Ralf-T. Grünendahl | Andreas F. Steinbacher | Peter H.L. Will

Das IT-Gesetz: Compliance in der IT-Sicherheit

Aus dem Programm IT-Sicherheit und Datenschutz

ITIL Security Management realisieren
von Jochen Brunnstein

Elektronische Signaturen in modernen Geschäftsprozessen
von Volker Gruhn, Vincent Wolff-Marting, André Köhler, Christian Haase und Torsten Kresse

Der IT Security Manager
von Heinrich Kersten und Gerhard Klett

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz
von Heinrich Kersten, Jürgen Reuter und Klaus-Werner Schröder

IT-Sicherheit – Make or Buy
von Marco Kleiner, Lucas Müller und Mario Köhler

IT-Risiko-Management mit System
von Hans-Peter Königs

IT-Sicherheit mit System
von Klaus-Rainer Müller

Handbuch Unternehmenssicherheit
von Klaus-Rainer Müller

Trusted Computing
herausgegeben von Norbert Pohlmann und Helmut Reimer

Praxis des IT-Rechts
von Horst Speichert

IT-Sicherheit kompakt und verständlich
von Bernhard C. Witt

Ralf-T. Grünendahl | Andreas F. Steinbacher |
Peter H.L. Will

Das IT-Gesetz: Compliance in der IT-Sicherheit

Leitfaden für ein Regelwerk zur IT-Sicherheit im Unternehmen

PRAXIS

VIEWEG+
TEUBNER

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage 2009

Lektorat: Sybille Thelen | Andrea Broßler

Vieweg+Teubner ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: Krips b.v., Meppel
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in the Netherlands

ISBN 978-3-8348-0598-0

Vorwort

Im Rückblick der vergangenen 15 Jahre hat die IT-Sicherheitsfunktion in Unternehmen drastische Veränderungen erfahren. Gestartet zu Mainframe Zeiten als wenig beachtetes Thema mit dem Charakter einer Geheimwissenschaft ist IT-Sicherheit heute eine unverzichtbare Unternehmensfunktion, deren Effektivität gegenüber Dritten verpflichtend nachgewiesen werden muss. Mit diesem Wandel der Bedeutung hat sich auch das Herangehen an dieses Thema fortentwickeln müssen. Während in der Vergangenheit IT-Sicherheit vornehmlich mit dem Einsatz geeigneter Sicherheitstechnologien, sowie deren Bedienung und Kontrolle verbunden war, steht heute die nachhaltige und effiziente Aufrechterhaltung eines angemessenen Sicherheitsniveaus im Vordergrund. Der Forderung nach Nachhaltigkeit und Effizienz wurde begegnet, indem zunächst Vorgehensweisen und Methoden des IT-Risikomanagements in die Methoden der IT-Sicherheit integriert wurden. Gleichzeitig rückte das Management der IT-Sicherheitsfunktion gegenüber ihrer operativen Rolle stärker in den Vordergrund. Es wurden IT-Sicherheitsmanagement-Prozesse definiert und standardisiert. Auf dieser Basis besitzen wir heute das theoretische und praktische Rüstzeug für das professionelle Management der IT-Sicherheit in Unternehmen. Dennoch konnten bei weitem nicht alle Unternehmen mit dieser Evolution der IT-Sicherheit Schritt halten. Branchen, deren Kernwertschöpfung eng mit dem Einsatz von Informationstechnologie verbunden ist, haben hier oft den höchsten Reifegrad erreicht, was sich durch deren extreme Abhängigkeit von Informationstechnologien erklärt. Andere Branchen werden hier folgen, da auch deren Abhängigkeit von Informations- und Kommunikationstechnologien stetig steigt. Das hier vorliegende Buch kann aus unserer Sicht einen wertvollen Beitrag zu einer Professionalisierung des Umgangs mit IT-Sicherheit und dem Management der IT-Sicherheitsfunktion im Unternehmen sein, indem es die wesentlichen Facetten des modernen IT-Sicherheitsmanagements zusammenfasst.

Dr. Bernd Eßer
Head of Group
ICT Risk & Security Management

Detecon International

Dr. Thomas Götz
Head of Practice
Information Technology Management
Detecon International

Ralf-T. Grünendahl und Andreas F. Steinbacher sind Mitarbeiter der EDS Business Solutions. Peter H.L. Will steht in Diensten der DETECON International. Die drei Autoren befassen sich seit Jahren in Kundenprojekten mit Regulierungsfragen (SOX, Basel II) sowie Risikomanagement und den daraus folgenden Implikationen für die IT und insbesondere für IT-Sicherheit.

Ralf-T. Grünendahl und Peter H.L. Will sind die Authoren von ‚Beyond Compliance - 10 Practical Actions on Regulation, Risk and IT-Management'.

Die Autoren danken ihren Kollegen für ihre Beiträge und Anregungen zu diesem Buch. Besonderer Dank gilt Andrea Ritschel, Moritz Klingholz und Michael Weissing.

Inhalt

1 Einleitung

Die Anzahl der IT-Systeme, die wichtige Unternehmensdaten halten oder die einen wichtigen Beitrag zur Geschäftstätigkeit eines Unternehmens leisten, nimmt ständig zu. Gleichzeitig nimmt die räumliche Verteilung dieser Systeme zu. Standorte müssen miteinander verbunden werden, Daten werden auf mobilen Geräten gehalten, wichtige Anwendungen beispielsweise des Vertriebes laufen auf mobilen Geräten. Schließlich sind immer mehr dieser IT-Systeme mit dem Internet verbunden um für das Unternehmen und seine Kunden die Vorteile diese Form der Kommunikation nutzbar zumachen.

Diese verteilte Haltung und die Mobilität von Daten erfordern, dass der Schutz dieser Daten und ihrer Kommunikationswege eine immer höhere Bedeutung erhält. Im Kapitel ‚Bedeutung der IT-Sicherheit in Unternehmen' werden wir exemplarisch auf einige der Bedrohungsszenarien eingehen. Die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität von Daten und der Systeme zu ihrer Speicherung und Verteilung sind mittlerweile so hoch einzuschätzen, dass das Thema IT-Sicherheit in Diskussionen einen Spitzenplatz einnimmt. Dabei wird der unbedarfte und auch professionelle Teilnehmer an diesen Diskussionen mit Begriffen und Inhalten überschüttet, die einer Erklärung und Erläuterung bedürfen und die es in einen sinnvollen Zusammenhang zu stellen gilt. Wir haben es uns mit diesem Buch zur Aufgabe gemacht, diesen Zusammenhang herzustellen.

Dieses Buch gibt den Begriffen, Inhalten und Zusammenhängen der IT-Sicherheit eine Struktur. Durch dieses Buch werden die Begriffe

- IT-Sicherheit und IT-Sicherheitsmanagement
- Sicherheitsziele und Sicherheitskonzept
- IT-Grundschutz, Schutzbedarfsfeststellung und Sicherheitsanalyse
- IT-Sicherheitsbeauftragte und IT-Sicherheitsrichtlinie,
- Sicherheitsreporting und IT-Sicherheitsorganisation,
- Datenschutz und Datensicherungskonzept
- Zutritt, Zugang und Zugriff
- K-Fall Handbuch, Business Continuity, Disaster Recovery

und viele mehr in einen sinnvollen Kontext überführt.

Die Struktur, die wir für diesen Zweck gewählt haben, ist mit einem Gesetzeswerk vergleichbar. Deshalb haben wir das Buch das ‚IT-Gesetz' genannt: Die Inhalte sind grundlegender Natur uns sollten in jedem Unternehmen auf eine vergleichbare Weise geregelt werden. Der Aufbau ist hierarchisch, ausgehend von einem übergeordneten Rahmenwerk, der ‚IT-Sicherheitspolicy' als einer Art Verfassung, hin zu detaillierteren Durchführungsgesetzen und schließlich einzelnen Arbeitsanweisungen.

Damit wendet sich dieses Buch sowohl an

- Manager, die vor der Herausforderung stehe, die Sicherheit in der IT ihres Unternehmens zu gewährleisten, als auch an
- IT Fachleute, die zwar die Inhalte und Begriffe kennen, aber auf der Suche sind nach einer Struktur, um die Dinge, von denen sie wissen, das sie richtig sind, auch in ihrem Unternehmen zu verankern.

Dieses Buch liefert komplette Lösungen für die notwendige Dokumentation aller sicherheitsrelevanten Aspekte der IT. Der IT-Sicherheitsbeauftragte und alle anderen mit der IT-Sicherheit beschäftigen Personen eines Unternehmens erhalten hiermit eine Vorlagensammlung, die (auf die speziellen Bedürfnisse einer Firma angepasst) ein umfassendes Regelungswerk zur IT-Sicherheit bilden, das auf bewährten Standards aufsetzt und als Startpunkt für die Entwicklung einer audit-fähigen Dokumentation zur IT-Sicherheit gelten kann.

Gesetzliche und regulatorische Vorgaben

Aus verschiedensten Rechtsvorschriften lassen sich Handlungsverpflichtungen oder sogar Haftungsrisiken für Unternehmensführer ableiten, wenn sie der Sicherheit der IT ihres Unternehmens nicht die notwendige Aufmerksamkeit und Führsorge widmen. Dies gilt sowohl für Geschäftsführungen von GmbH also auch für Vorstände von Aktiengesellschaften.

Insbesondere das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ergänzt das bestehende Handelsgesetzbuch und das Aktiengesetz um die Forderung nach einem Risikomanagement für Kapitalgesellschaften. Aktiengesellschaften und GmbHs unterliegen damit einer Reihe von neuen Verpflichtungen:

- Ein Vorstand haftet persönlich, wenn er Entwicklungen, die zukünftig ein Risiko für das Unternehmen darstellen könnten, nicht durch ein Risikomanagement überwacht und durch geeignete Maßnahmen vorbeugt (§ 91 Abs. 2 und § 93 Abs. 2 AktG).

- Geschäftsführern einer GmbH wird im GmbH-Gesetz „die Sorgfalt eines ordentlichen Geschäftsmannes" auferlegt (§ 43 Abs. 1 GmbHG).
- Die im Aktiengesetz genannten Pflichten eines Vorstands gelten auch im Rahmen des Handelsgesetzbuches (§ 317 Abs. 4 HGB). Weiterhin verpflichtet das Handelsgesetzbuch Abschlussprüfer zu prüfen, „ob die Risiken der künftigen Entwicklung zutreffend dargestellt sind" (§ 317 Abs. 2HGB).
- Die Bundesregierung hat im Jahr 2007 ein Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (StrÄndG) beschlossen. Damit wurden neue Straftatbestände für das Ausspähen und Abfangen von Daten und für diesbezügliche Vorbereitungshandlungen geschaffen.

Der Umgang mit personenbezogenen Daten wird zusätzlich in den Datenschutzgesetzen (Bundes und Länder), dem Gesetz über den Datenschutz bei Telediensten und der Telekommunikations-Datenschutzverordnung geregelt.

Auch aus dem Verbraucherschutz lassen sich Handlungsnotwendigkeiten in Bezug auf die Sicherheit der Unternehmens-IT ableiten. Die Verwendung von Informationstechnik, die Nutzung des Internets oder von Telekommunikationsdiensten werden im Gesetz zur Nutzung von Telediensten, im Telekommunikationsgesetz, im Mediendienste-Staatsvertrag und im Urheberrecht zum Teil sehr genau geregelt.

Doch nicht nur die Verpflichtungen, die das Unternehmen selbst betreffen, legen große Sorgfalt im Umgang mit den Risiken der IT nahe. Darüber hinaus existieren Vorschriften, die die Sicherheit der IT für ein Unternehmen zum kritischen Erfolgsfaktor werden lassen. Banken sind beispielsweise gemäß Basel II gezwungen, sogar bei der Vergabe von Krediten die Risiken der IT des Kreditnehmers zu berücksichtigen, da der nach dem Baseler Ausschuss für Bankenaufsicht erarbeiteten Konzept bei der Vergabe sowohl Markt- und Kreditrisiken als auch operationelle Risiken des Kreditnehmenden Unternehmens eine Rolle spielen sollen. Zu den operationellen Risiken eines Unternehmens zählen auch die Risiken, die sich aus dem Einsatz von Informationstechnologie in den Unternehmensprozessen ergeben. Ein aktives IT-Risiko-Management, das sich mit allen Aspekten der IT-Sicherheit für das jeweilige Unternehmen befasst, wird als wichtige Vorraussetzung gefordert. Darüber hinaus werden Kriterien wie die Redundanz wichtiger IT-Systeme, gesicherte Verfügbarkeiten, Existenz von Notfallplänen oder wirksame Abwehrmaßnahmen gegen Angriffe auf die IT-Systeme von innen und außen gefordert.

Dann ist da schließlich noch die große Keule: Die amerikanische Gesetzgebung, die unter dem Namen SOX, SOXA oder SARBOX so viel Furore gemacht hat. Im Sog der Bilanzskandale von Großunternehmen, hat der amerikanische Kongress im Juli 2002 den Sarbanes-Oxley Act verabschiedet. Dessen Ziel ist es, die Wiederholung einer solchen Krise zu vermeiden und das Vertrauen der Öffentlichkeit in Amerikas Finanzberichterstattung wiederherzustellen. Jedes Unternehmen, dessen Aktien an einer U.S.-amerikanischen Börse gehandelt werden, unterliegt ‚Sarbanes-Oxley'.

Der Sarbanes-Oxley Act ist ein weitreichendes Gesetz mit vielen Facetten – inklusive Strafmaßnahmen für leitende Angestellte von Unternehmen. Das Management soll – sowohl in seinem internen Bericht, als auch in der Stellungnahme des Wirtschaftsprüfungsunternehmens – eine schriftliche Feststellung zur Effektivität der internen Kontrollen zur Finanzberichterstattung treffen.

Viele der Detaillierungen der Implementierung von SOX wurden an die Securities and Exchange Commission (SEC) zur Ausgestaltung gegeben. Besonderes Augenmerk verdient Section 404, die mit „Management Assessment of Internal Controls" überschrieben ist. Im Kommentar der SEC zu Section 404 heißt es:

„Wir denken, dass der Zweck interner Kontrollen und Verfahren für die Finanzberichterstattung darin besteht Gewissheit zu schaffen, dass Unternehmen Prozesse gestaltet haben, die angemessen sicherstellen, dass die Rechnungslegung im Einklang mit den allgemein anerkannten Buchhaltungsprinzipien konform geht: Die Geschäftsvorfälle des Unternehmens sind verfahrensgemäß autorisiert; das Anlagevermögen des Unternehmens ist abgesichert gegen unautorisierte missbräuchliche Verwendung; die Geschäftsvorfälle des Unternehmens werden verfahrensgemäß aufgezeichnet und gemeldet."

Von den Forderungen der SEC betroffen sind damit aber auch Prozesse, die über die Erstellung der Rechnungslegung hinausgehen. Jeder Geschäftsprozess, der Geschäftsvorfälle des Unternehmens autorisiert, Anlagevermögen des Unternehmens nutzt, Geschäftsvorfälle aufzeichnet oder meldet, muss angemessen gestaltet sein. Dies dürfte die Mehrzahl aller Prozesse sein. Und damit ist vor allem auch die IT immer mit im Boot.

Derzeit hitzig diskutiert wird ob eine vergleichbare Gesetzgebung auch auf Europa übertragen werden sollte, oder ob eventuell die bestehenden gesetzlichen Vorschriften bereits in vergleichbarer Weise gedeutet werden könnten und sollten.

2 Bedeutung der IT-Sicherheit in Unternehmen

Es ist nicht nur die Legislative (also eigentlich die Guten), die Unternehmensführung und IT-Leitung in den letzten Jahren vor sich hertreiben. Es sind auch die Bösen, nämlich Hacker, Betrüger oder Erpresser, die ihnen schlaflose Nächte breiten. Oder jedenfalls bereiten sollten:

- In einer Befragung des Landeskriminalamtes und der IHK bei 2000 Unternehmen in Schleswig-Holstein gaben immerhin 39 Prozent an, innerhalb der letzten sechs Monate Opfer eines Angriffs geworden zu sein, teilweise mehrfach. Weitere 20 Prozent gaben an, nicht zu wissen, ob sie angegriffen worden sind! Bei 8 Prozent der Befragten – also 20 Prozent der betroffenen Unternehmen – kam es dabei zu Datenverlusten bzw. finanziellen Schäden.
- Nach Angaben von Websense, Hersteller von Sicherheitsprodukten, sind bereits in jedem fünften Unternehmen PCs mit Keyloggern infiziert, die die Tastatureingaben des Benutzers mitlesen, um an Passwörter und vertrauliche Informationen zu gelangen. Einige Keylogger-Varianten fertigen Screenshots an und versenden diese. Die Betrüger können dann später eine komplette Session inklusive Nutzereingaben ‚nachspielen'. Wenn inzwischen aber jedermann im Internet Spyware erwerben kann mag es nicht mehr verwundern, wenn sogar 92 Prozent der von Websense befragten IT-Entscheider vermuten, dass ihr Netz in den vergangenen zwölf Monaten mit Spyware infiziert war ohne es zu merken. Nicht umsonst lässt das Pentagon angeblich seine Netzwerke, die 20 Prozent des gesamten Internet darstellen, 6 Millionen Mal täglich nach Sicherheitslücken absuchen.
- Penguin Software hat ermittelt, das 27 Prozent aller E-Mails, die von Google Mailaccounts versendet werden, SPAM sind. Noch drastischer sind Aussagen von MessageLabs, die bereits im Jahr 2006 drei Viertel aller E-Mails als SPAM einstuften, was auch an der Ausbreitung von mailversendenden Trojanern läge. Inzwischen, so MessageLabs weiter, seien ca. 1% der E-Mails virenverseucht und jede 200ste E-Mail eine Phishing-Mail.

Websense sieht ein wesentliches Problem darin, das Mitarbeiter glauben, am Arbeitsplatz-PC besser vor Angriffen geschützt zu sein, und daher leichtfertiger auf Links und Anhänge klicken. 44 Prozent der Mitarbeiter sind nach Meinung der IT-Verantwortlichen nicht in der Lage sein, eine Phishing-Seite zu erkennen. Laut Anti-Phishing Working Group waren beispielsweise im May 2007 mehr als 37.000 Phishing Webseiten online. Inzwischen sei die Zahl der Phishing-Angriffe rückläufig, dafür nehme aber die Zahl der Webseiten mit Trojanern zu. Von 6500 URLs wurde im März diesen jahres Crimeware (Keylogger etc) verteilt. Allein in Deutschland habe Geheimzahlenklau 19 Million Euro Schaden im Jahr 2007 verursacht, hat Bitkom hochgerechnet. Bitkom zählt aktuell 25.000 gefälschte Bank-Webseiten.

- Der durch Viren, Spyware und Hackerangriffe verursachte Schaden in britischen Unternehmen beträgt laut einer Studie von PricewaterhouseCoopers jährlich rund 10 Milliarden Pfund.

  Mittlerweile setzen zwar 98 Prozent der Firmen Antiviren-Lösungen ein, allerdings sei ein Viertel gegen Spionageversuche durch Spyware ungeschützt. Die Kosten für einen Vorfall in großen Unternehmen beziffert PWC zwischen 65.000 und 130.000 britischen Pfund. Über alle Unternehmen liegt dieser Wert zwischen 8.000 und 17.000 Pfund.

- Computerwürmer werden immer zunehmend nicht dazu programmiert, direkt irreparable Schäden anzurichten. Angreifer versuchen vielmehr, so warnt das BSI, den befallenen Rechner für einen kontinuierlichen Missbrauch unter ihre Kontrolle zu bringen. Mit Hilfe Trojanischer Pferde missbrauchten Hacker oft mehrere tausend PCs und vermieteten diese so genannten Bot-Netze für kriminelle Zwecke, z.B. zur Verbreitung neuer Epidemien von Computerschädlingen, für DDoS-Attacken oder Versand von Spam.

- Arbor networks hat den Datenverkehr zwischen 70 Internet Providern analysiert und dabei 1.300 DDoS Attacken pro Tag gezählt, was 2 Prozent des Gesamtverkehres ausmacht. Noch erschreckender sind die Zahlen des Sicherheitssoftware-Herstellers Symantec. Der registrierte alleine bei seinen Kunden schon im zweiten Halbjahr 2006 durchschnittlich 5.200 DoS-Attacke pro Tag, ein deutlicher Rückgang gegenüber 6.100 Angriffen im ersten Halbjahr des selben Jahres. Wohlgemerkt: Täglich! Für die Zukunft erwarten die Experten des Georgia Institute of Technology die ersten Bot-DDoS Angriffe auf Mobilfunknetze.

- Doch die Probleme werden nicht nur von Externen verursacht. Zum Teil helfen die Unternehmen eben auch selbst kräftig mit. Das jedenfalls ist das Resultat einer Umfrage unter über 100 deutschen IT-Führungskräften, die die Compuware Corporation in Zusammenarbeit mit NIFIS (Nationale Initiative für Internet-Sicherheit) durchgeführt hat. Laut dieser Umfrage ist es mit dem Datenschutz in deutschen Unternehmen nicht zum Besten bestellt. Der Befragung zufolge nutzen 64 % der Entscheidungsträger echte Kundendaten für Anwendungstests. Das ist zunächst einmal laut Bundesdatenschutzgesetz – Stichwort Zweckbindung – nicht erlaubt. Doch dieses Gesetz, das seit 1990 gilt, kennen nach eigenem Bekunden 36% der Befragten nicht hinreichend. Zudem kann es, wenn solche Daten in die falschen Hände geraten, erheblichen Schaden, nicht nur im Hinblick auf die Reputation des Unternehmens, anrichten. Immerhin schließen 53% der Befragten mit externen Dienstleistern bei der Vergabe von Softwaretests Vertraulichkeitsvereinbarungen ab.
- Schließlich noch dies: Hätten sie gedacht, das allein am Frankfurter Flughafen im letzten Jahr 1.500 Notebooks vergessen wurden? Und das in Zügen der Deutschen Bahn fast 700 Notebooks gefunden und abgegeben wurden, von den nicht gemeldeten Fällen gar nicht zu reden? Leider ist nicht bekannt, wie viele dieser Rechner eine Festplattenverschlüsselungssoftware installiert hatten.

Fragt man die Unternehmen, worin sie die größten gefahren sehen, so zeigt sich konsequenterweise, das das Risiko unbefugter Kenntnisnahme bzw. Informationsdiebstahl deutlich geringer eingeschätzt wird, als die Risiken durch Viren und Trojaner oder auch durch Irrtümer und Nachlässigkeiten der eigenen Mitarbeiter.

Die nachfolgende Tabelle zeigt, welche Gefährdungsszenarien den Unternehmen am immanentesten erscheinen.

Gefahrenbereich	Bedeutung heute	Prognose	Schäden	
	Rang	Rang	Rang	Ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	2	1	49%
Malware (Viren, Würmer, Trojaner etc)	2	1	4	35%

Gefahrenbereich	Bedeutung heute	Prognose	Schäden	
Softwaremängel, -defekte	3	5	2	46%
Hardwaremängel, -defekte	4	6	3	45%
Unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	5	3	7	12%
Unbeabsichtigte Fehler von Externen	6	7	5	30%
Hacking (Vandalismus, Probing, Missbrauch etc)	7	4	8	12%
Mängel der Dokumentation	8	9	6	20%
Manipulation zum Zwecke der Bereicherung	9	8	10	11%
Höhere Gewalt (Feuer, Wasser etc)	10	11	9	12%
Sabotage (inkl. DoS)	11	10	11	10%
Sonstiges	12	12	12	3%

Bedeutung der Gefahrenbereiche für deutsche Unternehmen (Quelle: Lage der IT-Sicherheit in Deutschland, BSI 2007)

Zum Teil lässt sich diese Wahrnehmung durch eine Analyse der tatsächlich erfolgten Sicherheitsverstöße erklären, die in der folgenden Übersicht dargestellt sind. Dabei gilt es jedoch zu bedenken, das es sich hierbei um die bekannt gewordenen bzw. bemerkten Fälle handelt.

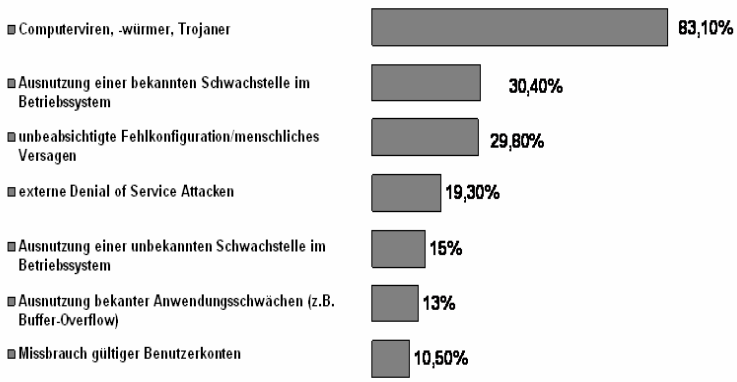

Abbildung 2–1: Verbreitung von Angriffsmethoden in deutschen und schweizerischen Unternehmen (Quelle: BSI)

Oft werden Trojaner und mehr noch Würmer als Kavaliersdelikt von Hobby-Anarchisten wahrgenommen, oder sogar als eigentlich ehrenwerter Kampf des Gallischen Dorfes gegen das Microsoft-Imperium. Zugegebenermaßen entbehren Fälle wie der des in Israel ansässige Anti-Spam-Start-up Blue Security auch nicht einer gewissen Ironie. Blue Security, wie gesagt ein Unternehmen das sein Geschäftsmodell in der Abwehr von Spammails für seine Kunden sieht, musste seine Dienste unter dem Druck eines andauernden verteilten Netzwerkangriffes eines Spammers einstellen. Der laut Online-Magazin Wired News von dem Spam-Versender PharmaMaster gestartete DDoS-Angriff legte zunächst die Datenbank-Server und somit die Website von Blue Security lahm. An die Adressen der ebenfalls von dem Angriff betroffen Kunden konnte der Spammer zudem wohl gelangen, indem er prüfte, welche E-Mail-Adressen in den vergangenen Monaten von Spam-Listen gestrichen wurden. Blue Security setzt zum Streichen der Adressen seiner Kunden auf das so genannte Opt-Out-Verfahren. Dabei veranlasst der Empfänger einer unerwünschten Werbe-Mail selbst, dass seine Adresse von einer Spam-Liste gestrichen wird. Die dafür entwickelte Software läuft auf den Rechnern der Kunden und liefert dem Unternehmen Rückmeldung über erhaltenen Spam. Dieses Vorgehen war zwar wohl erfolgreich, brachte dem kleinen Start-up jedoch auch Kritik ein: Die massenhaften Opt-out-Anfragen würden einem DDoS-Angriff gleichen und verstießen damit unter Umständen sogar gegen nationales Recht.

Das sympathisierende Lächeln vergeht jedoch sicher schnell, wenn man die Konsequenzen dieser Attacke bedenkt. Der von einem Bot-Netz durchgeführte Distributed-Denial-Of-Service-Angriff (DDoS) betraf nicht nur die Server des Unternehmens, sondern auch die Mail- und Web-Server eines Teils der rund 500.000 Blue-Security-Nutzer. Diese wurden mit massenhaftem Spam und sinnlosen Web-Anfragen ebenfalls überhäuft.

Die Erfolge der Strafverfolgungsbehörden sind dagegen bisher eher symbolischer Natur, die ergangenen Urteile mal mehr, mal weniger abschreckend:

- Ein 20 Jahre alter "Botmaster" ist von einem Gericht in Kalifornien unter anderem wegen Beschädigung von staatseigenen Computern zu einer Haftstrafe von 57 Monaten und anschließend drei Jahren Bewährung verurteilt worden. Der geständige Delinquent war in rund 400.000 Computer eingedrungen (unter anderem der Weapons Division des United States Naval Air Warfare Center in China Lake und der Defense Information Systems Agency des US-Verteidigungsministe-

riums) und hatte diese zu einem von ihm kontrollierten Bot-Netz zusammengeschlossen. Den Zugang zu seinem Bot-Netz hatte der Mann zum Zwecke des Spam-Versands oder für DDOS-Attacken verkauft. Sein Erlös aus auf den infizierten Rechnern platzierter Adware betrug 60.000 US-Dollar.

- Ein russisches Gericht hat drei Online-Erpresser zu jeweils acht Jahren Haft und 3700 US-Dollar Geldstrafe verurteilt. Die Männer hatten mehrere internationale Internet-Firmen mit DDoS Attacken erpresst und um insgesamt über vier Millionen US-Dollar erleichtert. Insoweit man acht Jahre in russischen Gefängnissen als milde angesehen kann, hatten die Erpresser sogar Glück: Bei den insgesamt 19 Anklagepunkten wäre eine Höchststrafe von 15 Jahren möglich gewesen.

Ob nun gesetzliche Anforderungen, die Einsicht in die Fehlbarkeit der eigenen Mitarbeiter, die Furcht vor der kriminellen Energie begabter Informatiker oder auch der Glaube an Murphys Law der Anstoß sind: Um die Erkenntnis, das ein strukturiertes Vorgehen zur Gewährleistung von Sicherheit in der IT eines Unternehmens, bei der inzwischen Erreichten Abhängigkeit und dem Grad der Komplexität von IT, unabdingbar ist, kommt wohl kein vernunftbegabter Mensch mehr herum. Dieses Buch gibt dafür wichtige Hilfestellung.

3 COBIT und BSI als Leitschnur der IT-Sicherheit

In Anbetracht der wachsenden Bedeutung von IT in Unternehmen und der damit einher gehenden wachsenden Bedrohung von Unternehmensdaten stellen sich zunehmend mehr Führungskräfte die Frage, wie sie IT-Sicherheit in ihrem Unternehmen umfassend verankern könne. Dieses Buch liefert dazu ein Konzept, das von einer Unternehmens-Policy zu IT-Sicherheit auf einer obersten Ebene bis hinunter reicht zu Hinweisen für operative Arbeitsanweisungen. Wir stellen ganz konkrete Vorschläge zu Formulierungen solcher Richtlinien als Beispiel und Grundlage für die Erarbeitung einer auf die Bedürfnisse ihres Unternehmens zugeschnittenen Regelwerkes vor. Diese Vorschläge adressieren drei Ebenen:

- Auf der obersten Ebene steht eine grundlegende Policy des Unternehmens zu IT-Sicherheit. Darin wird definiert, welches die relevanten Regelungsinhalte sind und welche Zielvorgaben das Unternehmen zu diesen Themenbereichen setzt.
- Auf einer zweiten Ebene werden, basierend auf den Vorgaben der Policy und in enger inhaltlicher Verknüpfung, Richtlinien zu abgeschlossenen Sicherheitsthemen mit konkreten Sicherheitszielen definiert. Die Themenblöcke, zu denen eine umfassendes IT-Sicherheits-Framework Vorgaben machen muss, haben wir folgendermaßen gegliedert:
  - Schutz von Daten
  - IT-Sicherheitsmanagement
  - IT-Betrieb
  - IT-Systeme
  - Organisation
  - Service Management
  - IT Continuity

  Jedem dieser Themenblöcke ist ein eigenes Kapitel gewidmet.
- Auf der dritten Ebene stehen schließlich operative Dokumente, welche erläutern, wie die in den Richtlinien gesteckten Ziele konkret umgesetzt werden. Zu diesen Handlungsanweisungen, Prozessbeschreibungen etc können wir im Rahmen dieses

Buches nur Hinweise geben. Die konkrete Ausgestaltung hängt ganz von den konkreten Rahmenbedingungen ihres Unternehmens ab. Die Umsetzung der Richtlinien in solche operativen Dokumente sollte durch die hier vorgeschlagenen Regelungsinhalte angeleitet werden.

- Die folgende Übersicht zeigt die Hierarchie der in diesem Buch vorgeschlagenen Dokumente und gibt einen ersten Überblick über die dort behandelten Themen.

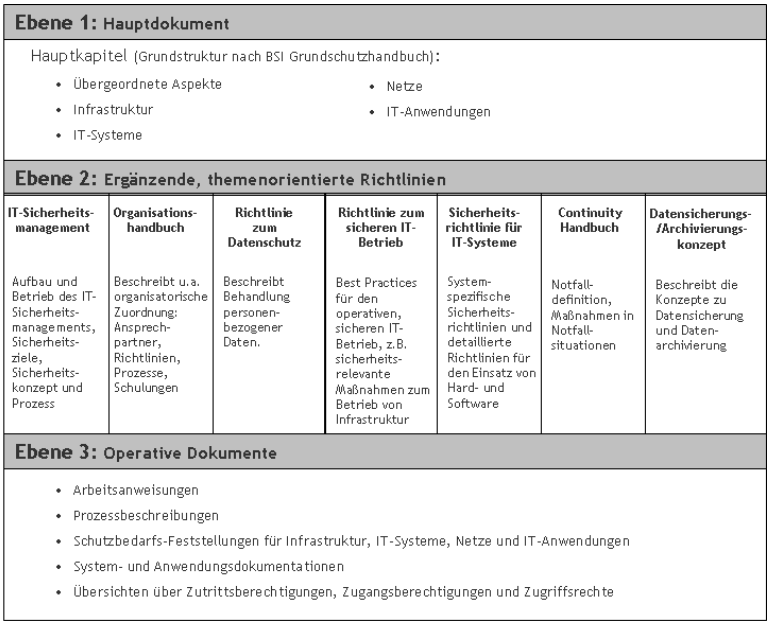

Abbildung 3–1: Dokumentenhierarchie der IT-Sicherheitsrichtlinien

Jedes Kapitel zu einem klar abgrenzbaren Bereich der IT-Sicherheit enthält einen konkreten Entwurf einer Richtlinie zu diesem Thema. Dieser Entwurf kann in kürzester Zeit für Ihr Unternehmen maßgeschneidert und in eine Ihren Belangen genügende Richtlinie umgesetzt werden. Die Policies und Richtlinien orientieren sich sehr stark an den Vorgaben des Grundschutzhandbuches des BSI. Die in diesem Standardwerk zusammengestellten umfangreichen Vorgaben und Maßnahmen haben wir auf die hier relevanten Bereiche eingegrenzt, entsprechend der verwendeten Dokumenthierarchie sortiert und in die Themenblöcke gruppiert.

Als ganzheitliches Konzept für IT-Sicherheit hat sich das Vorgehen nach IT-Grundschutz zusammen mit den IT-Grundschutz-

Katalogen des BSI als Standard etabliert. Es bietet sich daher an, die Bemühungen eines Unternehmens um Sicherheit in der IT auf diesen Vorgaben zu basieren. Das BSI formuliert den eigenen Anspruch folgendermaßen:

„BSI-Standards enthalten Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit. Das BSI greift dabei Themenbereiche auf, die von grundsätzlicher Bedeutung für die Informationssicherheit in Behörden oder Unternehmen sind und für die sich national oder international sinnvolle und zweckmäßige Herangehensweisen etabliert haben."

Das BSI orientiert sich selbst an internationalen Standards wie den ISO-Standards 13335, 17799 und 27001, deren sehr allgemeine Anforderungen das BSI mit seinen Vorschlägen, Hinweisen und Hintergrundinformationen operational machen will.

Allerdings ist der Regelungsumfang des BSI wiederum sehr weitreichend. Für dieses Buch haben wir uns daher auf die wesentlichen Inhalte beschränkt und diese für den Nutzer durch Neuordnung leichter zugänglich gemacht. Die weitergehenden Ausführungen des BSI in all seinen Verästelungen sind jedoch als Hilfestellung für die Definition der Handlungsanweisungen und Prozessbeschreibungen der dritten Ebene sehr empfohlen. Die vom BSI seit der Einführung 1994 laufend weiter entwickelten Methoden umfassen detaillierte Anweisungen zum

- Aufbau einer Sicherheitsorganisation zur Risikobewertung,
- Für die Überprüfung des vorhandenen IT-Sicherheitsniveaus sowie
- die Implementierung der angemessenen IT-Sicherheit.

Die IT-Grundschutz-Kataloge dienen zahlreichen Unternehmen und Behörden als Grundlage Ihrer Vorgehensmodelle.

Insbesondere im bereich der IT-Systeme liefern wir Ihnen bereits konkrete Vorschläge welche Detailregelungen zum Vorgehen in den Grundschutzmaßnahmen des BSI Ihr Unternehmen insbesondere berücksichtigen sollte. Das BSI selbst erläutert diese Maßnahmen wie folgt:

„In den IT-Grundschutz-Katalogen werden Standard-Sicherheitsmaßnahmen für typische IT-Systeme empfohlen. Das Ziel dieser IT-Grundschutz-Empfehlungen ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für

hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann."

Ein Grundgedanke dieses Buches ist die Ausrichtung der IT-Sicherheit an den relevanten Kernelementen anerkannter Standards. Neben dem Grundschutzhandbuch des BSI orientieren wir unsere Vorschläge zudem an den Kontrollzielen des Cobit Frameworks. Zum tieferen Verständnis des Zwecks und des notwendigen Regelungsumfanges ist jedem Richtlinienentwurf ein Kapitel vorangestellt, in dem aus den Vorgaben des Cobit Frameworks die wesentlichen Best-Practise-Vorgaben abgeleitet sind. Diese Ausführungen sollen auch die Detaillierung der jeweiligen Richtlinie in konkreten Handlungsanweisungen, Prozess- und Rollenbeschreibungen etc erleichtern, in dem sie das zu erreichende Ziel der angestrebten Sicherheitskontrollen beschreiben. Dabei muss nicht jeder Aspekt der aufgeführten Cobit Kontrollziele eines Kapitels durch die jeweilige Richtlinien dieses Kapitels abgedeckt werden. Die umfassende Berücksichtigung der Kontrollziele ergibt sich aus dem Zusammenwirken aller Richtliniendokumente.

COBIT wurde im Original vom IT Governance Institute in englischer Sprache publiziert. Die exklusive Genehmigung zur Übersetzung wurde der KPMG Österreich vom IT Governance Institute erteilt. Auf diese Übersetzung beziehen wir uns in unseren Referenzen.

Auch Cobit ist in Übereinstimmung gebracht worden mit anderen internationalen Standards und konzentriert sich auf die wesentlichen Erfordernisse, um ein angemessenes Management und eine angemessene Steuerung der IT umzusetzen. Insgesamt basiert Cobit auf mehr als 40 internationalen detaillierten IT-Standards, Frameworks, Guidelines und Best Practices. Die wesentlichen sind:

- Die Veröffentlichungen des Committee of Sponsoring Organisations of the Treadway Commission (COSO) zu:
  - Internal Control—Integrated Framework
  - Enterprise Risk Management—Integrated Framework
- Die vom Office of Government Commerce (OGC®) entwickelte IT Infrastructure Library® (ITIL®)
- Der ISO/IEC 17799:2005, Code of Practice for Information Security Management der *International Organisation for Standardisation*
- Den Software Engineering Institute (SEI®):
  - SEI Capability Maturity Model (CMM®)

    - SEI Capability Maturity Model Integration (CMMI®)
- Der Project Management Body of Knowledge (PMBOK®) des Project Management Institute (PMI®)
- Der Standard of Good Practice for Information Security des Information Security Forum (ISF)

Anders als das BSI Framework ist Cobit auf strategischer Ebene angesiedelt. COBIT integriert unterschiedlichen Standards und deren Regelungsziele in einen gemeinsamen Rahmen.

COBIT orientiert sich durch eine Verbindung von Unternehmenszielen zu IT-Zielen am Kerngeschäft des Unternehmens und stellt Messgrößen und Reifegradmodelle bereit, um die Zielerreichung zu messen. Zudem identifiziert es die jeweiligen Verantwortlichkeiten im Fachbereich und der IT.

Cobit ist Prozessorientiert. Das Prozessmodell untergliedert die IT in 34 Prozesse, die in die Bereiche Planung, Entwicklung, Betrieb und Monitoring strukturiert sind. Die nachfolgende Übersicht zeigt die Gruppierung der IT-Prozesse in die vier ‚Domains'.

Inhaltlich beschreibt Cobit Ziele von Kontrollen und Maßnahmen in der IT, die die Sicherheit von Informationen im Unternehmen gewährleisten sollen. Dazu definiert Cobit folgende Kriterien an Unternehmensinformationen:

- Effektivität
- Effizienz
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Compliance
- Verläßlichkeit

Um es der IT zu ermöglichen, erfolgreich die Geschäftsanforderungen zu erfüllen und die Sicherheit der Unternehmensinformationen zu gewährleisten, sollte vom Management ein Internes Kontroll-/Steuerungssystem umgesetzt werden, wie es von Cobit beschrieben wird.

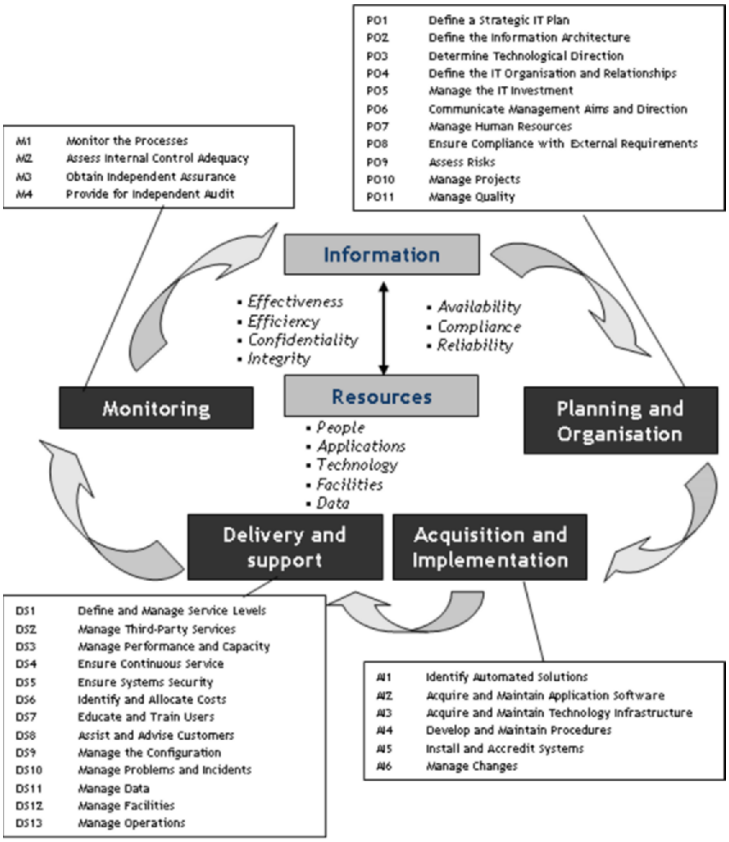

Abbildung 3–2: Das COBIT Framework

Für das Kapitel zum Service Management haben wir selbstverständlich auf die Terminologie und die Regelungsvorgaben von ITIL zurückgegriffen. Mit BSI, Cobit und ITIL basieren die hier vorliegenden Vorschläge also auf den wichtigsten internationalen Standards im Umfeld der IT.

Die IT Infrastructure Library (ITIL®) wurde Ende der achtziger Jahre von der britischen Regierung entwickelt. Das Ziel des Office of Government Commerce (OGC) war zunächst die Umsetzung einer Richtlinie für Service Management für eigene Zwecke. Das OGC sammelte dazu praktischen Erfahrungen im Bereich IT Service Management aus verschiedenen Organisationen. Daraus entstand schließlich eine Bibliothek mit zehn grundlegenden Büchern und dreißig weitere Bänder zu Spezialthemen. Insgesamt stellt die IT Infrastructure Library ein vollständiges Rahmenwerk

für das IT Service Management dar und ist inzwischen ist ein international anerkanntes Rahmenwerk bzw. ein de-facto-Standard für das IT Service Management. Basierend auf ITIL® spezifiziert die Norm ISO 20000:2005 seit neuestem Servicemanagement-Prozesse. Damit ist auf Basis von ITIL eine Grundlage für die Durchführung von Assessments von IT-Services geschaffen worden. Durch solche ISO 20000/ITIL-Assessment können Unternehmen die Schwachstellen in ihren IT-Prozessen aufdecken.

Aus dem umfangreichen Fundus der IT-Prozesse von ITIL haben wir unter dem Gesichtspunkt der IT-Sicherheit den Fokus auf Incident und Problem Management sowie Change-, Release- und Configuration-Management gelegt. Die Einführung weitere Prozesse nach den Vorgaben von ITIL sind dem Leser allerdings, im Interesse der Verbesserung der Effizienz der IT, sehr empfohlen.

4 ‚Grundgesetz' der IT-Sicherheit

Zunächst sollte sich ein Unternehmen so etwas wie eine ‚IT Verfassung' geben. Dieses Dokument der obersten Ebene kann beispielsweise IT-Sicherheitspolicy heißen. Es steckt den Rahmen ab, in dem IT-Sicherheit im Unternehmen sich bewegt und legt strukturelle und organisatorische Grundlagen für die detaillierten Richtlinien zu spezifischen Themen. Alle weiteren Dokumente nehmen Bezug auf die IT-Sicherheitspolicy und beziehen Ihre Legitimation aus diesem Grundlagendokument.

In der IT-Sicherheitspolicy wird beschrieben, wer im Unternehmen für IT-Sicherheit welche Verantwortung trägt und in welchem Umfang IT-Sicherheit geregelt werden soll. Damit erfüllt eine solche IT-Sicherheitspolicy auch wichtige Forderungen von regulatorischen Rahmenwerken wie Sarbanes-Oxley, die insbesondere eine klare Verantwortlichkeit fordern.

Die IT-Sicherheitspolicy ist, als eine Art ‚Verfassung', nicht der Ort um Detailregelungen zu treffen, z.B. bezüglich der Ausgestaltung von Passwörtern. In einem solchen Dokument sollte aber festgelegt werden, ob und in welchem Umfang ein Unternehmen Verschlüsselung von Kommunikation einsetzten will.

Wie in allen folgenden Kapitel wird im nächsten Unterkapitel nun zunächst erläutert, welche Anforderungen sich aus dem Cobit-Framework an eine solche ‚IT Verfassung' ergeben. Anschließend präsentieren wir einen konkreten Vorschlag, wie eine solche IT-Sicherheitspolicy aussehen könnte. Dieser Vorschlag ist mit dem Ziel erstellt worden, das er für die meisten Unternehmen mit geringem Aufwand an die jeweiligen Besonderheiten angepasst werden kann. Eine solche Vorgabe ersetzt aber natürlich nicht die unternehmensinterne Diskussion über die Ziele und die Ausgestaltung der IT-Sicherheit. Wir wollen lediglich diese Diskussion stimulieren und strukturieren und die Umsetzung der Ergebnisse erleichtern.

4.1 Regelungsziele nach Cobit

Die Inhalte des Cobit Frameworks im Zusammenhang mit IT-Sicherheit, die auf einer obersten Regelungsebene, also in einer IT-Sicherheitspolicy, verankert werden sollten, entstammen den Cobit Domains:

- Planung und Organisation
- Monitoring

Nicht jeder Aspekt der aufgeführten Cobit Kontrollziele muss durch dieses Policy-Dokument abgedeckt werden. Die umfassende Berücksichtigung der Kontrollziele ergibt sich aus dem Zusammenwirken aller Richtliniendokumente.

Planung und Organisation

Cobit betont sehr stark den Beitrag von IT-Prozessen zum Unternehmenserfolg. Dabei wird der Aspekt der Zuverlässigkeit von IT-Prozessen immer auch um eine Kosten-Nutzen-Betrachtung ergänzt. Gemäß Cobit sollten IT-Prozesse eine effektive und effiziente Bereitstellung der IT-Komponenten für Programme und ein Frühwarnsystem bieten für alle Planabweichungen (inklusive Kosten, Terminplan oder Funktionalität), welche die im Programm geplanten Ergebnisse beeinträchtigen können.

IT-Services sollten entsprechend vernünftiger und durchsetzbarer Service Level Agreements erbracht werden. Verantwortlichkeiten für die Erreichung des Wertbeitrags und für Kostenkontrolle sind klar festgelegt und werden überwacht. Eine angemessene, transparente, wiederholbare und vergleichbare Beurteilung von Business-Cases ist angestrebt, welche eine Aussage zur finanziellen Rechtfertigung, zum Risiko einer Nichterbringung eines Potentials und zum Risiko einer Nichtausschöpfung von erwartetem Nutzen zum Inhalt hat.

Die Geschäftsführung sollte gut informiert sein über aktuelle technologische Möglichkeiten und künftige Richtungen, über die Möglichkeiten, welche die IT bietet sowie über die durch das Unternehmen zu ergreifenden Maßnahmen, um diese Möglichkeiten nutzen zu können. Das Geschäft, an dem die IT ausgerichtet ist, sollte von den Planenden in der IT verstanden sein. Die Geschäfts- und IT-Strategie sollten integriert und allgemein kommuniziert werden; es sollte eine klare Verbindung zwischen Unternehmenszielen, IT-Zielen, erkannten Möglichkeiten und Grenzen des Potentials geben.

Dieselben Anforderungen, die Cobit an die Planung der IT als ganzes stellt lassen sich auch auf den bereich der IT-Sicherheit übertragen.

Es gilt zu identifizieren, in welchen Bereichen die Geschäftsstrategie von der IT kritisch abhängt und zu vermitteln zwischen den Erfordernissen des Kerngeschäfts und der Technologie, damit vereinbarte Prioritätenfestgehalten werden können. Die Performance der bestehenden Pläne und Informationssysteme auf deren Beitrag zu Geschäftszielen, Funktionalität, Stabilität, Komplexität, Kosten, Stärken und Schwächen ist dabei zu beurteilen.

In Zusammenarbeit mit den relevanten Stakeholdern sollte ein strategischer IT-Plan erstellt werden, welcher festlegt, inwieweit die IT zu den strategischen Zielen des Unternehmens beiträgt und der die damit verbundenen Kosten und Risiken aufzeigt. Der Plan bestimmt, inwieweit die IT die durch IT ermöglichten Investitionsvorhaben und die operative Leistungserbringung unterstützt. Er definiert, wie die Ziele erreicht und gemessen werden und wie diese durch die Stakeholder formell freigegeben werden. Der strategische IT-Plan sollte das Investitions- und operative Budget, Finanzierungsquellen, die Sourcing-Strategie, die Beschaffungsstrategie, sowie rechtliche und regulatorische Anforderungen abdecken.

Der strategische IT-Plan sollte detailliert genug gehalten sein, um die Definition von taktischen IT-Plänen zu ermöglichen. Ein Portfolio von taktischen IT-Plänen ergänzt den strategischen Plan und sind vom strategischen IT-Plan abgeleitet. Diese taktischen Pläne beschreiben notwendige IT-Vorhaben, Anforderungen an Ressourcen und wie die Verwendung von Ressourcen und die Generierung von Nutzen überwacht und gemanaged werden.

Die taktischen Pläne sollten genügend detailliert gehalten sein, um die Festlegung von Projektplänen zu ermöglichen. Die taktischen Pläne und Initiativen sollten aktiv durch die Analyse von Projekt- und Service-Portfolios gemanaged werden. Dies umfasst die regelmäßige Abstimmung von Anforderungen und Ressourcen, den Abgleich derselben mit strategischen und taktischen Zielen und erwartetem Nutzen und das Ergreifen geeigneter Maßnahmen bei Abweichungen.

Das Portfolio an IT-unterstützten Investitionsvorhaben, die für die Erreichung der strategischen Unternehmensziele erforderlich sind, sollte ebenfalls aktiv und in Abstimmung mit dem Kerngeschäft angegangen werde, indem die relevanten Programme identifiziert, definiert, evaluiert, priorisiert, ausgewählt, initiiert, gemanaged und gesteuert werden. Dies umfasst auch:

- die Abklärung der erwünschten Geschäftsergebnisse,
- die Sicherstellung, dass Programmziele die Erzielung der Ergebnisse unterstützten,
- das Verstehen des Gesamtaufwands, um die Ergebnisse zu erreichen,
- die Zuweisung klarer Verantwortlichkeiten mit unterstützenden Maßnahmen,
- die Definition von Projekten innerhalb des Programms, die Bereitstellung von Ressourcen und Finanzmitteln,
- die Übertragung von Autorität und die Beauftragung von erforderlichen Projekten zu Beginn des Programms.

Bestehende und künftige Technologien gilt es zu analysieren und zu planen, welche technologische Richtung für die Umsetzung der IT-Strategie und der Architektur der Geschäftsanwendungen angemessen ist. Der Plan sollte für die Komponenten der Infrastruktur die Systemarchitektur, technologische Richtung, Migrationsstrategien sowie Aspekte im Rahmen der Notfallplanung (contingency) behandeln.

Ein technischer Infrastrukturplan sollte mit den strategischen und taktischen IT-Plänen abgestimmt sein. Der Plan basiert auf der technologischen Ausrichtung und umfasst Maßnahmen zur Notfallvorkehrung und Vorgaben für die Beschaffung von technischen Ressourcen. Er betrachtet Änderungen im Wettbewerb, Skaleneffekte bei Stellenbesetzung und Investitionen, sowie die verbesserte Interoperabilität von Plattformen und Applikationen.

Ein IT-Strategieausschuss auf Ebene der Unternehmensleitung sollte etabliert werden. Dieser Ausschuss stellt sicher, dass IT-Governance, als Teil der Corporate Governance angemessen adressiert wird. Er berät bei der strategischen Ausrichtung und beurteilt im Namen der Unternehmensleitung wesentliche Investitionen.

Ein IT-Lenkungsausschuss (oder ein äquivalentes Gremium), das sich aus Mitgliedern der Unternehmensleitung, Kerngeschäftsprozess- und IT-Management zusammensetzt, sollte ebenfalls eingesetzt werden um,

- die Prioritäten der durch IT unterstützten Programme in Abstimmung mit der Unternehmensstrategie und deren Prioritäten festzulegen,
- Stati von Projekten zu verfolgen und Ressourcenkonflikte zu lösen und

- die Service-Levels und Verbesserung von Services zu monitoren.

Die IT-Organisationseinheit muss in die Gesamtorganisation unter Beachtung der Bedeutung der IT für das Unternehmen, speziell deren Kritikalität für die Unternehmensstrategie und die Abhängigkeit des operativen Betriebs von der IT platziert werden. Die Stelle, an die der/die CIO berichtet, entspricht der Bedeutung der IT im Unternehmen. Rollen und Verantwortlichkeiten für alle Mitarbeiter der Organisation, die mit Informationssystemen in Verbindung stehen, müssen definiert und kommuniziert werden, um ausreichend Autorität für die Umsetzung der festgelegten Rollen und Verantwortlichkeiten zu ermöglichen.

Rollenbeschreibungen müssen regelmäßig aktualisiert werden. Diese beschreiben sowohl Autorität als auch Verantwortung, umfassen eine Festlegung der Kenntnisse und Erfahrungen, die für die Position erforderlich sind, und können auch geeignet sein für die Performancebeurteilungen. Rollenbeschreibungen sollten die Verantwortung für Internal Control umfassen.

Richtlinien zur Unterstützung der IT-Strategie müssen entwickelt und unterhalten werden. Diese Richtlinien sollten die Absicht der Richtlinie, Rollen und Verantwortlichen, Prozesse zur Ausnahmebehandlung, Ansatz zur Compliance und Referenzen zu Verfahren, Standards und Anleitungen umfassen. Die Richtlinien sollten die wichtigsten Themen, wie Qualität, Sicherheit, Vertraulichkeit, Internal Controls und Schutz von geistigem Eigentum behandeln. Die Relevanz der Richtlinien sollte regelmäßig bestätigt und bewilligt werden.

Dem IT-Personal sollte bei der Anstellung eine entsprechend Einweisung angeboten werden. Laufende Schulungen sind durchzuführen, um Wissen, Fähigkeiten, Begabungen und ein Bewusstsein für Internal Controls und Security auf dem Niveau zu erhalten, das notwendig ist, um die Unternehmensziele zu erreichen. Ein allgemeiner Qualitätsplan, der eine kontinuierliche Verbesserung fördert, wird regelmäßig gewartet und kommuniziert.

MONITORING

In Zusammenarbeit mit der Geschäftsleitung sollte ein IT-Governance Framework festgelegt und eingerichtet werden, das Führung, Prozesse, Rollen und Verantwortlichkeiten, Informationsbedarf und Organisationsstrukturen umfasst, um sicherzustellen, dass die IT-gestützten Investitionsprogramme des Unternehmens an den Unternehmensstrategien und -zielen ausgerichtet sind und entsprechend diesen arbeiten. Diese Unter-