikationsarchitekturmodelle erstellt, welche ebenfalls das Zusammenwirken der Applikationen wiedergeben. Ergebnis der Realisierungsebene ist ein detaillierter Maßnahmenkatalog, welcher die im Sicherheitskonzept definierten Maßnahmen konkretisiert.

Eine weitere Aufgabe der Realisierungsebene ist es, die ordnungsgemäße Umsetzung der Maßnahmen zu überwachen. Hier sind die Richtigkeit der Umsetzung sowie der zeitliche Faktor zu betrachten.

4.4 Anwendung des Vorgehensmodells

Nach Definition der Maßnahmen, sind diese zur Sicherstellung eines widerspruchsfreien und ökonomischen Einsatzes bezüglich ihrer Zielerreichung, möglicher Wechselwirkungen sowie Auswirkungen auf andere Bereiche zu analysieren. Die Maßnahmen sind hinsichtlich ihres Beitrags zur Erreichung der Ziele der Strategieebene zu kontrollieren. Tragen sie nicht im gewünschten Maße zur Zielerreichung bei, so ist ein Rücksprung zur Risikosteuerung notwendig. Ebenso sind die Auswirkungen der Maßnahmen auf die Gesamtsicherheit zu überprüfen und gegebenenfalls anzupassen. Weiterhin sind die Maßnahmen bezüglich ihrer Wechselwirkungen untereinander zu überprüfen und gegebenenfalls einander anzupassen. Wechselwirkungen können aufgrund von Abhängigkeiten zwischen den Schutzzielen, Funktionsüberlappungen oder der zeitlichen Abfolge der Maßnahmen bestehen. Ebenso sind bei der Anwendung des Vorgehensmodells die Auswirkungen der Maßnahmen auf andere Unternehmensbereiche zu überprüfen. Die Maßnahmen sind bezüglich ihrer Beeinflussung der regulären Arbeitsabläufe zu untersuchen. Gegebenenfalls ist die Eingliederung der Maßnahme in den entsprechenden Prozess zu beachten und die EPK dementsprechend zu erweitern.

5 Zusammenfassung und weitere Schritte

In dem vorliegenden Papier wird ein Vorgehensmodell für das IT-Sicherheitsmanagement für Unternehmen aller Größenordnungen und aller Sicherheitsansprüche vorgestellt. Geeignete Methoden und Techniken des Business Engineering werden adaptiert, wodurch eine Vorgehensweise entwickelt wird, die Querbezüge zum Business Engineering herstellt. Der Forderung nach einer ganzheitlichen und umfassenden Betrachtung der IT-Sicherheit wird durch den Ansatz der Prozessorientierung Rechnung getragen. Damit ist allerdings auch das Vorgehensmodell von der Qualität und Lückenlosigkeit der Prozessabbildung abhängig. Diese sollte jedoch aufgrund der Querbezüge zum Business Engineering leichter realisierbar sein, als bei anderen Verfahren. Durch die Analyse von Wechselwirkungen zwischen den Maßnahmen ist die Auswahl eines widerspruchsfreien Maßnahmenbündels möglich. Im Gegensatz zu bereits existierenden Vorgehensweisen ist eine individuelle

Anpassung des Vorgehensmodells an das Unternehmen notwendig. Die Leistungssicht des Vorgehensmodells leistet einen Beitrag zu einer ökonomischen Betrachtung der IT-Sicherheit, welche allerdings noch einer näheren Betrachtung bedarf.

Weiterhin erscheint es sinnvoll, zur Unterstützung des vorgestellten Vorgehensmodells ein Software-Tool zu entwickeln, welches Sicherheitsverantwortliche bei ihrer Arbeit unterstützt.

Literatur

[BfSidIB04] Bundesamt für Sicherheit in der Informationstechnik (BSI). IT-Grundschutzhandbuch. http://www.bsi.de/gshb/deutsch/download/GSHB2004.pdf (2005-08-05), 2004.

[Car03] Nicholas G. Carr. IT Doesn't Matter. *Harvard Business Review*, 81(5):41–49, Mai 2003.

[FS90] O.K. Ferstl und E.J. Sinz. Ein Vorgehensmodell zur Objektmodellierung betrieblicher Informationssysteme im Semantischen Objektmodell (SOM). *Wirtschaftsinformatik*, 32(Heft 6):566–581, 1990.

[FS91] O.K. Ferstl und E.J. Sinz. Ein Vorgehensmodell zur Objektmodellierung betrieblicher Informationssysteme im Semantischen Objektmodell (SOM). *Wirtschaftsinformatik*, 33(Heft 6):477–491, 1991.

[GK03] W. Gora und T. Krampert. *Handbuch IT-Sicherheit*. Addison Wesley, 2003.

[HP03] G. Hoppe und A. Prieß. *Sicherheit von Informationssystemen, Gefahren, Maßnahmen und Management im IT-Bereich*. Verlag Neue Wirtschafts-Briefe, Herne/Berlin, 2003.

[JR02] M. Jörg und P. Roßbach. Messung und Bewertung operationeller Risiken. Seiten 71–93, 2002.

[Kra03] T. Krampert. *Handbuch IT-Sicherheit, Strategien, Grundlagen und Projekte*, Kapitel Holistischer Ansatz zur IT-Sicherheit. Addison-Wesley, 2003.

[Mül05] Klaus-Rainer Müller. *IT-Sicherheit mit System*. Vieweg, Wiesbaden, 2005.

[ÖW03] H. Österle und R. Winter. *Business Engineering. Auf dem Weg zum Unternehmen des Informationszeitalters*. Springer, 2003.

[RD04] T. Rauschen und G. Disterer. Identifikation und Analyse von Risiken im IT-Bereich. *Praxis der Wirtschaftsinformatik*, (HMD 236), April 2004.

[Sch91] A.-W. Scheer. *Architektur integrierter Informationssysteme*. Springer, 1991.

[Sch01a] A.-W. Scheer. *ARIS - Modellierungsmethoden, Metamodelle, Anwendungen*. Springer, 4. Auflage, 2001.

[Sch01b] A.-W. Scheer. *ARIS - Vom Geschäftsprozess zum Anwendungssystem*. Springer, 4. Auflage, 2001.

[Öst95] H. Österle. *Business Engineering: Prozess- und Systementwicklung, Band 1 Entwicklungstechniken*. Springer, 2. Auflage, 1995.