

Sicherheit, die zählt

Die IT-Security-Scoring-Method (*IT-SSM*)
als Ratingverfahren im Rahmen von BASEL II

Dr. Wolfgang Böhmer¹
Bernd Donabauer²

PASS Network Consulting GmbH,
Schwalbenrainweg 24, D-63741 Aschaffenburg
EMail: wolfgang.boehmer@pass-consulting.com
Tel.: 060213881-260, Fax: 06021-3881-400

BASEL II soll unterschiedlichen Risiken, denen ein Unternehmen insgesamt ausgesetzt ist, Rechnung tragen – Kredit-Risiken, Markt-Risiken und Operationellen Risiken. Dabei hat das Basel II Komitee zur Bewertung von Operationellen Risiken mehrere Verfahren abstrakt und grob umrissen. In diesem Artikel wird speziell der Aspekt der operationellen Risiken, konkret die IT-Security-Risiken, betrachtet und ein griffiges Rating-Verfahren zu deren Bestimmung vorgeschlagen – aus der Sichtweise eines externen Prüfers wie etwa einer Bank.

Wie wichtig die IT-Infrastruktur wirklich ist

Die IT-Infrastruktur eines Unternehmens ist längst ein unverzichtbares Mittel für die betriebliche Leistungserstellung. Störungen der Verfügbarkeit oder mangelnde Funktionalität sind existenzielle Bedrohungen für Unternehmen. Kaum ein Geschäftsprozess läßt sich heute über einen längeren Zeitraum aufrecht erhalten, ohne die IT-Strukturen in Anspruch zu nehmen. Die IT-Infrastruktur im allgemeinen und die Security-Strukturen insbesondere sind somit als Produktivanlagen zu betrachten. Diese wesentliche Ansicht ist für eine klassische Produktionsanlage zur Herstellung materieller Güter unbestritten, wird im Falle der IT-Infrastruktur jedoch nach wie vor vernachlässigt.

Die Gründe für die weiterhin wachsende Bedeutung der IT-Infrastrukturen und damit der IT-Security für die Leistungserstellung sind vielfältiger Natur, sie lassen sich jedoch wie folgt zusammenfassen:

- Durchdringung und damit die Abhängigkeit aller Geschäftsprozesse von den Funktionen der IT-Systeme.
- Zunehmende Integration des elektronischen Datenaustausches über alle Geschäftsprozesse der wirtschaftlichen Wertschöpfungskette (SCM³, CRM⁴) hinweg – häufig unter das Schlagwort e-Business subsumiert.
- Die damit verbundene Ausweitung der Standards, Funktionen und Geschäftsprozesse, etwa auf Kunden und Partner, über klassische Organisationsgrenzen hinweg, wie sie bereits in weltweit verteilten, „virtuellen“ Forschungs- und Entwicklungszentren zu finden ist.

¹ Lehrbeauftragter der Technische Universität Darmstadt, Fachbereich Theoretische Informatik

² IT Security Strategist. Freier Mitarbeiter der PASS Network Consulting GmbH.

³ Supply Change Management (Zulieferkette)

⁴ Customer Relationship Management (Kundenbeziehung)

- Darüber hinaus die Öffnung bzw. Anbindung der Systeme zum Zweck der Datenübermittlung an öffentliche Netze mit intransparenten Sicherheitsstandards und der fehlenden Möglichkeit der Einflussnahme.
- Die fehlende Möglichkeit, die Standards, Funktionen und Geschäftsprozesse in alternativen, von der IT-Infrastruktur unabhängigen, Systemen abzubilden, bzw. die Abschaffung alternativer Systeme aus Kosten- und Standardisierungsgründen.

Die wachsende Abhängigkeit, einhergehend mit einer zunehmenden Komplexität der IT-Systeme, wird die physischen und nicht physischen Risiken, die durch eben jene Systeme entstehen, zumindest tendenziell erhöhen.

Risiken bewerten

Nach dem zweiten Konsultationspapier zur neuen Basler Eigenkapitalvereinbarung (Basel II) wird das operationale Risiko als „die Gefahr von unmittelbaren oder mittelbaren Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder von externen Ereignissen eintreten“⁵, bezeichnet.

Das Risiko wird als der zu erwartende Verlust verstanden und ergibt sich aus der Multiplikation der folgenden Faktoren:

- Gefährdungsindikator (Exposure Indicator, EI)
 - Wahrscheinlichkeit eines Schadensfalles (Probability of Loss Event, PE)
 - Verlusthöhe im Schadensfall (Loss Given that Event, LGE)
- Verlust (Expected Loss, EL) = EI x PE x LGE

In einer Weiterentwicklung dieses Ansatzes durch den Bundesverband Öffentlicher Banken Deutschlands e.V. (VÖB) wird das operationale Risiko als „das Risiko eines unerwarteten direkten oder indirekten Verlustes verstanden, der durch menschliches Verhalten, Prozess- und Kontrollschwächen, technologisches Versagen, Katastrophen und durch externe Einflüsse hervorgerufen wird“⁶. Auch wenn es sich hierbei um sehr allgemeine Definitionen handelt, so beinhalten diese unzweifelhaft auch solche Risiken wie etwa den Ausfall eines Datenbanksystems, die Überflutung eines Unternehmens mit Computerviren oder die Verbreitung von Raubkopien durch einen Mitarbeiter und die hieraus drohenden Schadensersatzforderungen.

In beiden Ansätzen, dem der Baseler Eigenkapitalvereinbarung und dem des VÖB, sind demnach die mit den IT-Systemen und –Strukturen verbundenen Risiken aufgeführt und daher den mit Eigenkapital zu hinterlegenden operationellen Risiken zugehörig.⁷

In dem Maße, wie die technische und organisatorische Abhängigkeit der Kernprozesse gegenüber der IT innerhalb der Wertschöpfungskette stetig zu nimmt, ist es unerlässlich, die damit verbundenen IT-Risiken zu bewerten. Zweifelsohne nimmt damit auch der Bedarf zur Einschätzung dieser Risiken zu – und letztendlich die Bedeutung der Verfügbarkeit sowie der Aufrechterhaltung der Kernprozesse im Rahmen der Beurteilung der Gesamtunternehmensrisiken. Letztlich ist dies die unverzichtbare Voraussetzung, um Maßnahmen zur Risikominimierung ergreifen zu können, und um damit auch einen Teil zur Optimierung des Finanzmanagements einer Unternehmung beizutragen.

⁵ Basler Ausschuss für Bankenaufsicht, 2001.

⁶ Bundesverband öffentlicher Banken Deutschlands, 2001.

⁷ Vgl. hierzu auch Gaulke, 2002, S. 18 f.

Wie in jedem komplexen System greift auch in heute typischen IT-Systemen die Beurteilung einzelner und vom Ganzen der Wertschöpfungskette losgelöster Komponenten zu kurz, um das Risiko einer möglichen Betriebsunterbrechung einschätzen zu können. Vielmehr bricht die Sicherheitskette der von den IT-Systemen abhängigen Wertschöpfung an ihrem schwächsten Glied. Hierbei kann es sich auch um das Nichtbeachten eines Gesetzes, das Fehlverhalten eines unzureichend geschulten Mitarbeiters oder um fehlerhafte Organisationsstrukturen handeln. Wird weiterhin berücksichtigt, dass IT-Systeme oftmals nicht nur einen, sondern mehrere Geschäftsprozesse gleichzeitig unterstützen, ist eine dedizierte Betrachtung notwendig. Die hieraus resultierenden Wechselwirkungen zwischen verschiedenen technischen Systemen und Organisationsstrukturen können zu einer Kumulation, aber auch zu einer gegenseitigen Abschwächung von Risiken in einzelnen Schlüsselsystemen führen, die bei einer Einzelbetrachtung der Systeme und ihrer immanenten Risikopotenziale nicht oder nur schwer erkannt wird. Die klassischen Bewertungsmodelle der IT, die historisch aus dem Risikomanagement im Rahmen von Softwareprojekten stammen, berücksichtigen diese systemimmanenten Wechselwirkungen nur unzureichend; sie sind in ihrer praktischen Anwendung sehr aufwendig.

Auf der anderen Seite existieren eine Reihe von Methoden, Werkzeugen und Verfahren, um die IT-Sicherheit in einem Unternehmen auf einem akzeptablen Niveau zu halten. Will man allerdings dieses Niveau beurteilen, muss von einem generellen Ansatz ausgegangen werden. Dieser hat nicht nur den Anspruch, die Umsetzung eines einzelnen Verfahrens zu bewerten, sondern die gesamte IT-Sicherheit mit einem vertretbaren Aufwand zu bewerten. Ebenso muss diese Bewertung im Prinzip für den Mittelstand genauso wie für Großunternehmen heranzuziehen sein, und sie soll hierbei den höchst unterschiedlichen Grad der Durchdringung und damit der Abhängigkeit der Geschäftsprozesse von der IT-Infrastruktur berücksichtigen. Weiterhin hat ein solches Bewertungssystem den branchenspezifischen Anforderungen Rechnung zu tragen. Demnach muss es sich auf einzelne Branchen anpassen lassen, ohne seine Gültigkeit für Vergleiche über Branchengrenzen hinweg zu verlieren. Mit anderen Worten: Es muss ein genereller funktionaler Zusammenhang gefunden werden, der „bewertungstauglich“ im Sinne der IT-Security ist.

Insbesondere stellt sich die Frage nach der Bewertungsmetrik, vorausgesetzt, dass ein genereller funktionaler Zusammenhang gefunden wird. In der Literatur⁸ lassen sich verschiedene Verfahren finden; sie zielen entweder auf eine Rangliste gemäß dem Zensurenbild ab, das im englischen Sprachraum angewandt wird und einen Bereich zwischen CCC bis AAA abdeckt, oder auf einem Punktesystem von z.B. 0 bis 100 Punkten. Die Gemeinsamkeit beider Verfahrenstypen besteht in der *linearen* Abbildung eines Zustandes, der auf eine Bewertungseinheit CCC bis AAA oder 0 bis 100 projiziert wird. Wesentlich wichtiger ist jedoch die Frage, ob alle sicherheitsrelevanten Aspekte erfasst sind, und wenn ja, wie?

Effiziente Systeme sind sichere Systeme

In einer ersten Annäherung ist es sinnvoll, die für das Sicherheitsniveau verantwortlichen Systeme und Strukturen in drei Kategorien zu gliedern. Als primäres System bezeichnen wir die IT-Systeme, deren eigentliche Aufgabe es ist, die Geschäftsprozesse in der Wertschöpfungskette abzubilden. Demnach handelt es sich hierbei etwa um Datenbank- oder Fileserver, die aktiven und passiven Netzwerkkomponenten, die Endgeräte, die Betriebssysteme und Anwendungssoftware etc. Fehler, die bei der Auswahl, der Implementierung und dem Betrieb dieser Systeme begangen werden, lassen sich, wenn überhaupt, nur durch einen erheblichen Mehraufwand in nachgeordneten Sicherungssystemen ausgleichen. Gleichzeitig beinhaltet die

⁸ So z.B. die Statements von Rick Fleming zum Thema Digital Defense

Betrachtung der primären IT-Systeme unter Sicherheitsaspekten eine Chance, bisher ungenutzte Optimierungspotenziale zu erschließen. Der Fokus richtete sich hierbei auf die genaue Erfassung, Bewertung und Optimierung der notwendigen betrieblichen Prozesse. In einem zweiten Schritt werden die Abbildung dieser Prozesse durch die primären IT-Systeme überprüft, ineffiziente Systeme und Strukturen überarbeitet sowie überflüssige Systeme und Strukturen eliminiert. Durch die Reduktion auf die notwendigen Kernprozesse kann die Komplexität der Systeme und Strukturen auf ein angemessenes Maß reduziert werden. Hierdurch sinkt, zumindest tendenziell, die Wahrscheinlichkeit eines Schadensfalles.

Effiziente primäre IT-Systeme sind daher auch immer sichere IT-Systeme.

Die sekundären Systeme sind zur Absicherung der Funktion der primären Systeme erforderlich, haben jedoch keine originäre Aufgabe bei der Abbildung der Geschäftsprozesse. Allerdings ermöglichen sie durch ihre Funktion erst den geregelten und sinnhaften Betrieb der primären Systeme. Demnach handelt es sich hierbei etwa um Firewall-Systeme, Virens Scanner, Intrusion Detection-Systeme, Daten-Backupsysteme etc. Während primäre Systeme oft weitestgehend unverändert und über Jahre hinweg ihre Funktion erfüllen, zeichnen sich sekundäre Systeme durch ihre außerordentliche Dynamik in der Anpassung auf neue Gefahrenpotenziale aus. Gerade diese Systeme müssen in einem ständigen, zyklischen Prozess auf ihre Angemessenheit überprüft und gegebenenfalls angepasst werden.

Management	Organisation, Personalentwicklung, Recht, Systemdokumentation, Audit, Hard- und Softwaremanagement, Budget-Planung, Projektmanagement, Riskmanagement, Notfallkonzepte, Datenschutz
Infrastruktur	Passive und aktive Netzkomponenten, Versorgung, Gebäudesicherheit, Serverraum, Arbeitsplatz
IT-Systeme	Server- Client-Hardware, Server- Client-OS, TK-Anlage, mobile Geräte
Netze	Netzmodell, heterogene Netze, verteilte Standorte, Anbindung, Netz- und Systemmanagement, Backup-Geräte, Backup-Systeme, Test-Systeme
Anwendungen	Serveranwendungen, Clientanwendungen, Internetanwendungen, Anwenderdaten in Dateiform, programmgebundene Anwenderdaten (z.B. Database)
Sicherungs-systeme	Firewall, AV-Software, SPAM-Filter, IDS, VPN, Verschlüsselung, Signatur, Biometrie, DRS

Quelle: Eigene Darstellung.

Abbildung 1: Übersicht der zu berücksichtigende Systeme und Strukturen.

Den primären und sekundären Systemen zugeordnet sind jene Organisationsstrukturen, die für Betrieb, Wartung und Erweiterung der Systeme verantwortlich sind, also etwa die IT-Abteilung, ihre Mitarbeiter und die übergeordneten Entscheidungsinstanzen; weiterhin die IT-Prozesse und eingesetzten Managementtools, etwa das Projektmanagement oder ein Tool zur Erfassung und Auswertung der Support-Calls.

IT Security als integriertes Managementkonzept

In vielen Unternehmen wird mit dem Thema IT-Sicherheit sehr ähnlich umgegangen, wie etliche Studien der jüngsten Zeit deutlich machen (KES/KPMG/2002). Alle Studien finden nahezu übereinstimmend heraus, dass heutzutage wesentlich mehr in sekundäre IT-Sicherheitskomponenten wie z.B. Firewall-Systeme, Virens Scanner, etc. investiert wird, als in ein übergreifendes Sicherheitsmanagement. Der Eindruck dieser Studien bestätigt sich bei der Betrachtung der Liste der möglichen Werkzeuge und Tools. Auch hier wird deutlich, dass der Schwerpunkt der Marktunterstützung auf das Segment der technischen IT-Sicherheitskomponenten abzielt.

Wie bereits erwähnt ist damit keinesfalls gewährleistet, dass die Wertschöpfung in einem Unternehmen nicht unterbrochen werden kann.

Erst, wenn weitere Maßnahmen getroffen sind, lässt sich zuverlässig sagen, ob ein Unternehmen generell gewappnet ist. Die in Abbildung 2 dargestellte Grafik zeigt das Idealbild, nach dem Unternehmen ihre IT-Infrastruktur unter dem Aspekt der IT-Sicherheit ausrichten sollten. Die hierarchische Darstellung der ineinander verschachtelten Dreiecke zeigt die Abhängigkeiten: Die IT-Security-

Policy übt ein Diktat auf die tieferen Schichten aus. Unterhalb der Policy-Ebene ist die Konzept-Ebene angesiedelt, die konkreter auf die Randbedingungen eingeht, welche die Policy vorgibt. Die technischen Randbedingungen werden in der IT-Security-Architektur bestimmt, die dann in der untersten Ebene, der Realisierung der IT-Security Operation, umgesetzt werden. Auf dieser untersten Ebene sind sowohl die typischen o.g. sekundären IT-Sicherheitskomponenten angesiedelt als auch die sicherheitskonforme Ausprägung der primären IT-Systeme, deren Aufgabe es ist, die Geschäftsprozesse in der Wertschöpfungskette abzubilden.

In vielen Fällen empfiehlt es sich, die dazu gehörenden Organisationsstrukturen des IT-Sicherheitsmanagements nicht in die eigentlichen IT-Organisationsstrukturen zu integrieren. Da es sich bei den IT-Systemen und Strukturen ja um Querschnittsfunktionen handelt, deren Störung die gesamte Wertschöpfungskette beeinträchtigen kann, sollte das Sicherheitsmanagement in einer beratenden Funktion als Stabsstelle direkt der Unternehmensführung zugeordnet werden. Nur so können letztlich die Unabhängigkeit des Sicherheitsmanagements und die Vermeidung von inhärenten Zielkonflikten gewährleistet werden. Dem entspricht die Forderung von Basel II nach einem unabhängigen Management- und Kontrollverfahren sowie die Einbeziehung der obersten Managementebene in ein Sicherheits- und Risikomanagement. Nachfolgend werden zwei Beispiele für den Aufbau einer IT-Sicherheitsorganisation dargestellt.

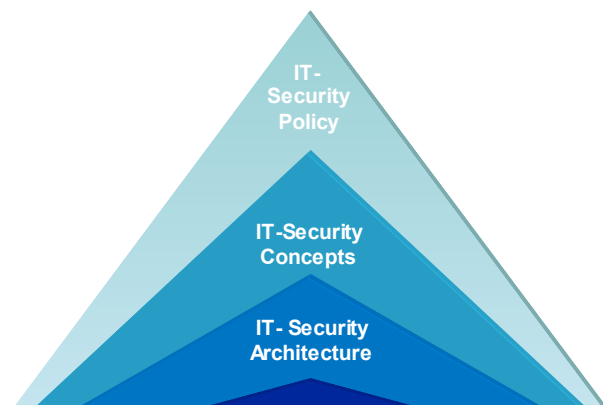
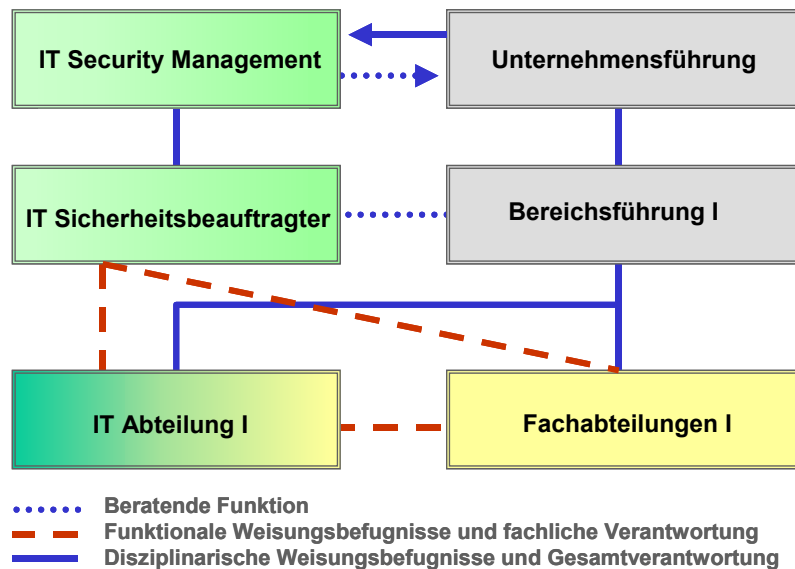


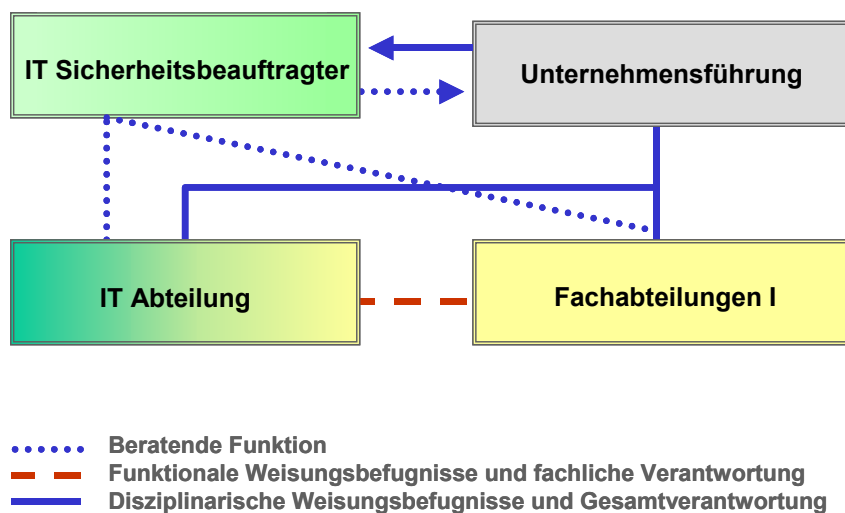
Abbildung 0: Idealbild der Sicherheitsstrukturen in Unternehmen



Quelle: Donabauer, Bernd, 2004.

Abbildung 2 Aufbau einer IT-Security-Management-Organisation I.

Das erste Beispiel ist eher geeignet für große Organisationen an verteilten Standorten oder für Organisationen mit wenig ausgeprägten Weisungshierarchien. In diesem Fall besteht der Vorteil darin, dass die IT-Security-Management-Organisation parallel zu der Organisationsstruktur des Unternehmens aufgebaut werden kann.



Quelle: Donabauer, Bernd, 2004.

Abbildung 3: Aufbau einer IT-Security-Management-Organisation II.

Das zweite Beispiel eignet sich hingegen für Organisationseinheiten mittlerer Größe – nicht zuletzt, weil der hierfür notwendige Ressourceneinsatz wesentlich geringer ist. Kann keines der beiden Beispiele Anwendung finden, etwa weil die eben genannten Ressourcen nicht vorhanden sind, ist zu überlegen, ob das IT-Sicherheitsmanagement in Teilen oder als Ganzes in ein Outsourcing-Modell überführt wird.

In der Praxis sind ausgeprägte IT-Security-Management-Organisationen nur selten zu finden, auch wenn die Einsicht in deren Notwendigkeit zunimmt. Das Eingangs geforderte Bewertungssystem und die dazugehörigen Metriken müssen demnach sowohl defizitäre Organisati-

onsstrukturen beurteilen können als auch solche, in denen ein übergeordnetes Sicherheitsmanagement existiert.

IT-Security: Verfahren und Regeln

Neben den technischen IT-Sicherheitskomponenten, dem Sicherheitsmanagement und der dazugehörigen Organisation gibt es eine Reihe von Verfahren und Regelwerken, die eingesetzt werden können, um ein funktionierendes IT-Security-Rahmenwerk zu schaffen. Im folgenden ein Überblick über die bekanntesten Management-Werkzeuge und -Verfahren:

- Grundschriftbuch (IT-GsHB) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (Zertifizierung möglich)
- British Standard 7799 Part 1 (BS7799-1)
- British Standard 7799-2 (BS7799-2): Information Security Management Systems – Specification with guidance for use
- ITSec (europäische Ausrichtung),
- CommonCriteria (globale Ausrichtung)
- ISO /IEC TR 13335: Guidelines for Management of Security (GMITS)
- ISO /IEC IS 17799: Code of practice for Information Security Management
- COBIT (Control Objectives for Information and related Technology)
- Business Continuity Planning (BCP)
- Business Impact Analysis (BIA)
- COBRA ???, IT Infrastructure Library (ITIL)
- Business Continuity Planning (BCP)
- Business Impact Analysis (BIA)
- KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich), Artikel V, Basel II
- HGB §289, §315

Eine Sonderstellung nimmt die Personalzertifizierung zum IT Security Coordinator nach ISO/IEC 17024:2003⁹ ein. Hierbei handelt es sich um ein in Deutschland entwickeltes Verfahren der Personalentwicklung nach international gültigen Normen, in der nicht das Unternehmen, sondern eine konkrete Person zertifiziert wird. Grundlage dieser Zertifizierung ist die arbeitsprozessorientierte Aneignung von Handlungskompetenz in einem realen Security-Projekt, das i.d.R. im eigenen Unternehmen durchgeführt wird. Der Standard eignet sich daher sehr gut, um eigene Humanressourcen zu schaffen, und gleichzeitig dazu, in Verbindung mit anderen hier genannten Verfahren das IT-Security-Rahmenwerk zu entwickeln bzw. zu verbessern.

In Deutschland hat sich in den letzten Jahren das IT Grundschriftbuch des BSI zu einem „Quasistandard“ entwickelt. Dennoch ist zu betonen, dass sich die Inhalte der verschiedenen Verfahren z.T. überschneiden, gegenseitig ergänzen bzw. sich lediglich durch unterschiedlich gesetzte Schwerpunkte auszeichnen.

In einem IT-Security-Rating muss das Unternehmen, das sich einem Rating unterzieht, daher die Freiheitsgrade haben, beliebige Verfahren und Tools einzusetzen bzw. aus den unterschiedlichen Verfahren eine eigene Best-Practice-Vorgehensweise zu entwickeln. Dennoch muss es möglich sein, den Zustand der Gesamtunternehmenssicherheit festzustellen und an

⁹ Vergleiche hierzu www.cert-it.de.

nen, ist es zielführend, ein Architekturmodell heranzuziehen. Einerseits soll dies die Komplexität reduzieren, andererseits wiederholbare und vergleichbare Größenbetrachtungen ermöglichen. Diese finden dann in einem späteren Benchmarking Verwendung.

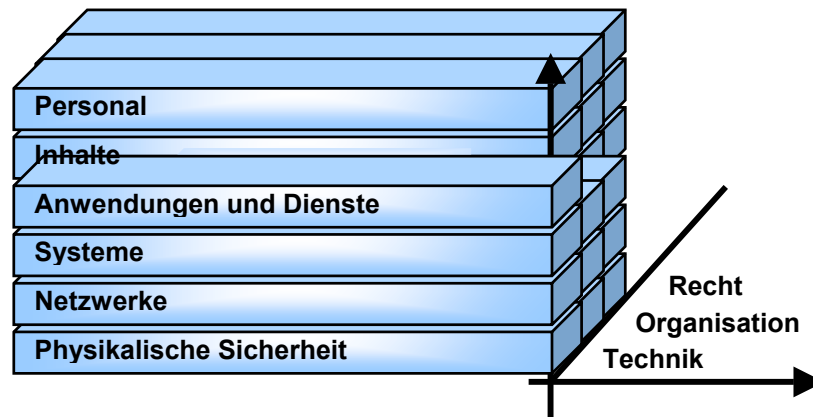


Abbildung 6: Architekturmodell zur Reduktion der Komplexität

In der Anwendung des Architekturmodells werden alle an einem Prozess beteiligten Komponenten in vertikale und horizontale Komponenten überführt. Dabei werden die vertikalen Komponenten durch die Größen *Personal*, *Inhalt*, *Anwendungen* sowie *Dienste*, *Systeme*, *Netzwerke* und *physikalische Sicherheit* abgebildet. Die horizontalen Komponenten werden durch die Größen *Recht(Mensch)*, *Organisation* und *Technik* abgebildet. Die horizontalen Größen stellen dabei auch gleichzeitig die Kerngrößen eines jeden Unternehmens dar und bilden gleichzeitig das Hauptsegment des Verfahrens wie in Abbildung 7 dargestellt. Hier werden im Rahmen der Erstbewertung vier Module gezeigt, die ihrerseits jeweils Haupt- und Nebenkriterien in einer untergeordneten Ebene enthalten.

In späteren Anwendungsszenarien (Laufende Bewertung) können bei einer Wiederholung bestimmte Kriterien als zwingend etc. eingestuft werden. Es werden alle dabei gewonnenen Informationen der Haupt- und Nebenkriterien in eine Datenbank abgelegt. Die Bewertung der Kriterien erfolgt nach einer 5-Punkte-Skala, um einen neutralen Medianwert zuzulassen.

Entscheidend für die Anwendung der Methode ist allerdings die geeignete Wahl der Messpunkte, die sich auf die Haupt- und Nebenkriterien in den jeweils vier Modulen verteilen. Dabei wird eine bestimmte Gewichtung der Messpunkte sowie der Haupt- und Nebenkriterien vorgegeben. An den Messpunkten werden empirische und metrische Kennzahlen erfasst. Als Gesamtergebnis entsteht eine verdichtete Kennzahl, die sich in eine Scoring-Klasse einordnen lässt.

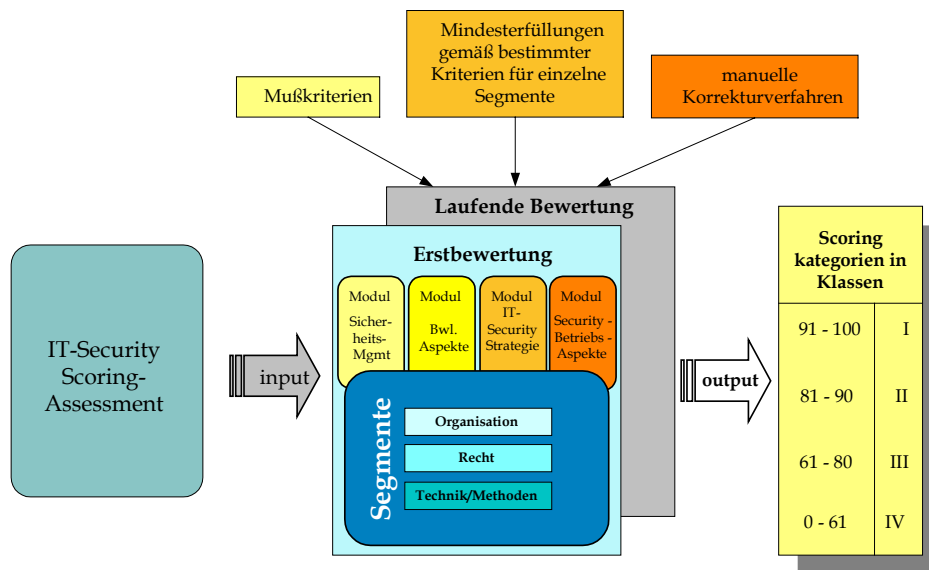


Abbildung 7: Ablauf der IT-Security-Scoring-Method zur Evaluierung einer Gesamtunternehmenssicherheit.

Status und Anreize

In Zusammenarbeit mit anderen Organisation und Institutionen soll eine Datenbank aufgebaut werden, in die in anonymisierter Form Ergebnisse eingepflegt werden. Damit besteht die Möglichkeit, eigene (firmeninterne) Ergebnisse in einem Benchmarking-Verfahren gegen Firmen z.B. aus der gleichen Branche zu spiegeln. Im Verlauf der Zeit entstehen dann fundierte anonymisierte Daten über das IT-Sicherheitsniveau bestimmter Branchen.

Die Scoring-Method bietet einen starken Startanreiz für die Teilnehmer: Das Verfahren wird zunächst mit mehreren Pilotkunden durchgeführt, um einerseits eine Datenbasis zu etablieren und andererseits Erfahrungen und Potenzial für die Bewertungsskalierung aufzubauen. Im Gegenzug erhalten die Pilotkunden nach der Einführungsphase und einer weiteren Durchführungsphase eine zweite Durchlaufphase, um die Aussagekraft der ersten Ergebnisse auf eine solide Datenbasis zu stellen.

1 Literaturverzeichnis

Basler Ausschuss für Bankenaufsicht (Hrsg.), 2002	Die neue Basler Eigenkapitalvereinbarung – Konsultationspapier in der Übersetzung der Deutschen Bundesbank, 1/2001.
Böhmer, Wolfgang, 2001	Enterprise Security Management (ESM) in Danet Nachrichten 1/2001
Böhmer, Wolfgang 2002a	CASTforum, Veranstaltung am 15.05.02, Netze http://www.cast-forum.de/events/cast/2002/Netzwerksicherheit
Böhmer, Wolfgang 2002b	CAST-Forum, Veranstaltung am 15.08.02, Sicherheitsengineering http://www.cast-forum.de/events/cast/2002/ITSec
Böhmer, Wolfgang 2002c	VPN, die reale Welt der virtuellen Netze, Hanser Verlag, ISBN 3-446-21532-8, Kap.3 Informations- und Kommunikationssicherheit, München 2002
Bundesverband öffentlicher Banken Deutschlands (Hrsg.)	Aktuelles – Ausgabe II/2001, S. 12-13.
Donabauer, Bernd	CAST-Forum, Workshop „Recht und IT-Sicherheit“ am 22.04.2004 http://www.cast-forum.de/events/cast/2004/???
Gaulke, Markus	Risikomanagement in IT-Projekten. Oldenburgverlag. München, Wien, 2002. ISBN 3-486-25743-9
KES/KPMG/2002:	Sonderdruck KES/KPMG-Sicherheitsstudie 2002; SecuMedia Verlags GmbH, D-55205 Ingelheim
Martin Kütz (Hrsg.)	Kennzahlen in der IT; dpunkt.verlag, Heidelberg 2003, ISBN 3-89864-225-9
Romeike, Frank	RiskNet Institute, http://www.risknet.de/
Schäfer/Pösel	Werteanalyse