

G 59071  
4,50 EUR\*

# RATING **C** aktuell

Information für Unternehmen und Finanzdienstleister

**05/2004**  
Oktober/November

[www.ratingaktuell-news.de](http://www.ratingaktuell-news.de)  
[www.ratingaktuell-ticker.de](http://www.ratingaktuell-ticker.de)

\* zzgl. Versand und 7 % MwSt.

## IT-SECURITY

Risiken in den  
Griff kriegen

## WETTBEWERBSVORTEIL

Automatisierte  
Kreditentscheidung

## RATING-PROZESS

Pro und Contra der  
Geheimhaltung

## Rating von Krankenversicherern

Top-Interview mit PKV-Chef Gerd Bilsing

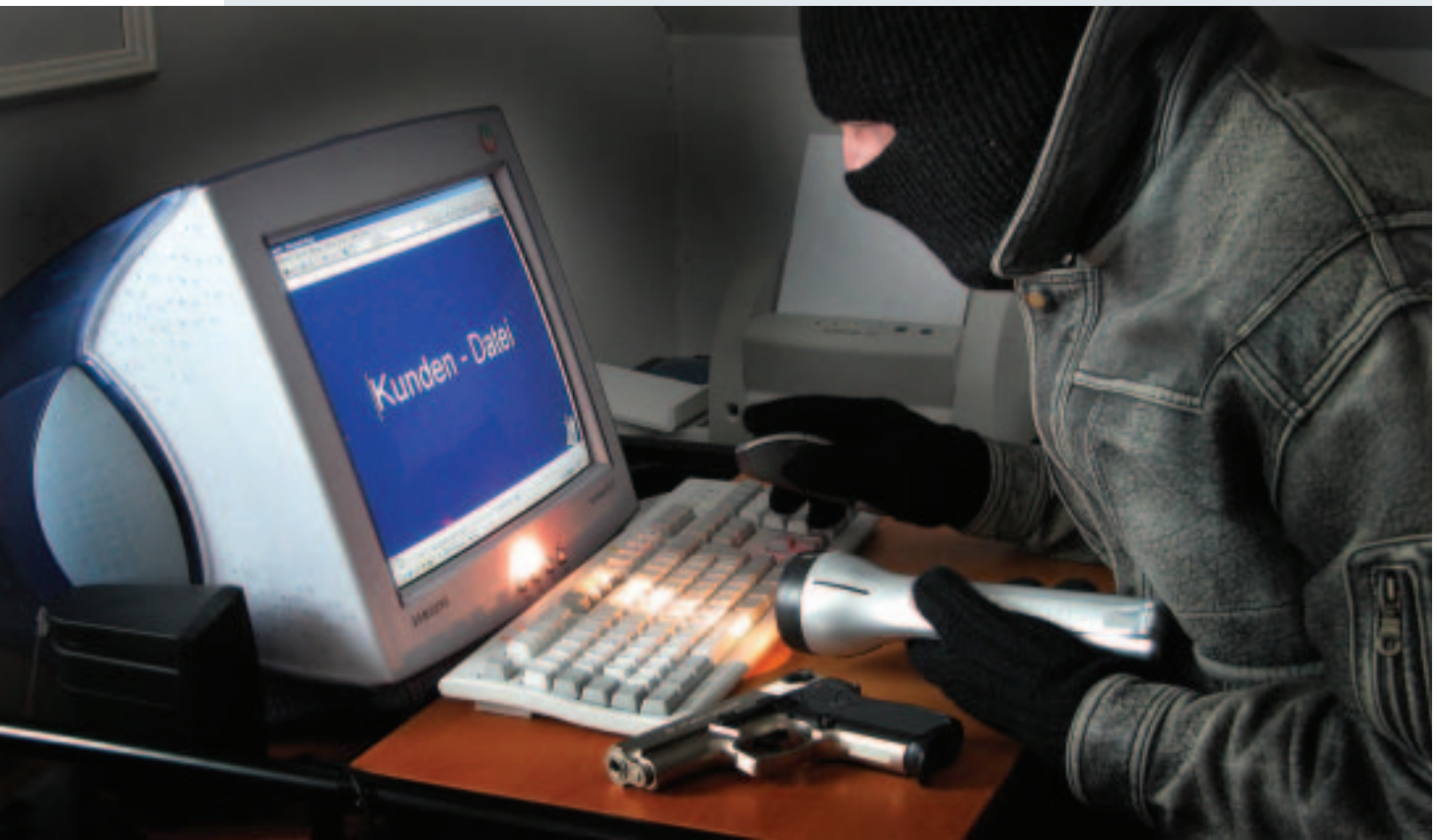
Mit Themen-Schwerpunkt  
**Fonds-Rating**

# IT-Risiken in den Griff kriegen

## Rating-Verfahren für IT-Security

Wolfgang Böhmer/Bernd Donabauer

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. Mit einem speziellen Rating-Verfahren, so zeigt unser Beitrag, lässt sich die Qualität der IT-Sicherheit bewerten.



Die IT-Infrastruktur im Allgemeinen und die Security-Strukturen im Besonderen sind in der modernen Betriebswirtschaftslehre als so genannte Produktivanlagen zu betrachten. Diese einhellige Meinung 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 liegen u. a. in der Durch-

dringung und damit in der Abhängigkeit aller Geschäftsprozesse von den Funktionen der IT-Systeme. Die zunehmende Integration des elektronischen Datenaustausches über alle Geschäftsprozesse der wirtschaftlichen Wertschöpfungskette (SCM<sup>1</sup>, CRM<sup>2</sup>) hinweg,

# eSe Security®



## Diese Sicherheitslösung kann Ihr Rating verbessern

Umfassende IT-Sicherheit für Ihr Unternehmen können auch Firewalls oder Virenschutzprogramme alleine nicht bieten.

Mit **En.Gate** kommt von **eSe Security** jetzt neu ein ganzheitlicher IT-Security-Service.

Für den gewerblichen Mittelstand, Freiberufler und Gewerbetreibende.

Ab 49 Euro pro Monat.

**En.Gate** entspricht der ISO Norm 17799 für Sicherheit in der Informationstechnologie.

Der IT-Security Service **En.Gate** passt sich den individuellen betrieblichen Bedürfnissen an.

**En.Gate** ist ideal geeignet für kleine Datennetze bis zu 50 PC-Arbeitsplätze.

Der **En.Gate** IT-Security-Service umfasst:

- ein ganzheitliches, unternehmensspezifisches IT-Security Konzept
- eine ISO-Norm-konforme Sicherheit des Datennetzes
- ein auf das unternehmensspezifische IT-Security-Konzept abgestimmtes Mitarbeiter-Training

Im Ergebnis heißt das:

Verbesserte Kreditwürdigkeit bei Ihrer Bank.

**Weitere Informationen zu En.Gate unter:**

eSe Security GmbH, Europaplatz 7, D-44269 Dortmund  
Telefon +49 (0) 231.56 76 47-0, Telefax +49 (0) 231.56 76 47-147  
E-Mail: [info@ese-security.de](mailto:info@ese-security.de), Internet: [www.ese-security.de](http://www.ese-security.de)

häufig unter dem Schlagwort E-Business subsumiert, sowie 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, spielen eine gewichtige Rolle. Darüber hinaus sind die Öffnung bzw. Anbindung der Systeme zum Zweck der Datenübermittlung an öffentliche Netze mit intransparenten Sicherheitsstandards und der fehlenden Möglichkeit der Einflussnahme sowie die fehlende Möglichkeit, Standards, Funktionen und Geschäftsprozesse in alternativen, von der IT-Infrastruktur unabhängigen, Systemen abzubilden, bzw. die Abschaffung alternativer Systeme aus Kosten- und Standardisierungsgründen als weitere Treiber für diese Entwicklung zu nennen. 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.

### Bewertung von Risiken

Nach dem zweiten Konsultationspapier zur neuen Baseler 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“, bezeichnet. Auch wenn es sich hierbei um sehr allgemeine Definitionen handelt, so enthalten diese unzweifelhaft auch solche Risiken,

<sup>1</sup> Supply Chain Management (Zulieferkette).

<sup>2</sup> Customer Relationship Management (Kundenbeziehung).

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. Demnach sind die mit den IT-Systemen und -Strukturen verbundenen Risiken eindeutig den operationellen Risiken zugehörig.<sup>3</sup> In gleichem Maße, wie die technische und organisatorische Abhängigkeit der Kernprozesse gegenüber der IT innerhalb der Wertschöpfungskette stetig zunimmt, ist es unerlässlich, die damit verbundenen IT-Risiken zu bewerten. Zweifelsohne nimmt damit auch der Bedarf zur Einschätzung dieser Risiken und die Bedeutung der Verfügbarkeit sowie der Aufrechterhaltung der Kernprozesse im Rahmen der Beurteilung der Gesamtunternehmensrisiken zu. Letztlich ist dies die unverzichtbare Voraussetzung, um Maßnahmen zur Risiko-Minimierung ergreifen zu können und um damit auch einen Teil zur Optimierung des Finanzmanagements einer Unternehmung beizutragen.

### Abhängigkeit der Geschäftsprozesse von der IT-Infrastruktur

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 Risiko-Potenziale nicht oder nur schwer erkannt wird. Die klassischen Bewertungsmodelle der IT, die historisch aus dem Risiko-Management 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 Fachliteratur lassen sich verschiedene Verfahren finden; sie zielen entweder auf eine Rang-Liste gemäß dem Zensurenbild ab, das im anglo-amerikanischen Raum 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

<sup>3</sup> Vgl. Markus Gaulke: Risikomanagement in IT-Projekten, München/Wien 2002, S. 18 ff.

ausgleichen. Gleichzeitig beinhaltet die Betrachtung der primären IT-Systeme unter Sicherheitsaspekten eine Chance, bisher ungenutzte Optimierungspotenziale zu erschließen. Der Fokus richtet 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 zurückgeführt werden. Hierdurch sinkt, zumindest tendenziell, die Wahrscheinlichkeit eines Schadensfalls.

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 usw. 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 (Abb. 1). Den primären und sekundären Systemen zugeordnet sind jene Organisationsstrukturen, die für Betrieb, Wartung und Erweiterung der Sys-

Abb. 1: Übersicht der zu berücksichtigenden Systeme und Strukturen

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

teme 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 Erhebungen der jüngsten Zeit deutlich machen (KES/KPMG/2002). Alle Studien sind nahezu übereinstimmend zu dem Ergebnis gekommen, dass heutzutage wesentlich mehr in sekundäre IT-Sicherheitskomponenten, wie etwa Firewall-Systeme, Virens Scanner etc. investiert wird, als in ein übergreifendes Sicherheitsmanagement. Der Eindruck 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.

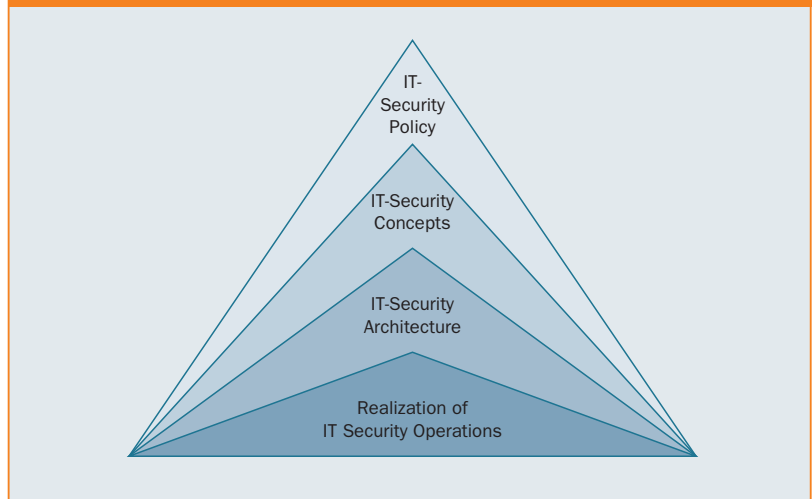
Erst, wenn weitere Maßnahmen getroffen sind, lässt sich zuverlässig sagen, ob ein Unternehmen generell gewappnet ist. Die in Abb. 2 dargestellte Grafik zeigt das Idealbild, nach dem Unternehmen ihre IT-Infrastruktur unter dem Aspekt der IT-Sicherheit ausrichten. Die hierarchische Darstellung der ineinander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

gentlichen 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 (Abb. 3). 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 Risiko-Management.

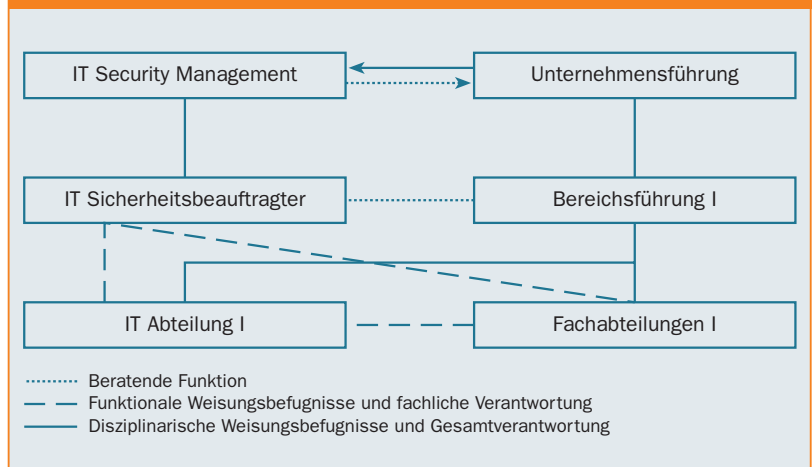
Das erste Beispiel ist eher geeignet für große Organisationen an verteilten Standorten oder für Organisationen mit wenig ausgeprägten Weisungshierarchien. In diesem Fall besteht der Vorteil darin, dass die IT-Security-Management-Organisation parallel zu der Organisationsstruktur des Unternehmens aufgebaut werden kann. Das zweite Beispiel (Abb. 4) 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 Organisationsstrukturen beurteilen

Abb. 2: Idealbild der Sicherheitsstrukturen in Unternehmen



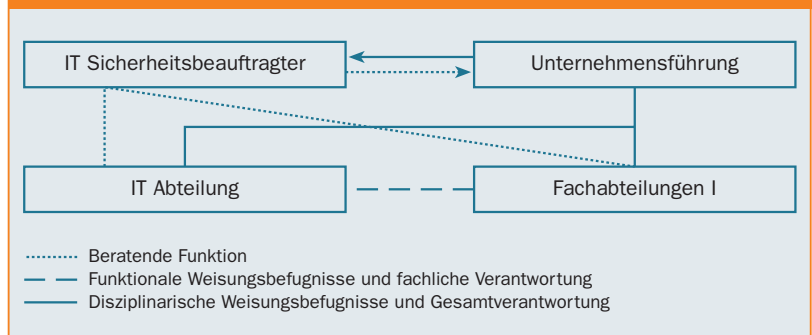
Quelle: Böhmer, Die reale Welt der virtuellen Netze (2002), S. 19

Abb. 3: Aufbau einer IT-Security-Management-Organisation I



Quelle: Donabauer (2004)

Abb. 4: Aufbau einer IT-Security-Management-Organisation II



Quelle: Donabauer (2004)

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. Hierfür stehen eine Reihe von Management-Werkzeugen und -Verfahren zur Verfügung (siehe Kasten 1).

Eine Sonderstellung nimmt die Personalzertifizierung zum IT Security Coordinator nach ISO/IEC

17024:2003<sup>4</sup> 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

Grundschutzhandbuch 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 einer Werteskala zu raten. Denn was nicht messbar ist, ist nicht bewertbar und was nicht bewertbar ist, ist nicht verbesserungsfähig. Dies entspricht der Forderung von Basel II nach der systematischen Erfassung und Dokumentation von Risiken.

### IT-Security-Scoring-Method

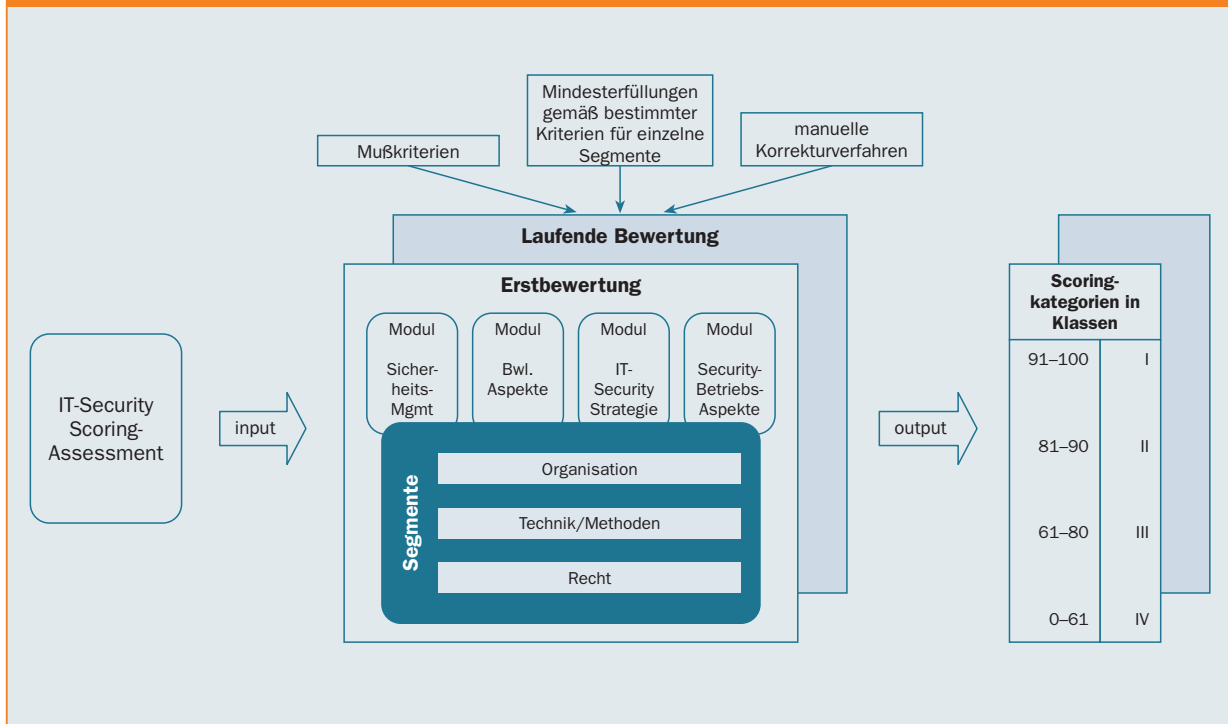
Der Kerngedanke des IT-Security-Scoring-Method (IT-SSM) kann durch ein gleichschenkeliges Dreieck ausgedrückt werden. Dabei bestehen die Antipoden aus den Größen Organisation, Technik und Mensch (eingebettet in rechtliche Rahmenbedingungen). Mit diesen drei Antipoden lassen sich im Prinzip sämtliche Verfahrensabläufe, Prozesse und deren Wechselwirkungen untereinander beschreiben – innerhalb eines Unternehmens ebenso wie organisationsübergreifend. Diese Grundidee fließt in die IT-SSM vollständig ein. Die IT-Security-Scoring-Method ist ein diagnostisches Verfahren; es ermöglicht auf Basis metrischer Größen und typischer Kennzahlen eine Beurteilung des IT-Sicherheits-Niveaus ei-

#### Kasten 1: IT-Security-Rahmenwerke 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

<sup>4</sup> Vergleiche hierzu [www.cert-it.de](http://www.cert-it.de).

Abb. 5: Ablauf der IT-Security-Scoring-Method



Quelle: Böhmer, Die reale Welt der virtuellen Netze (2002), S. 122

nes Unternehmens, bezogen auf seine unternehmerischen Kernprozesse. Dabei werden jene Größen, die in einem Unternehmen an der IT-Sicherheit beteiligt sind, als komplexes Zusammenspiel zwischen technischen, organisatorischen und rechtlichen Komponenten begriffen, und diese werden in ihrer Gesamtheit in einem Unternehmen bewertet; auch im Vergleich zu anderen Unternehmen.

Nach dem Benchmarking besitzt die Unternehmensführung zum einen eine Positionierung relativ zu anderen Unternehmen der gleichen Branche und erhält somit einen aufschlussreichen Hinweis über Optimierungspotenziale (Außenwirkung). Zum anderen treten wertvolle Informationen darüber zu Tage, an welchen Stellen das komplexe Zusammenspiel der IT (IT-Sicherheit) innerhalb des Unternehmens einen Handlungsbedarf aufweist (Innenwirkung). Zur Er-

fassung der Prozesse wird ein Prozessanalysetool benutzt, um auf einer abstrakten Ebene die beteiligten Prozesskomponenten zu erfassen. Dabei werden die Prozesse in Kernprozesse, begleitende und unterstützende Prozesse untergliedert. Eine weitere Einordnung geschieht durch die Unterteilung in Primär- und Sekundärprozesse. Um anschließend die teilweise komplexen Prozesse sicherheitstechnisch behandeln zu können, 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.

### Scoring-Verfahren

In der Anwendung des Architekturmodells werden alle an einem Prozess beteiligten Komponenten in vertikale und horizontale

le 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. Abb. 5 zeigt im Rahmen der Erstbewertung vier Module, die ihrerseits jeweils Haupt- und Nebenkriterien in einer untergeordneten Ebene enthalten. In späteren Anwendungsszenarien (Laufende Bewertung) können bei einer Wiederholung bestimmte Kriterien als zwingend usw. 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.

#### Status und Anreize

In Zusammenarbeit mit anderen Organisationen und Institutionen soll in der praktischen Umsetzung des Rating-Verfahrens 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 aus der gleichen Branche zu spiegeln. Im Verlauf der Zeit entstehen dann fundierte anonymisierte Daten über das IT-Sicherheitsniveau bestimmter Branchen. 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. ■

**Dr. Wolfgang Böhmer** ist Lehrbeauftragter der Technischen Universität Darmstadt, Fachbereich Theoretische Informatik. **Bernd Donabauer** ist IT Security Strategist und freier Mitarbeiter der PASS Network Consulting GmbH, Aschaffenburg.

Finanzierung  
Leasing  
Factoring



## FLF – sechsmal jährlich lesen und profitieren

Werden Sie Insider! Testen Sie

FLF – Finanzierung Leasing Factoring.

### FLF – herausgegeben von den führenden Verbänden der Branche

Eine Plattform für Praktiker und Wissenschaftler zur Diskussion aktueller und grundsätzlicher Tendenzen und Problemlösungen auf den Gebieten

- ▶ des Konsumentenkredits
- ▶ der Investitionsfinanzierung
- ▶ des Geschäfts der Autobanken
- ▶ der Leasing- und Factoring-Gesellschaften.

Die Inhaltsverzeichnisse der letzten 10 Jahre finden Sie unter: [www.flf.de](http://www.flf.de)

### Bestellen Sie jetzt das kostenlose Probeabonnement

Wir senden Ihnen zwei aktuelle Ausgaben kostenlos zum Probelesen. Wenn Sie nicht innerhalb von zwei Wochen nach Erhalt des zweiten Heftes abbestellen, liefern wir FLF weiter im Abonnement.

Der Abonnementpreis beträgt für jährlich 6 Hefte Euro 75,00 + Euro 5,60 Versandkosten zuzüglich 7 % MwSt., zahlbar im Voraus für das Kalenderjahr. Die Bezugsdauer verlängert sich jeweils um ein Jahr, wenn das Abonnement nicht schriftlich bis zum 15. November zum Jahresende gekündigt wird.

#### Fax-Antwort:

**(0 30) 2 46 25 96-20**

Ja, wir bestellen hiermit zwei aktuelle Ausgaben der Fachzeitschrift FLF kostenlos zum Probelesen.

Firma .....

Lieferung z.Hd.

Name / Vorname .....

Position / Abt. ....

Telefon .....

Fax .....

E-Mail .....

Straße / Nr. ....

PLZ / Ort .....

Datum / Unterschrift .....

**Verlag für Absatzwirtschaft**

**Littenstraße 10**

**10179 Berlin**

**Telefon: (0 30) 2 46 25 96-13**

**E-Mail: [info@flf.de](mailto:info@flf.de)**

**Internet: [www.flf.de](http://www.flf.de)**