Auf der sicheren Seite –

Informationssicherheitsmanagement und IT-Governance

Treten im Zusammenhang mit einem kritischen Geschäftsprozess infrastrukturelle IT-Störungen auf, so sind oftmals längere Ausfallzeiten mit erheblichen Kosten die Folge. Leider werden solche Störungen und Risiken bei der Prävention immer noch kaum oder wenig ins Kalkül gezogen [KES/KPMG 2002]. Eines der wichtigen Probleme im Sicherheitsmanagement besteht darin, dass mit der Entwicklung hin zu verteilten IT-Systemen die Einschätzung der Sicherheitslage immer schwieriger wird. Zugleich ist das Bewusstsein für IT-Risiken allgemein unzureichend – erst langsam macht sich bei den Unternehmen die Erkenntnis breit, dass allein die Absicherung der IT-Komponenten nicht mehr ausreicht. Auch ist die IT-Sicherheitsorganisation weiterhin das Stiefkind der Unternehmen [KES/KPMG 2002]. Vor diesem Hintergrund gewinnt der Begriff IT-Governance zunehmend an Bedeutung. Dabei kann IT-Governance zurückgeführt werden auf die Führung, Organisationsstrukturen und Prozesse, die sicherstellen, dass die IT die Unternehmensstrategie und deren Ziele unterstützt. Um die heute zur Verfügung stehenden Verfahren und Modelle zur IT- oder Informationssicherheit hinsichtlich ihrer Unterstützung der IT-Governance zu überprüfen, werden nachfolgend das IT-Grundschutzmodell des Bundesamts für Sicherheit in der Informationstechnologie (BSI) dem British Standard 7799 gegenübergestellt.

Autor
Dr. Wolfgang Böhmer

arbeitet als Lehrbeauftragter am Lehrstuhl für Theoretische Informatik, Kryptographie und Computeralgebra der Technischen Universität Darmstadt. Seine Forschungsgebiete sind kryptograpische Protokolle in IP-Netzen sowie die zertifikatsbasierte Authentifizierung und deren Implementierung in IPSec. Kontakt: wboehmer@sec.informatik.tu-darmstadt.de

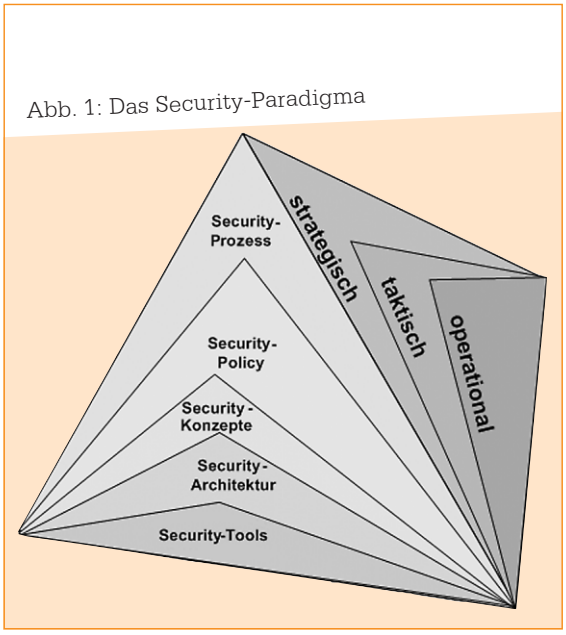
Es stehen heute eine Reihe von Ansätzen, Modelle und Verfahren zur Verfügung, die Unternehmen zur Sicherung ihrer IT-Infrastruktur anwenden können. Dabei folgen prinzipiell alle Ansätze dem heutigen Security-Paradigma, das vor allem auf die interne Sicherheitsproblematik eines Unternehmens fokussiert ist. Der anhaltende Trend zum Outsourcing in der IT und die Notwendigkeit, ein abgestimmtes firmenübergreifendes Sicherheitsniveau zu adressieren, wird in den Modellen bisher allerdings nur dürftig reflektiert. Oberhalb der Security-Policy ist der IT-Sicherheitsprozess angesiedelt, der zu einer Verzahnung mit der Organisation führt. Je nach Verfahren und Modell (IT-Grundschutzhandbuch oder British Standard 7799-2) werden unterschiedliche Zielrichtungen verfolgt.

Security-Paradigma

Das heute gültige Security-Paradigma ist als ein Rahmenwerk aufzufassen, welches die IT-Sicherheit in einem Unternehmen in ihren unterschiedlichen Aspekten systematisch erfassen und ordnen soll. Es lässt sich als Pyramide mit drei Seiten darstellen, die unterschiedliche Sichten auf die IT-Sicherheit präsentieren (vgl. Abb. 1).

Auf der Vorderseite sind die Security-Prozesse, Security-Policy, Security-Konzepte, und Security-Architektur hierarchisch angeordnet sowie Tools und Werkzeuge dargestellt. Auf der zweiten Seite wird der inhaltliche (Strategie, Taktik und Operationen) sowie zeitliche (lang-, mittel- und kurzfristig) Bezug zur Unternehmensplanung dargestellt. Die Security-Policy wird – ebenso wie die Security-Konzepte und Security-Architektur – als Gegenstand taktischer Planung verstanden. Ergebnisse taktischer Planung münden in Tools sowie Werkzeuge, die operational eingesetzt werden. Die dritte Seite der Pyramide ist noch unbesetzt, sie könnte dazu verwendet werden, um die zweite Seite in zwei spezielle Planungsbereiche und ihren Schnittstellen zum Information-Security-Management-System (ISMS) zu differenzieren. Eine Seite könnte den Bezug zum Risikomanagement her-

Abb. 1: Das Security-Paradigma



stellen, die andere zum allgemeinen Unternehmens-, Informations- oder Qualitätsmanagement.

Das Rahmenwerk beschreibt im Kern, wie die generellen IT-Sicherheitsziele (Vertraulichkeit, Verfügbarkeit, Integrität) mittels eines gestuften Planungsprozesses von der strategischen bis hin zur operationalen Ebene verfolgt werden sollen.

Mit der IT-Security-Policy werden die IT-Sicherheitsziele in einer abstrakten Weise festgelegt und zudem ein Rahmen für die untergeordneten Ebenen gesetzt. Dabei ist die IT-Security-Policy in dem übergeordneten Sicherheitsprozess des Unternehmens eingebunden und resultiert aus diesem. Unter einem Sicherheitsprozess sind diejenigen Schritte und Abläufe zu verstehen, die zur Einführung und Anpassung einer Security-Policy dienen. In den Security-Konzepten der taktischen Ebene sind konkrete Richtlinien für spezifische Themen mit unterschiedlichen Geltungsbereichen zu definieren. Dabei sind aus der Security-Policy angemessene Sicherheitsniveaus abzuleiten und qualitativ und gegebenenfalls auch quantitativ zu konkretisieren. Auf der nächsten Ebene ist die IT-Sicherheitsarchitektur angesiedelt, die den Vorgaben der übergeordneten Konzeptebene folgt. Diese zählt ebenfalls noch zur taktischen Ebene. Bestandteile einer solchen Sicherheitsarchitektur sind neben der Beschreibung der Absicherung der IT-Plattform konkrete Schutzmaßnahmen wie etwa für den Virenschutz, Remote Access, SAP-Systeme etc. Die operative Umsetzung (Implementierung) ist auf der untersten Ebene platziert. Hier werden die Maßnahmen umgesetzt, die aus dem IT-Sicherheitskonzept und der IT-Sicherheitsarchitektur resultieren [Böhmer 2005].

Die zentrale Idee dieses Paradigmas ist, dass die jeweils höhere Ebene den Rahmen und Vorgaben für die tiefer liegende Ebene definiert. Dabei nimmt die Granularität sowie die Technikorientierung bezüglich der einzusetzenden Absicherungsmaßnahmen sukzessive zu, während rein organisatorische Aspekte in den Hintergrund treten. Das Modell des Security-Paradigmas ist aus der Beherrschungssicht zu sehen, die notwendigen Umsetzungs- und Begleitprozesse – wenn beispielsweise IT-Service-Prozesse nach ITIL hinzugezogen werden – liegen nicht direkt im Fokus des Modells.

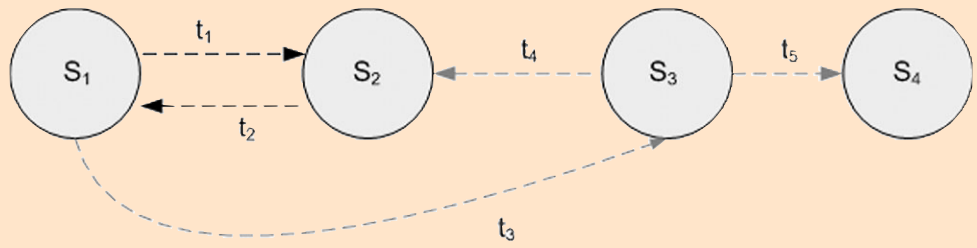
Security-Policies

Bei näherer Betrachtung des Begriffs Security-Policy sind inhaltlich sehr unterschiedliche Vorgaben denkbar, je nachdem, auf welche Ebene (strategisch, taktisch, operativ) sie sich beziehen. Grundsätzlich kann eine Security-Policy als Zustandsbeschreibung betrachtet werden, die für ein System autorisierte (oder sichere) und nicht autorisierte (oder unsichere) Zustände definiert [Bishop 2004].

Damit bilden Security-Policies die Grundlage für die Definition eines „sicheren" Systems: ein solch sicheres System startet in einem sicheren, autorisierten Zustand und kann diesen idealerweise nicht verlassen. Für einen einfachen Zustandsautomaten bedeutet dies etwa bei vier Zuständen und fünf Übergängen {t1…t5}, dass die Security-Policy die Zustände definiert, die autorisiert sind – hier beispielsweise A = {S1, S2}. Die anderen Zustände UA = {S3, S4} sind dagegen nicht autorisiert. Abb. 2 zeigt die Zustände und möglichen Zustandsübergänge für dieses Beispiel.

Allerdings beinhaltet das Modell des einfachen Zustandsautomaten nicht, welche Ereignisse dazu führen können, dass der Automat in den Zustandsübergang t_3 wechselt und schließlich in den Zustand S_3 kommt. Hierzu können Betrachtungen angestellt werden, welche Bedrohungen und Schwachstellen geeignet sind, das System in einen unsicheren Zustand zu überführen und es kann die Wahrscheinlichkeit eines Zustandsübergangs geschätzt werden. Allgemein werden diese Analysen als Risiko-Analysen verstanden. Damit definiert eine Security-Policy die Sicherheit für ein System oder auch für eine Reihe von Systemen. Security-Policies

Abb. 2: Security-Policy und Zustandsautomat



können qualitativ oder auch quantitativ beschrieben werden, sie können jedoch auch auf einem hohen mathematischen Abstraktionsgrad formuliert werden.

Bei näherer Betrachtung der in der Security-Pyramide systemimmanenten Grundziele der IT-Sicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) wird deutlich, dass diese ebenfalls auf generelle Zustandsbeschreibungen zurückgeführt werden können. Damit sind Policies zur Verfolgung von Sicherheitszielen geeignet [Bishop 2004]. Für die Zustandsbeschreibungen der Vertraulichkeit, Verfügbarkeit und Integrität sind der Literatur verschiedene formale Modelle zu entnehmen [siehe zu Modellen der Vertraulichkeit etwa das Bell-Lapadula-Modell: Bell/LaPadula 1973; Bell/LaPadula 1975, zu Modellen der Verfügbarkeit das Kiba-Modell: Kiba 1977 und zu Modellen der Integrität die Ausführungen von Schneewieß 1973].

Verfahren und Methoden zur Aufrechterhaltung der Security-Policy

Neben reinen technischen Aspekten müssen in einer Security-Policy ebenso organisatorische, personelle und räumliche Belange berücksichtigt werden. Erst das Zusammenwirken der verschiedenen Elemente einer Sicherheitsarchitektur ermöglicht das Erreichen eines angemessenen IT-Sicherheitsniveaus, da hier funktionelle, zeitliche und örtliche Beziehungen bestehen [Petzel 1996].

In den letzten nahezu zwei Dekaden haben sich mehrere Verfahren zur Einführung und Aufrechterhaltung einer Security-Policy etabliert. Bishop diskutiert beispielsweise verschiedene Arten von Security-Policies und definiert eine Security-Policy als Richtlinie, die besagt, was erlaubt und was nicht erlaubt ist und grenzt den Begriff gegen den des Security-Mechanismus ab [Bishop 2004; Bishop 2005]. Ein Security-Mechanismus ist demgemäß eine Methode oder ein Tool/eine Prozedur zur Durchsetzung einer Security-Policy [Bishop 2004]. In der Literatur wird der Begriff der Security-Policy uneinheitlich definiert. Dieser Begriff kann jedoch eingegrenzt werden auf eine Art Dokument, das Regeln beinhaltet, die aussagen, wer mit wem bestimmte Aktivitäten durchsetzen kann und Komponenten wie Entities (Akteure/Objekte), erlaubte Aktivitäten (Aktionen/ Beziehungen), sichere Konfigurationen/Vorwarnungen und Umsetzungen bezüglich Absicherung, Erkennen, Reagieren beschreibt.

Somit führt die Frage nach der Security-Policy ebenfalls zur Frage nach Verfahren und Adaption zur Initialisierung und zur Aufrechterhaltung, die nachfolgend diskutiert wird.

Zu nennen ist hier zum einen das IT-Grundschutzmodell, entworfen vom Bundesamt für Sicherheit in der Informationstechnologie in Bonn, zum anderen der vom Britisch Standard Institute (BSI-GB) in zwei Teilen gegliederte BS 7799. Beide Ansätze adressieren seit dem Jahr 2004 die gleichen Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit), schlagen jedoch unterschiedliche Vorgehensmodelle vor, um eine Security-Policy zu erstellen und zu managen [BSI-GB 2002a bzw. BSI-GB 2002b].

In beiden Modellen wird auch die Verknüpfung der IT-Sicherheitsziele mit den bedeutsamen Geschäftsprozessen eines Unternehmens unterschiedlich gehandhabt. Während der BS 7799 stärker die Geschäftsprozesse fokussiert und den umfassenden Begriff des Managements der Informationssicherheit einführt, betrachtet das Grundschutzmodell vornehmlich das Management der IT-Sicherheit und stellt eine Reihe von konkreten Maßnahmen in Form von so genannten Grundschutzbausteinen in systematischer Form zur Verfügung. Diese unterschiedlichen

Vorgehensmodelle hinsichtlich eines IT-Sicherheitsmanagements beim IT-Grundschutzmodell und des Informationssicherheitsmanagementsystems beim BS 7799 lässt sich ebenso in der Positionierung der Risiko-Analyse wieder finden. Die Risiko-Analyse nach BS 7799 ist auf der strategischen Ebene angesiedelt und adressiert Geschäftsprozesse. Beim IT-Grundschutzmodell ist sie dagegen auf der taktischen Ebene platziert und adressiert IT-Komponenten.

Das Grundschutzmodell des BSI

Abb. 3 zeigt das Vorgehensmodell zur Einführung und Erhaltung des IT-Grundschutzes [BSI 2004]. Auf der strategischen Ebene ist der IT-Sicherheitsprozess angesiedelt. Neben der Erstellung einer IT-Sicherheitsleitlinie stützt sich dieser im Wesentlichen auf eine Verantwortungsübernahme durch die Unternehmensführung. Die eigentliche Erstellung beziehungsweise Einführung des Grundschutzes wird über das IT-Sicherheitskonzept beziehungsweise die IT-Security-Policy geregelt. Dies erfolgt durch einen hierarchischen Ablauf, der von der Definition des IT-Verbundes und der IT-Struktur-Analyse ausgeht und auf der Basis einer Schutzbedarfsfeststellung in die Auswahl relevanter Bausteine nach dem IT-Grundschutz mündet. Dabei wird zwischen Muss- und Kann-Bausteinen unterschieden. Eine gesonderte IT-Sicherheits- oder Risiko-Analyse wird nur erforderlich, wenn der Schutzbedarf der betrachteten Objekte oberhalb der Kategorie „hoch“ angesiedelt ist. Nach einem Vergleich zwischen den vorhandenen und den vom Grundschutz vorgesehenen Maßnahmen (Basis-Sicherheitscheck) wird die Umsetzung vorgenommen. Im weiteren zeitlichen Verlauf wird für die Erhaltung der IT-Sicherheit gesorgt („Aufrechterhaltung im laufenden Betrieb“). Wie gut die Umsetzung der IT-Sicherheitsmaßnahmen in einem Unternehmen vorgenommen wurde, wird entweder durch die IT-Revision oder durch eine Zertifizierung durch das BSI geprüft. Beim Vorgehensmodell des BSI handelt es sich aus der Perspektive eines Unternehmens im Kern um ein Erhaltungsmodell. Denn die einmal getroffene Schutzbedarfseinstufung und die Auswahl der Bausteine nebst Maßnahmen wird – falls sich die Parameter der IT-Infrastruktur nicht ändern – beibehalten. Bei festgestellten Abweichungen zwischen den vorhandenen Sicherheitsmaßnahmen und den aus den Bausteinen resultierenden Maßnahmen wird eine Korrektur durch die betreffende Organisationseinheit des Unternehmens vorgenommen.

Eine Metrik zur Beurteilung der Realisierung des Grundschutzes ist nicht vorgesehen. Als Nachweis dient allein ein Audit oder die Zertifizierung nach den Formalien des BSI.

BS 7799-1 und BS 7799-2

Der angelsächsische Ansatz BS 7799 des British Standard Institute (BSI-GB) wurde nach einem Reifeprozess in den Jahren 1993 bis 1997 in zwei Teile aufgespalten. Der erste Teil (BS7799-

Abb. 3: Verfahren zur Umsetzung des Grundschutzes nach dem BSI (GER)

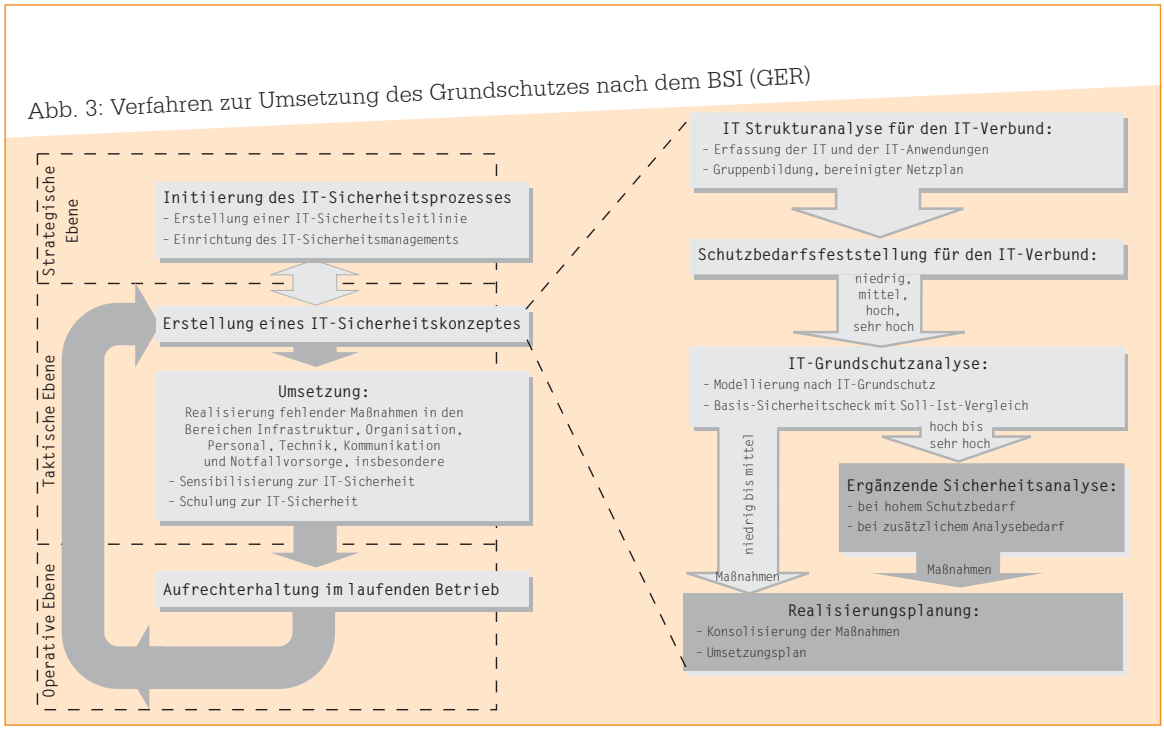
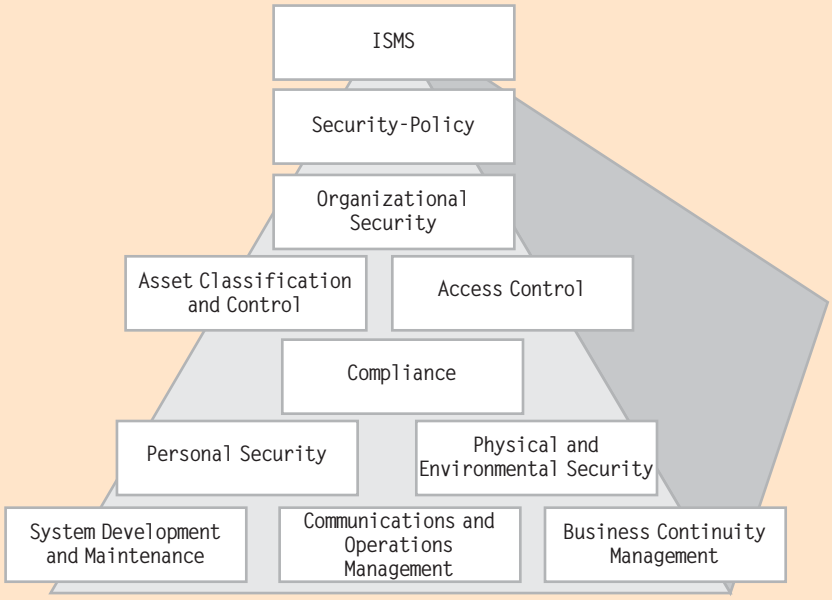


Abb. 4: Security-Paradigma und BS 7799-1



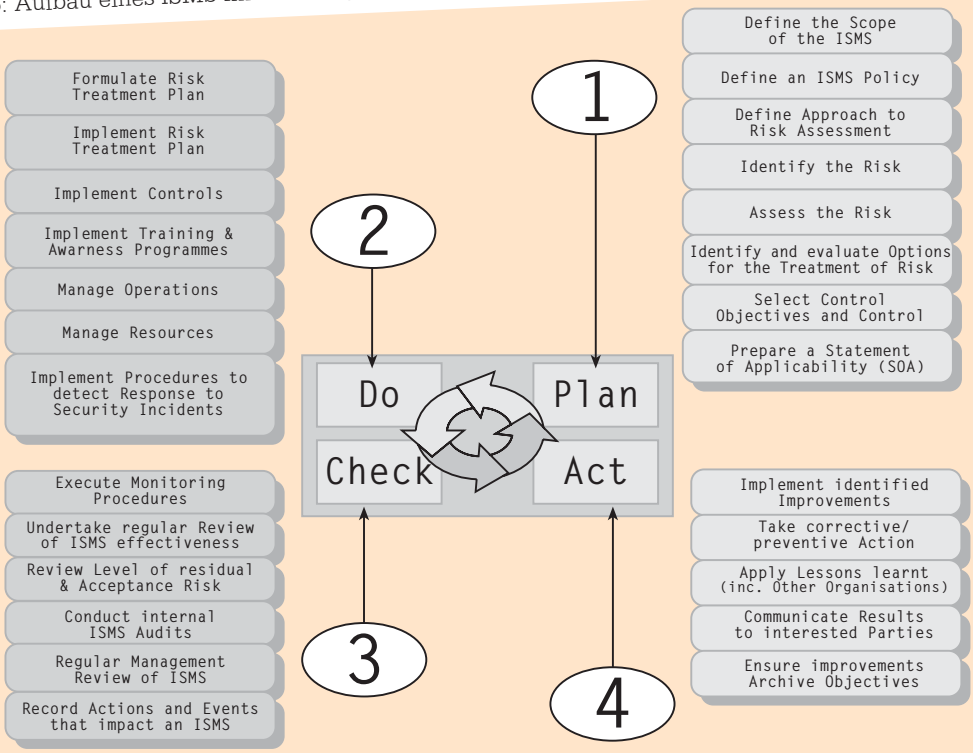
1:2002) stellt dem Anwender zehn Normenelemente als mögliche Richtlinien für eine Security-Policy zur Verfügung. Diese Normenelemente sind, abstrakt betrachtet, mit den Grundschutzmaßnahmen des BSI-GER vergleichbar [BSI 2003].

Inzwischen ist das BS7799-1:2002 in die ISO/IEC 17799:2002 überführt und im Jahr 2005 novelliert worden. Die aktuelle Version trägt die Bezeichnung ISO/IEC 17799:2005. Die novellierte Version hat einige Verbesserungen erfahren, unter anderem im Bereich Outsourcing und beim Umgang mit Fremdfirmen [ISO/IEC 2005]. Abb. 4 zeigt, wie die zehn Normen (Control Sections) in das Security-Paradigma einzuordnen sind. Für die zehn Normen sind 36 Sicherheitsziele (Security Objectives) definiert. Für diese gibt es wiederum eine oder mehrere Sicherheitskontrollen (Security Controls), insgesamt sind es 127. Oberhalb der Norm ist das ISMS angesiedelt, das dem Sicherheitsprozess zuzuordnen ist und die Initialisierung vornimmt.

Um ein effektives Management der Informationssicherheit in einem Unternehmen zu erreichen, ist der zweite Teil des BS7799 notwendig. BS7799-2 zielt auf eine Implementierung eines Management-Systems ab, das einerseits die bedeutsamen (kritischen) Geschäftsprozesse hinsichtlich ihrer IT absichert und andererseits in Anlehnung an die ISO 9001:2000 eine stetige Verbesserung in Form einer Qualitätssteigerung nach dem Deming Vier-Phasen-Qualitätskreis (PDCA-Cycle) fordert (siehe Abb. 5). In der Planungsphase (Plan = P) werden in acht Schritten diejenigen Normen und Sicherheitsziele aus dem BS7799-1 selektiert, die zur Sicherung der Geschäftsprozesse anzuwenden sind. Diese selektierten Normen oder „Statements of Applicability (SOA)“ bilden die Basis einer Sicherheitspolitik (Security Policy). Auch in diesem Modell werden – ähnlich wie in ITIL und CoBiT – normative Kontrollziele und Maßnahmen eingesetzt. Herausragende Bedeutung hat die Risiko-Analyse (Risk-Assessment), welche die kritischen Geschäftsprozesse (KP) und die abhängigen Assets (A) nach der Bedrohungs- und Schwachstellensituation beurteilt und entsprechende Maßnahmen postuliert.

Durch die stetige Verbesserung des PDCA-Cycles bekommt der ISMS-Ansatz eine andere Qualität als das Erhaltungsmodell des BSI. Beim BS7799-2 handelt es sich um ein iteratives Qualitätsmodell, das eine kontinuierlichen Verbesserung des Informationssicherheitsniveaus anstrebt. Hierzu gibt es die Methoden der „Präventive/Corrective Action“, die in der vierten Phase (A = Act) angesiedelt sind. Somit steuert das ISMS die Security-Policy im Unternehmen, erhält das notwendige IT-Sicherheitsniveau und verbessert es kontinuierlich. Allerdings gibt es bisher noch keine Metrik, um die Güte eines ISMS festzustellen. Es wurden weder Leistungsindikatoren oder Qualitätsmesspunkte de-

Abb. 5: Aufbau eines ISMS im PDCA-Cycle.



finiert, noch kann eine Messung der Effektivität eines umgesetzten ISMS vorgenommen werden. Allerdings hat die ISO eine spezielle Arbeitsgruppe (die ISO/IEC JTC 1/SC 27) ins Leben gerufen, die sich mit Metriken der ISO 17799 beschäftigt. Ein Ergebnis ist aber wahrscheinlich nicht vor 2007 zu erwarten.

Da das IT-Grundschutzmodell ein IT-Sicherheitsmanagement in den Fokus stellt, wohingegen die IT-Governance eine umfassendere Forderung an die Unternehmen stellt, ist es in diesem Zusammenhang nur bedingt hilfreich. Außerdem schließt das ISMS bereits das IT-Sicherheitsmanagement ein. Damit wird deutlich, dass für die IT-Governance ein System, das lediglich die IT-Sicherheit betrachtet und keine direkte Beziehung zu den Geschäftsprozessen vorsieht, eher nachrangig hinzugezogen werden sollte

Beurteilungsbereiche eines ISMS

Um die Güte eines realen ISMS zu beurteilen, sind der Sicherheitsprozess und die Security-Policies Policy auf den verschiedenen Ebenen, die Güte der entwickelten Sicherheitskonzepte und Sicherheitsarchitekturen sowie die operationellen Sicherheitsmaßnahmen und die operativ eingesetzten Werkzeuge zu betrachten. Ferner ist von Bedeutung, wie das ISMS in das Planungssystem des Unternehmens integriert ist, und mit welchen monetären und personellen Ressourcen es ausgestattet ist. Damit ist zwar auch relevant, welcher Ansatz oder welche Ansätze verfolgt werden (etwa BS7799, ITIL, IT-GSHB, CoBIT oder COSO), deren Kenntnis reicht jedoch allein nicht zur Beurteilung aus und sie sagen erst recht nichts über eine adäquate Ressourcenausstattung aus.

Um den Beurteilungsbereich eines ISMS festlegen zu können, ist es erforderlich, den Begriff des ISMS exakt zu definieren. Da insbesondere die IT vielfach ausgegliedert und ausgelagert wird, ist hinsichtlich der Reichweite eines ISMS der Trend der Konzentration auf Kernkompetenzen und der Ausgliederung und Auslagerung der anderen Leistungsbereiche zu beachten. Diesen strukturellen Veränderungen wurden bereits bei der Novellierung der ISO/IEC 17799 Rechnung getragen. Unter Berücksichtigung dieser Entwicklungen wird an dieser Stelle folgende Definition vorgeschlagen:

„Ein ISMS hat die Aufgabe, die Sicherheit arbeitsteiliger und unternehmensübergreifender Geschäftsprozesse aufgrund möglicher Fehler

und Schäden hinsichtlich des Zielniveaus in allen relevanten Dimensionen der Sicherheit festzulegen und die Erreichung dieser Ziele mittels geeigneter Vorgaben, Konzepte, Architekturen und operativer Maßnahmen sicherzustellen. Mittels Kontrollen sind Zielabweichungen durch externe oder interne Umstände zu erkennen und Gegenmaßnahmen zu ergreifen."

Damit wird ein Beurteilungssystem notwendig, das als Maßstab für die Zusammenarbeit gerade im Bereich der Liefer- und Leistungsbeziehungen mit anderen Unternehmen und Organisationen einsetzbar ist. Dieser Maßstab muss sowohl für große als auch kleine Unternehmen geeignet sein. Weiterhin ist das Beurteilungssystem so aufzubauen, dass es die Struktur des Realsystems ausreichend genau widerspiegelt. Grundsätzlich sind hierfür Kennzahlensysteme geeignet, welche die unterschiedlichen Ebenen und Bereiche in ihrem logischen Zusammenhang repräsentieren. Damit ist zunächst die Struktur eines geeigneten Beurteilungssystems zu entwerfen.

Struktur eines Beurteilungssystems

Ausgehend vom BS7799 und den dort beschriebenen Dokumentationspflichten für ein Unternehmen kann ein Framework zur Qualitätssicherung definiert werden und als Grundlage für ein Beurteilungssystem dienen. Unter Qualität kann in Anlehnung an CobiT die Effektivität (Wirksamkeit) und Effizienz (Wirtschaftlichkeit) verstanden werden [ISACA 2002]. Weiterhin ist der BS7799-2:2002 in enger Verzahnung mit der ISO 9001:2000 und dem dort definierten Qualitätsmanagementsystem (QM) entstanden [CEN 2002]. Nach der ISO 9001:2000 werden die Geschäftsprozesse beschrieben, jedoch nicht nach Bedeutung oder Kritikalität bewertet.

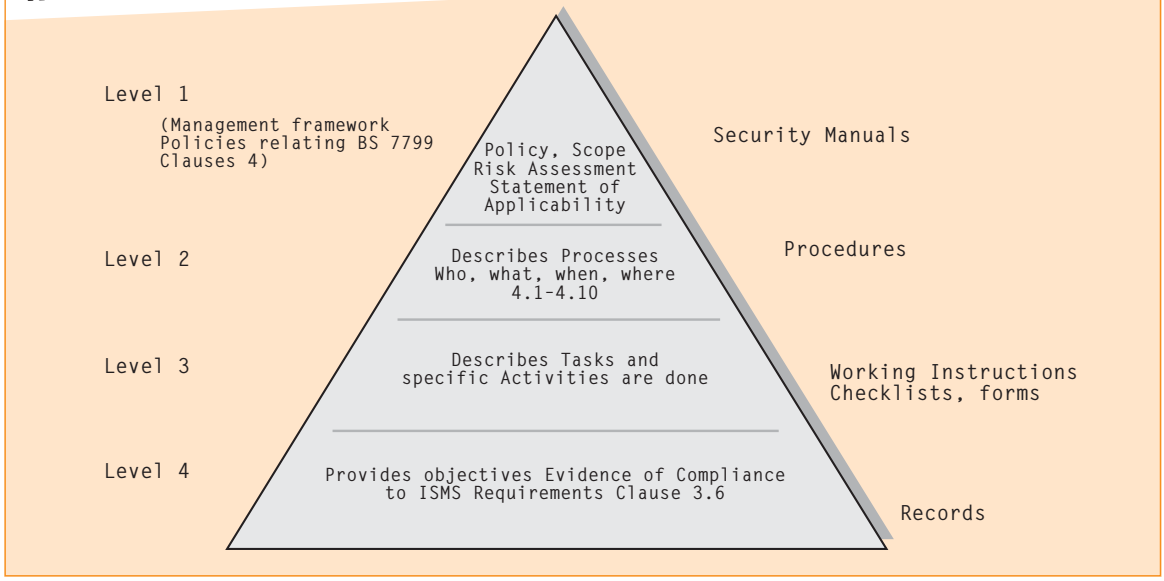
Genau hier setzt BS7799-2 an. Diejenigen Prozesse, die maßgeblich zum Geschäftserfolg beitragen, werden besonders behandelt. Damit findet aus Sicht des BS7799-2 eine Abstufung der Geschäftsprozesse statt. Die Dokumentation ist im BS7799 gemäß Clauses 4 zwingend vorgeschrieben und sieht vier verschiedene hierarchische Ebenen ($\lambda 1, \ldots \lambda 4$) vor. Diese vier Ebenen (Level) entsprechen den Ebenen der Security-Pyramide. Ergänzt werden müssen lediglich Beurteilungsgrößen für diese Ebenen. Aus der Literatur lassen sich zwei Gruppen solcher Größen als zweckdienlich ableiten. Zum einen sind es Bewertungsgrößen, mit denen Veränderungen (Leistungsindikatoren) – vornehmlich von Prozessen – beschrieben werden, zum anderen sind es Größen, mit denen eine Zielerreichung (Erfolgsfaktor) bewertet wird [Kütz 2003]. Dabei sind die letztgenannten statusorientiert. Nach ähnlichen Kriterien wird zum Beispiel typischerweise eine ITIL-Implementierung – oder im Bereich der Revision mittels CobiT – eine Bewertung der IT vorgenommen [ISACA 2002].

Als Voraussetzung einer Beurteilung eines ISMS wird angenommen, dass sich seine relevanten Eigenschaften durch die Beurteilung von Prozessen und kritischen Erfolgsfaktoren messen lassen. Dabei wird ein Prozess als eine logisch zusammenhängende Reihe von Aktivitäten zur Erreichung eines vorab definierten Ziels aufgefasst. Der Prozess muss also grundsätzlich zum Erreichen des Zieles geeignet sein, das heißt: er muss effektiv sein. Weiterhin lassen sich quantitative Leistungsindikatoren (Key Performance Indicators, KPI) in Form von Variablen ableiten, anhand derer sich der Fortschritt hinsichtlich wichtiger Zielsetzungen oder kritischer Erfolgsfaktoren innerhalb eines ISMS ableiten lässt. Setzt man diesen Fortschritt in das Verhältnis zu den dazu benötigten Ressourcen, so erhält man ein Maß für die Effizienz des ISMS. Hier setzen neue Überlegungen an, die eine ebenenbezogene Betrachtung (Level) vorsehen. Erste Ergebnisse dieser aktuellen Forschungsarbeiten sind noch 2005 zu erwarten.

Reifegradbetrachtungen als alternativer Beurteilungsmaßstab eines ISMS

Eine alternative Möglichkeit, ein ISMS zu beurteilen, kann beispielsweise durch ein Reifegradmodell (Capability Maturity Model, CMM) vorgenommen werden. Hierzu liegen etwa für die Softwareentwicklung weit reichende Vorschläge von der Carnegie Mellon University vor [CMMSEI 2002]. Außerdem existiert ein Vorschlag für ein CMM der Informationssicherheit vom National Institute of Standards (NIST) in den USA [NIST 2003]. Im Kern wird – ebenso wie im Ursprungsmodell – ein fünfstufiges Reifegradmodell in der Ausprägung eines iterativen Optimierungsmodells entworfen, um den Zustand (Reifegrad) des zu betrachtenden Systems zu beurteilen. Als das entscheidende Beurteilungskriterium dienen dabei die Prozesssicht und die Möglichkeit der Nachvollziehbarkeit sowie die Prozesstreue. Nach diesem Modell kann ebenso eine Implementierung von CoBiT als auch ITIL beurteilt werden. Denn bei allen genannten Verfahren handelt es sich im Kern um prozessorientierte Verfahren.

Abb. 6: Struktur der Dokumentation nach BS7799-2



Die Beurteilungskriterien des Reifegradmodells scheinen allerdings unschärfer als ein Beurteilungssystem nach konkreten Messgrößen wie beispielsweise für die Effektivität und Effizienz. Ebenso sagt das Reifegradmodell nichts bezüglich der Wirtschaftlichkeit eines ISMS aus. Aus der Perspektive der IT-Governance und der damit zuhängenden notwendigen Führungs- und Beurteilungsverantwortung der IT, der IT-Prozesse sowie der IT-Sicherheitsprozesse ist ein reines Reifgradmodell nur indirekt geeignet.

Fazit

Vor dem Hintergrund des IT-Governance wurde zunächst das herrschende Security-Paradigma diskutiert. Anschließend wurden zwei bedeutende Sicherheitsmodelle (BSI-Grundschutzmodell und BS 7799) dargestellt und hinsichtlich ihrer Unterstützung zur IT-Governance bewertet. Es hat sich herausgestellt, dass ein prozessorientiertes und auf die Geschäftsprozesse ausgerichtetes ISMS deutliche Vorteile hinsichtlich der IT-Governance-Unterstützung gegenüber einem reinen Erhaltungsmodell bietet. Metriken zur Messung der Effektivität und Effizienz eines ISMS sind derzeit noch nicht verfügbar. Ansätze wie CoBiT greifen nach ersten Einschätzungen zu kurz, denn vor einer praktischen Nutzung müssten die eigentlichen Kennzahlen erst detailliert definiert werden. ■

Literaturverzeichnis: KES/KPMG [Hrsg.]: Sicherheitsstudie 2002, Ingelheim 2002 / Böhmer, W.: VPN, die reale Welt der virtuellen Netze, 2. Aufl., München Juni 2005 / Biba, K.: Integrity Considerations for Secure Computer Systems, Technical Report MTR-3153, Bedford 1977 / Bishop, M.: Introduction to computer security, 2004 / Bishop, M.: Computer Security: Art and Science Pearson Education, Addison 7 Aufl. 2005 / Beuning, M.: Analyse und Bewertung verschiedener Methoden zur Ermittlung des IT-Betriebsrisikos anhand charakteristischer Kenngrößen., Diplomarbeit an der BA Mannheim/FB Informatik, Mannheim 2003 / Brewer, D.; Nash, M.: The Chinese Wall Security Policy, in: Proceedings of the 1989 IEEE Symposium on Security and Privacy, S. 206-214, 1989 / Bundesamt für Sicherheit in der Informationstechnik (BSI) [Hrsg.]: BS 7799 Part1 – Vergleich mit dem IT-Grundschutzhandbuch, Studie 2003, elektronisch veröffentlicht unter: http://www.bsi.de/gshb/deutsch/hilfmi/bs7799.htm, Stand: 20.08.2005 / Bundesamt für Sicherheit in der Informationstechnik (BSI) [Hrsg.]: IT-Grundschutzhandbuch – Standard Sicherheitsmaßnahmen, Köln 2004 / Britisch Standard Institute (BSI-GB) [Hrsg.]: BS 7799 Part 1:2002, Code of Practice for Information Security Management / Britisch Standard Institute (BSI-GB) [Hrsg.]: BS 7799 Part 2:2002, Information Security management System (ISMS) – Specification with guidance for use / Clark, D.; Wilson, D.: A Comparison of Commercial and Military Security Policies, in: Proceedings of the 1987 IEEE Symposium on Security and Privacy, S. 184-194, 1987 / CMMI Product Team [Hrsg.]: Capability Maturity Model Integration (CMMI) – CMMI for Systems Engineering and Software Engineering, Carnegie Mellon University, 2002 / ISACA [Hrsg.]: CoBiT Framework, Information System Audit & Control 3. Aufl. 2000 / ISO/IEC [Hrsg.]: ISO/IEC 17799:2005, Code of Practice for Information Security Management / Kairab, S.: A Practical Guide to Security Assessments, 2005 / Kütz, F. [Hrsg.]: Kennzahlen in der IT, Werkzeuge für Controlling und Management, 2003 / Matschke, K.-D.: Security-Quality-Management Handbuch – Grundsätze und Verfahren für umfassende Unternehmenssicherheit, Ingelheim 1998 / McLean, J.: A Comment on the „Basic Security Theorem" of Bell and LaPadula, in: Information Processing Letters 20(2), S. 67-70, 1985 / McLean, J.: Reasning About Security Models, in: Proceedings of the 1987 IEEE Symposium on Security and Privacy, S. 123-131, 1987 / NIST [Hrsg.]: National Institute of Standards, special document NI-800-55 / Petzel, E.: Managment der Informationssicherheit, Weiden-Regensburg 1996 / Schneewieß, W.: Zuverlässigkeitstheorie – Eine Einführung über Mittelwerte von binären Zufallsprozessen, Berlin/Heidelberg/New York 1973.