TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

Informationssicherheitsmanagement

Praxisleitfaden für Manager

Autoren

Werner Wüpper; WMC; Leiter der TeleTrusT-AG "Informationssicherheitsmanagement"
Christian Aust; consecco
Dr. Joachim Gerber; INFORA
Daniel Hecker; INFORA
Dr. Mathias Herrmann; apsec
Peter Herrmann, TÜV IT
Dr. Holger Mühlbauer; TeleTrusT
Christian Schmitz, AuthentiDate
Harald Wacker, TÜV IT
Hilde von Waldenfels; itWatch
Jochen Wildner; ditis
Iryna Windhorst; Fraunhofer AISEC
Ellen Wüpper; WMC

Diese Publikation wurde in der Arbeitsgruppe "Informationssicherheitsmanagement" des TeleTrusT - Bundesverband IT-Sicherheit e.V. erarbeitet. Für interessierte Verbandsmitglieder steht die Mitarbeit in dieser Arbeitsgruppe offen. Darüber hinaus stehen die Autoren gern als fachliche Ansprechpartner für die in dieser Publikation behandelten Themen zur Verfügung.

Impressum

Herausgeber:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 306
Fax: +49 30 400 54 311
E-Mail: info@teletrust.de
http://www.TeleTrusT.de

Herstellung:

DATEV eG, Nürnberg

1. Auflage

Inhalt

Abbildungsverzeichnis

(Abkürzungsverzeichnis S. 39)

1 Vorwort

Täglich passieren Hunderte von Informationssicherheitsvorfällen auch in Ihrer Organisation, zum größten Teil unbemerkt und im Verborgenem. Informationssicherheit ist die Basis für die Wettbewerbsfähigkeit, ist unabdingbar für langfristigen Profit und Erfolg. Zu wenig Sicherheit ist fahrlässig, zu viel Sicherheit ist unwirtschaftlich. Daher sollten mit dem richtigen Augenmaß nur bedarfsgerechte Maßnahmen in Ihrem Unternehmen implementiert werden. Es werden die Aufgaben zum Schutz von Unternehmensdaten und Informationen an Compliance Manager, Sicherheitsbeauftragte, Datenschutzbeauftragte und in den seltensten Fällen an einen Risikomanager delegiert. Bei allen Bemühungen dieser "Verantwortlichen" erreichen die Informationen und Berichtswege über mögliche Gefahren und Risiken für das Unternehmen und die implementierten Schutzmaßnahmen die Unternehmensführung nicht. Darum gehen die Ergebnisse in die Unternehmensplanung und –Strategie selten ein. Die Einführung und nachhaltige Umsetzung von Compliance-Anforderungen zur Informationssicherheit und eines wirksamen Risikomanagements, sind in allen größeren Unternehmen komplexe Aufgabenstellungen. Es reicht bei weitem nicht aus, nur die technische Infrastruktur mit Sicherheitsprodukten abzusichern; vielmehr bezieht ein funktionierendes Management System die gesamte Organisation auch in Bezug auf menschliches Verhalten und die Geschäftsprozesse mit ein.

Hand aufs Herz, können Sie mit gutem Gewissen sagen, dass Ihr persönliches Handeln als verantwortlicher Manager anders ist? Testen Sie es und beantworten Sie die Fragen in Abschnitt 2.3: wie fit ist Ihre Organisation?

Mit diesem Praxisleitfaden für Manager stellt TeleTrusT eine umsetzbare Anleitung für das Management der Informationssicherheit zur Verfügung. Sie werden in diesem Leitfaden bewusst wiederholt immer wieder darauf aufmerksam gemacht, dass erst durch die uneingeschränkte Aufmerksamkeit des Managements sich die notwendigen Erfolge einstellen. Erst die Organisation und die Regeln - dann die Technik. Mit der Einführung einer ganzheitlichen und nachhaltigen Informationssicherheit werden auch die Themen Compliance-, Risikomanagement und Business Continuity Management behandelt. Erst durch eine übergreifende Betrachtung werden die Anforderungen an das Management, diese wesentlichen Managementfelder zu bearbeiten, erfüllt. Die Aufgabe des Managements ist nicht nur die Vermeidung von Gefahren, sondern auch die Identifizierung von Chancen. Damit das Risikomanagement diese Funktion erfüllen kann, müssen Risiken - und hier sind auch die operationalen Risiken mit einzubeziehen – definiert, erkannt und bewertet werden. In der Studie "Risk-Management-Benchmarking 2011/2012"[1] analysiert PWC die Strukturen und Prozesse mit denen deutsche Großunternehmen Risiken bearbeiten. Die gesetzlichen Anforderungen an ein Risikofrüherkennungssystem wurden erfüllt (§ 91 II AktG), aber beim Risikomanagement, Risikostrategie und Risikokultur, zeigen sich laut der Studie Defizite.

Wir zeigen Ihnen auf, dass mit dem Informationssicherheitsmanagement und der damit verbundenen Compliance- und Risikokultur ein strategisches Steuerungsinstrument vorhanden sein kann, das Ihnen die Sicherheitslage auf einen Blick veranschaulicht. Wir wünschen Ihnen viel Erfolg bei der Lektüre und der anschließenden Umsetzung der Informationssicherheitsanforderungen in Ihrer Praxis.

[1] PWC Studie Risk-Management-Benchmarking 2011/2012

2 Informationssicherheit beginnt beim Management

2.1 Managementbereitschaft

Die Meinung, dass eine Organisation mit technischen Sicherheitsmaßnahmen in der IT, einem Datenschutzbeauftragten und dem Werksschutz (Zugangskontrolle und physische Sicherheit) gut aufgestellt sei, ist leider nach wie vor weit verbreitet. Jedoch fungieren IT-Abteilungen von heute als Herzstück des reibungslosen Ablaufs der meisten täglichen Geschäftsprozesse, sind nahezu mit allen Unternehmensbereichen verbunden und damit weit mehr als reiner Lieferant von Technologie.

Heutige Bedrohungen im Zusammenspiel von Menschen, Maschinen und Kommunikationsmedien erfordern, den gesamten Zyklus aller Aktivitäten im Unternehmen organisatorisch, prozessual, physisch und technisch zu betrachten und diesen integriert zu begegnen. Wichtig dabei ist, die organisatorische Planung vor der unkoordinierten technischen Umsetzung durchzuführen. Leider ist diese Sicht vom Mittelstand bis hin zu größten Unternehmen nicht durchgängig etabliert. Die Erkenntnis der Notwendigkeit, die Informationssicherheit als Managementaufgabe zu betrachten, ist bei weitem nicht überall in den Geschäftsführungsebenen angekommen.

Ein erfolgreiches Informationssicherheitsmanagementsystem (nachfolgend ISMS genannt) wird ausgehend von der Geschäftsleitung in der Organisation implementiert.
Das Thema Informationssicherheit wird auf dieser Ebene häufig vernachlässigt, da es sich nicht unmittelbar im Tagesgeschäft wiederfindet und ein Bezug zwischen Geschäftszielen und Informationssicherheit oftmals nicht hergestellt wird. Dabei haben Gefährdungen der IT auch einen direkten Einfluss auf die Erreichung der Geschäftsziele, sofern deren Erreichung durch IT-Prozesse unterstützt wird.

Informationssicherheitsmanagement hat also einen direkten Bezug zum Tagesgeschäft der Geschäftsleitung und sollte daher auch den entsprechenden Stellenwert erhalten. Dies geschieht durch die Einrichtung eines ISMS.

Es empfiehlt sich, einen Informationssicherheitsbeauftragten (ISB) zu benennen, der der Geschäftsleitung als Stabsstelle zugeordnet ist und diese in allen Belangen rund um das ISMS beratend und handelnd zur Seite steht.

2.2 Schritt für Schritt zum Erfolg

Die aktive Unterstützung des Managements und die Mitarbeit der Fachbereiche ist bei der Einführung eines Informationssicherheitsmanagementsystems (ISMS) zwingend erforderlich. Im Folgenden wird der Begriff Informationssicherheits-Risiko (IS-Risiko) verwendet. Hierunter werden alle Risiken verstanden, die auf die Unternehmenswerte Infrastruktur, Personal, IT, Prozesse, Informationen wirken und hierbei einen oder mehrere der Grundwerte von Informationssicherheit (z.B. Vertraulich, Integrität, Verfügbarkeit) beeinträchtigen.

Schritt für Schritt zum Erfolg mit 7 Ratschlägen für den richtigen Weg:

1. **Das Management bestimmt die strategische Ausrichtung**
   - Frühzeitige Einbeziehung der Geschäftsführungsentscheidung zur konsequenten Sicherheitspolitik
   - Gemeinsame Darstellung des Nutzens des ISMS für die Geschäftsziele und das Unternehmen durch die IT- und Fachabteilungen
   - Erstellung einer ersten Übersicht einer Informationssicherheitsanalyse
   - Ernennung eines Informationssicherheitsbeauftragten (ISB) mit Weisungsbefugnis durch die Geschäftsführung
2. **Festlegung der Vorgehensweise**
   - Festlegung eines überschaubaren Anwendungsbereichs
   - Auswahl der Bereiche mit kritischen Geschäftsprozessen
   - Einführung von Grundsätzen, Leitlinien; Implementierung der ISMS Organisation
   - Festlegung der relevanten Methoden und Regelwerke für das ISMS
   - Erstellung eines durchgängigen Konzeptes für die Informationssicherheit
3. **IS-Risikomanagement durchführen**
   - Etablierung des IS-Risikomanagements im Management
   - Ermittlung der Asset-Werte zur Bildung eines Kennzahlen-Systems
   - Analyse der Bedrohungen und Schwachstellen in der Systemlandschaft
   - Bewertung der Risiken
   - Erstellung eines Risikobegegnungsplans
4. **IS-Risikobegegnung durchführen**
   - Präsentation und Kommunikation der bewerteten Risiken im 'Management Board'
   - Entscheidung zur Akzeptanz oder des Transfer von Risiken
   - Durchführung von erforderlichen Sofortmaßnahmen
   - Etablierung oder Anpassung eines Business Continuity Managements (BCM) (vgl. Abschnitt 4.6)
5. **Maßnahmenmanagement durchführen**
   - Informieren und Einbinden der Fachabteilungen in die Maßnahmen
   - Terminierung und Initiierung notwendiger Projekte
   - Überprüfung der Umsetzung eingeleiteter Maßnahmen
   - Konzeptausarbeitung
   - Einführung von Maßnahmen zur Sensibilisierung und Schulung der Mitarbeiter
   - Absicherung durch Etablierung des Notfallmanagements

6. **Methode Plan-Do-Check-Act umsetzen**
   - Sicherstellung der Nachhaltigkeit der Informationssicherheit
   - Aufzeigen von Einsparpotenzialen durch eine bedarfsgerechte Umsetzung
7. **Den Wandel verdeutlichen**
   - Entwicklung zu einer an den Unternehmenswerten orientierten Informationssicherheit ersetzen

2.3 Wie fit ist Ihre Organisation

Informationssicherheit ist die Basis für die Wettbewerbsfähigkeit und ist unabdingbar für langfristigen Profit und Erfolg. Verfolgt Ihre Organisation eine ganzheitliche Strategie, um ihre Daten, Informationen und ihr Know-how zu schützen? Hier können Sie testen, welchen Stellenwert das Thema in Ihrer Organisation und bei Ihnen persönlich hat. Die Fragen sind so formuliert, dass Sie die Beantwortung aus der Sicht des verantwortlichen Managers vornehmen. Beantworten Sie die 19 Fragen und zählen Sie Ihre Punkte am Schluss zusammen. Sie haben je Frage 3 Antwortmöglichkeiten mit Punkten 0, 1, 2! Nur eine Antwort ist erlaubt.

Viel Erfolg!

1. **Verfolgen Sie eine ganzheitliche GRC (Governance, Risk, Compliance) Strategie?**
   - □ Ja, wir haben ein strategisches Managementsystem (2)
   - □ Nein (0)
   - □ Ja, wir haben schon im 'Management Board' über das Thema gesprochen (1)
2. **Haben Sie eine Informationssicherheitsorganisation?**
   - □ Ja, im vorhandenen Managementsystem integriert (2)
   - □ Nein (0)
   - □ Ja, in dem Bereich Informationstechnologie (1)
3. **Haben Sie einen Informationssicherheitsbeauftragten?**
   - □ Ja, er berichtet an den CIO (1)
   - □ Ja, er berichtet direkt an die Geschäftsführung (2)
   - □ Nein (0)
4. **Haben Sie eine offizielle Ernennung des Informationssicherheitsbeauftragten durchgeführt?**
   - □ Ja, der Informationssicherheitsbeauftragte wurde schriftliche ernannt und der Organisation bekanntgegeben (2)
   - □ Ja, die Mitarbeiter wurden per Mail / informell in Kenntnis gesetzt (1)
   - □ Nein, er hat keine schriftliche Ernennung erhalten (0)
5. **Hat der Informationssicherheitsbeauftragte ein eigenes Budget?**
   - □ Nein, der Informationssicherheitsbeauftragte hat kein eigenes Budget (0)
   - □ Ja, der Informationssicherheitsbeauftragte hat ein geringes Budget für die Mitarbeiter-Awareness (1)
   - □ Ja, er hat ein umfassendes Budget für die Einführung und den Betrieb eines ISMS (2)
6. **Haben Sie ein Risikomanagementsystem?**
   - □ Ja, wir haben ein eingeführtes Risikomanagement mit einer IS-Risikobewertung (2)
   - □ Nein, wir haben kein Risikomanagement (0)
   - □ Ja, wir haben eine gelebte Risikomanagement-Methode, aber nicht offiziell eingeführt (1)

7. Wie viel Zeit widmen Sie diesen Themen

- ☐ 1 x im Jahr (1)
- ☐ Nie (0)
- ☐ 1 x im Quartal und nach aktuellen Vorkommnissen (2)

8. Haben Sie eine Notfallorganisation?

- ☐ Ja, wir haben eine Notfallorganisation für Feuer (1)
- ☐ Nein, wir haben keine Notfallorganisation (0)
- ☐ Ja, wir haben eine Notfallorganisation für Notfälle und Katastrophen (2)

9. Haben Sie an einer Notfallübung teilgenommen?

- ☐ Ja, ich habe an einer Notfallübung für Feuer teilgenommen (1)
- ☐ Nein, das habe ich an meine Fachleute delegiert (0)
- ☐ Ja, wir führen jährlich kleine Notfallübungen und alle 2 Jahre eine übergreifende Notfallübung mit meiner Beteiligung durch (2)

10. Kennen Sie Ihre Geschäftsprozesse?

- ☐ Ja, alle Geschäftsprozesse sind dokumentiert (2)
- ☐ Nein, es ist keine Geschäftsprozessdokumentation vorhanden (0)
- ☐ Ja, wir dokumentieren gerade die Geschäftsprozesse (1)

11. Kenn Sie Ihre kritischen Geschäftsprozesse?

- ☐ Ja, alle Geschäftsprozesse sind hinsichtlich ihrer Kritikalität bewertet (2)
- ☐ Nein, wir kennen unsere kritischen Geschäftsprozesse nicht (0)
- ☐ Ja, aber nicht ganzheitlich (1)

12. Bisher lief doch alles glatt, warum sollten wir mehr tun?

- ☐ Ja, so sehe ich es auch (0)
- ☐ Nein, ich will meinen Kontroll- und Aufsichtspflichten besser nachkommen und meine persönlichen Haftungsrisiken minimieren (2)
- ☐ Nein, aber mal sehen was die anderen tun (1)

13. Verlassen Sie sich auch auf Ihre gefühlte Informationssicherheit?

- ☐ Ja, die IT-Abteilung wird schon alles Notwendige unternehmen (0)
- ☐ Nein, ich will die volle Transparenz in meinen Geschäfts- und IS-Risiken (2)
- ☐ Nein, aber meine Organisation arbeitet nicht richtig mit (1)

14. Ist ein funktionierender und sicherer IT-Betrieb für Ihren Geschäftserfolg wichtig?

- ☐ Ja, unser Geschäftserfolg ist vom sicheren IT-Betrieb abhängig (2)
- ☐ Nein, die IT muss nur funktionieren (0)
- ☐ Ja, aber mein CIO wird die Aufgabe schon erfüllen (1)

15. Kennen Sie Ihre gesteigerte Bedrohungslage?

- ☐ Ja, das zeigt spektakuläre Datendiebstähle, Steuersünder CDs, Wikileaks, Flame, DuQu, Stuxnet (2)
- ☐ Nein, die trifft auf uns nicht zu (0)
- ☐ Ja, aber meine Organisation wird es wohl im Griff haben (1)

16. Kennen Sie die Arbeitsweise der Wirtschaftskriminellen?

- ☐ Ja, ein Viertel aller Wirtschaftskriminellen-Fälle passieren über das Internet und sind individuell auf die Opfer zugeschnitten (2)
- ☐ Nein, habe ich mich noch nicht mit beschäftigt (0)
- ☐ Nein, aber dafür habe ich meine Fachleute (1)

17. Kennen Sie Ihre Sicherheitsvorfälle?

- ☐ Ja, alle Sicherheitsvorfälle werden mit in einem Managementreport berichtet (2)
- ☐ Nein, haben wir welche? (0)
- ☐ Nein, aber meine Organisation kennt sie (1)

18. Haben Sie ein softwaregestütztes Managementsystem?

- ☐ Ja, wir dokumentieren alles mit Excel, Word und PowerPoint (1)
- ☐ Nein, wir haben kein Managementsystem (0)
- ☐ Ja, wir haben eine ganzheitliche, für alle Mitarbeiter verfügbare Webanwendung (2)

19. Gehen Sie mit gutem Beispiel voran?

- ☐ Ja, ich beachte alle gesetzlichen und internen Regeln (2)
- ☐ Nein, aber immer öfters (0)
- ☐ Ja, aber mit vielen Privilegien (1)

2.4 Ihre Ergebnisse

Alle Fragen beantwortet? Dann schauen Sie, wie viele Punkte Sie haben. Schlechte Punktzahl? - Kein Problem, auf den nächsten Seiten gibt es jede Menge Tipps. Und wer fit ist, kann die Tipps nutzen, um fit zu bleiben.

Auswertung mehr als 34 Punkte

Gratulation. Sie haben die besten Voraussetzungen für eine abgesicherte Organisation, denn Sie tun eine Menge für die Informationssicherheit. Ihr Awarenesskonto steht auf Plus. Sie haben Ihrer Organisation einen regelrechten Sicherheitspanzer zugelegt. Überprüfen Sie weiterhin regelmäßig mit Hilfe des Plan-Do-Check-Act (PDCA)-Zyklus und einem externen Auditor den Status, dann bleibt es auch bei diesem guten Ergebnis. Auch wenn sich die Gegebenheiten in der globalisierten Welt permanent ändern, darf es sich nicht negativ auf Ihre Informationssicherheit auswirken.

Auswertung 20 bis 33 Punkte

Nun, ganz unbekannt ist Ihnen das Thema Informationssicherheit nicht. Nur leider geben Sie der Informationssicherheit nicht die notwendige Aufmerksamkeit, damit Sie und die in Ihrer Verantwortung befindliche Organisation auch gegen die bestehenden Bedrohungen geschützt sind. Ihr Verhältnis zu den tatsächlichen Gegebenheiten ist nicht optimal. Sorgen Sie für die notwendige Aufmerksamkeit bei Ihnen und Ihrer Organisation / Mitarbeitern. Stellen Sie die durchgängigen Regelwerke und Organisationsstrukturen auf. Holen Sie sich externe Hilfe für die anstehenden Aufgaben.

Auswertung 0 bis 19 Punkte

Ihre Einstellung und der daraus resultierende Grad an Informationssicherheit für Ihre Organisation ist ein offenes Scheunentor. Ihre mageren Vorkehrungen bieten keinen wirkungsvollen Schutz. Sie können äußeren und

inneren Einwirkungen nichts entgegensetzen. Aufwändige Einzelmaßnahmen rauben Ihnen und Ihrer Organisation ihre Leistungskraft und Effektivität. Sie sollten dringend etwas tun. Für Sie ist diese Broschüre der erste Einstieg in die Thematik. Sie sollten dringend Maßnahmen ergreifen. Ihnen kann diese Broschüre hilfreiche Praxishinweise geben. Etablieren Sie eine Sicherheitsorganisation und handeln Sie schnell. Eine externe Unterstützung mit einem Sicherheitscheck gibt Ihnen einen schnellen Überblick mit den richtigen Handlungsschwerpunkten.

2.5 Fazit und Empfehlungen

Trauriges Fazit vorweg: In vielen Unternehmen fehlen die strategischen, organisatorischen und personellen Voraussetzungen für eine wirksame Informationssicherheit. Und das Thema ganzheitliche Informationssicherheit hat trotz der Zunahmen an Social Engineering-, Hacker- und Wirtschaftsspionageangriffen die Aufmerksamkeit des Managements längst nicht erreicht.

Informationssicherheit ist in allen Organisationen keinesfalls nur ein Thema der IT - vielmehr betrifft ein Informationssicherheitsmanagementsystem das gesamte Unternehmen, vom entscheidungstreffenden Management bis zu den informationsverarbeitenden Sachbearbeitern. Durch diesen übergreifenden Charakter ist es enorm wichtig, klar und deutlich die Verantwortung jedes Einzelnen im Sicherheitsprozess zu definieren und dieser Person die Verantwortung bewusst zu machen, denn nur so können die angestrebten Sicherheitsziele effizient und kostengünstig erzielt werden.

Definieren und implementieren Sie neben der Funktion des Informationssicherheitsbeauftragten (ISB) weitere grundlegende Instanzen für die Informationssicherheit innerhalb der Organisationsstruktur des Unternehmens, um das ISMS erfolgreich im Unternehmen zu etablieren und Informationswerte auch über Standorte hinweg angemessen zu schützen

Im Unternehmen muss durch das Management eine Informationssicherheitsorganisation aufgebaut und überwacht werden, die u.a.:

- die Arbeit des ISB über alle Ebenen der Organisation hinweg unterstützt;
- Risiken frühzeitig erkennt und angemessene Maßnahmen einleitet und nachverfolgt;
- die Kontrolle der Einhaltung von Policies und Richtlinien ermöglicht;
- Verbesserungsmöglichkeiten in den (ISMS-) Prozessen aufzeigt;
- an die Größe und Struktur des Unternehmens angepasst ist;
- es jederzeit ermöglicht den momentanen Zustand des ISMS zu ermitteln;
- Sicherheitsvorfälle aufdecken und angemessen untersuchen kann;
- in der Lage ist, zielgerichtete Sensibilisierungs- und Schulungsmaßnahmen zu initiieren.

Verpflichten Sie Ihre Verantwortlichen für Informationssicherheit die Aufgaben im Management immer wieder transparent darzustellen, wie wichtig eine ganzheitliche Sicht des Themas für das gesamte Unternehmen ist, und stellen Sie dabei folgende Argumente und Themen heraus:

- Erfüllung der Compliance Anforderungen;
- Reduzierung der Haftungsrisiken;
- Verhinderung von Konventionalstrafen ;

- Reduzierung der Risiken;
- Senkungen der Betrugsfälle;
- Schutz der Reputation und Stärkung des Kundenvertrauens;
- Sicherung der Systemarchitektur und Prozessketten;
- Steigerung der Prozessqualität;
- Steigerung der Wettbewerbsfähigkeit;
- Steigerung der Mitarbeiterzufriedenheit.

Versuchen Sie als Verantwortlicher im Management es doch mal mit ein paar wöchentlichen Aktivitäten für Ihre Alltags-Informationssicherheit!
Sprechen Sie 1mal pro Woche mit Ihren Managern über Vorkommnisse!
Erinnern Sie 1mal pro Woche einen Mitarbeiter an richtiges Sicherheitsverhalten!
Lassen Sie bei sich auch keine Ausnahmen zu!

3 Für immer angemessen sicher

3.1 Wie viel Informationssicherheit ist notwendig?

Um herausfinden zu können, ob die bereits implementierten Sicherheitsvorkehrungen den Geschäftsanforderungen gerecht werden, sollten Sie das angestrebte Sicherheitsniveau definieren; das heißt, es muss entschieden werden, wie hoch die potenzielle Bedrohung für Ihr Unternehmen sein darf. Dazu definieren Sie eine branchenunabhängige finanzielle, rechtliche und immaterielle Risikobereitschaft. Sie setzt den Rahmen zu entscheiden, welche Risiken zu mindern sind und welche aufgrund geringer finanziellen Auswirkungen in Kauf genommen werden können. Betrachten Sie folgende drei strategische Ziele bei der Ermittlung der unternehmensspezifischen Risikobereitschaft:

- Kunden-/ Kundenzufriedenheit und Qualität;
- der Wertbeitrag des Unternehmens;
- nachhaltiges und kontrollierbares Wachstum.

Um die Frage "Wieviel Informationssicherheit ist notwendig?" zu beantworten haben wir als Basis die Klassifizierung der Informationen und Geschäftsprozesse in vier Stufen herangezogen und dafür die Informationsklassen für Unternehmen exemplarisch definiert. Diese Einstufungen müssen von der Organisation fallweise und spezifisch für die jeweiligen Themen angepasst und von der Geschäftsführung verabschiedet werden Die Methode ist unabhängig von der Unternehmensgröße, der Unternehmensart und der Branche. Die Einstufung erfolgt in gering, mittel, hoch, sehr hoch. Die verfolgten Ziele je Einstufungslevel beziehen sich auf unterschiedliche Arten von Informationen und müssen aufgrund Ihrer Anforderungen auf Basis der unten aufgeführten Schutzziele klassifiziert werden nach:

- Vertraulichkeit;
- Integrität;
- Verfügbarkeit;
- ggf. Zurechenbarkeit;
- Nichtabstreitbarkeit.

Level	Ziele	Beschreibung	Merkmale	Aufwendungen
gering	Vertraulichkeit Verfügbarkeit Integrität	- keine oder unbedeutende rechtlichen Auswirkungen, - keine oder unbedeutenden Auswirkungen auf den Kapitalmarkt, - keine oder geringfügige Auswirkungen auf Teile des Geschäftsbetriebes, - keine oder wenig Einbeziehung des Managements notwendig - einzelne Projekte sind betroffen	wenige kritische Geschäftsprozesse, kaum vertrauliche Informationen, geringfügige gesetzliche Vorgaben	Keine oder normale Aufwendungen für Personen- und Gebäudeschutz
mittel	Vertraulichkeit Verfügbarkeit Integrität	- Ermittlungen gegen einzelne Mitarbeiter, - spürbare Auswirkungen auf den Kapitalmarkt, - Auswirkungen auf den gesamten Geschäftsbetrieb, - zeitweise Einbeziehung des Managements notwendig - Kernprojekte sind beeinträchtigt	Kritische Geschäftsprozesse in der Leistungserstellung vertrauliche Informationen, Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen, geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen	Spezielle Aufwendungen für Personen- und Gebäudeschutz, Ableitung von speziellen Notfallverfahren für leistungserstellende Prozesse
hoch	Vertraulichkeit Verfügbarkeit Integrität Authentizität Zurechenbarkeit Nichtabstreitbarkeit	- rechtliche Involvierung des Managements, ggf. Strafbefehle - starke Auswirkungen auf den Kapitalmarkt, Verlust der Kreditwürdigkeit - starke Auswirkungen auf den gesamten Geschäftsbetrieb mit Umsatzeinbußen - starke Einbeziehung des Managements notwendig - Kernprojekte sind gefährdet	Kritische Geschäftsprozesse in der Leistungserstellung, sowie in Führung und Support, geheime Informationen, Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen, Vertragsverletzungen mit hohen Konventionalstrafen	Hohe Anforderungen an die Informationssicherheit in Bezug auf IT-Security, physikalische Sicherheit, Produktschutz und Werkschutz. Ein Managementsystem ist unumgänglich.
sehr hoch	Vertraulichkeit Verfügbarkeit Integrität Zurechenbarkeit Nichtabstreitbarkeit	- unternehmensweite rechtliche Auswirkungen mit Öffentlichkeitswirkung (Prestigeverlust), Auswirkungen auf Kunden und Lieferanten - langfristig schädigende Auswirkungen auf den Kapitalmarkt - Verlust von strategischen Geschäftseinheiten - durchgehende Einbeziehung des Managements notwendig - Kernprojekte sind obsolet	hochkritische Geschäftsprozesse in der Leistungserstellung, sowie in Führung und Support, geheime Informationen, fundamentaler Verstoß gegen Vorschriften und Gesetze, Vertragsverletzungen, deren Haftungsschäden ruinös sind	Sehr hohe Anforderungen an die Informationssicherheit an ein valides Management-System, eine effektiv ausgerichtete Compliance basierend auf einem etablierten Risikomanagement sowie getesteten Business Continuity Strukturen.

Abbildung 1: Best Practice Informationsklassen

Diese Informationsklassen orientieren sich an dem Best Practice Ansatz der beschriebenen Standards und sind eine Hilfestellung für die Frage nach dem ausgewogenen Informationslevel für ein Unternehmen. Eine international anerkannte und durchgängige Methode ist bisher nicht vorhanden. Das BSI gibt im IT-Grundschutz eine entsprechende Methode vor. Auch die ISO/IEC Norm 27001 fordert eine solche Einstufung ohne sie detailliert zu beschreiben; Anhand der Informationsklassen lassen sich alle Leitlinien, Richtlinien und Standards ausrichten. Die Geschäftsführung gibt die Informationssicherheitsleitlinie und die Richtlinie IT-Sicherheit vor, die Fachabteilungen werden dann die Standards nach den vorgegebenen Sicherheitslevel ausarbeiten. Diese Informationsklassen sollten so präzise wie möglich an die Umgebung des Unternehmens angepasst werden, um ein Höchstmaß an gemeinsamem Verständnis und die Nachvollziehbarkeit der Bewertungen zu erreichen.

3.2 Wie wirtschaftlich ist die Informationssicherheit (ROI)?

Fachleute behaupten, dass sich auch bei der Informationssicherheit der Return on Investment (RoI) oder auch RoSI (Return on Security Investment) exakt beziffern lässt. Praktikern und dabei gerade den Controllern sind die Ergebnisse jedoch nicht aussagekräftig genug, gemessen an dem Ziel, durch ein höheres Sicherheitsniveau eine höhere Wettbewerbskraft zu erreichen.

Eine Kosten-Ertrags-Rechnung für das Gesamtunternehmen beim Thema Informationssicherheit ist schwierig. Verlässliche Daten sind nur mit einem enormen Aufwand zu ermitteln und bei verhinderten Schäden nur schwer zu interpretieren. Bei sich ständig ändernden Szenarien ist eine Einzelfallrechnung vorzuziehen. Doch letztlich muss jedes Unternehmen seinen Bedarf an Sicherheit individuell einschätzen und ihn technisch sowie organisatorisch abdecken, denn wenn sich ein Unternehmen versichern möchte, ist ohne eine Grundsicherheit im IT-Bereich und in der ganzheitlichen Informationssicherheit der Versicherer nicht bereit, Risiken abzudecken.

Die Kernfrage ist, wie hoch Informationssicherheitskosten sein dürfen. Das hängt zum einem vom Sicherheitslevel und zum anderen in den meisten Fällen vom Anteil am IT-Budget ab. Rund zehn Prozent für laufende Security-Ausgaben gelten branchenübergreifend als akzeptabler Wert.

Bei Schadenszenarien muss genau nachgerechnet werden, ob sich die Schäden tatsächlich negativ auf die Bilanz auswirken. Oft werden Risiken falsch eingeschätzt. Häufig ließen sich die entstandene Schäden durch Hacker- oder Virenangriffe mit Überstunden und zusätzlichen Kosten durch die IT-Abteilungen beheben. Wesentlich größer ist immer noch die Gefahr interner Diebstähle, Know-how-Diebstähle, Betrug oder Manipulationen insbesondere Datenmanipulation. Die größte Bedrohung liegt in den Vorfällen die über einen längeren Zeitraum gar nicht bemerkt wurden. In der Praxis spielten RoSI-Erwägungen eine geringere Rolle als das Argument, durch ein hohes Sicherheitsniveau erhöhe sich die Wettbewerbskraft.

Ist auf eine RoSI Berechnung Verlass? Laut dem Ergebnis der Studie der Sloan School of Management am Massachusetts Institute of Technology (MIT), der Stanford University und dem US-Unternehmensberatung Stake[2] sind IT-Sicherheitsinvestitionen umso kostengünstiger, je früher sie realisiert werden.

[2] Return of Security Invest / Veröffentlichung im CIO Magazin: http://www.cio.de/news/cionachrichten/805837/

Eine Umfrage unter 500 US-Unternehmen ergab einen RoSI-Wert von 21 Prozent, wenn bereits beim Design von IT-Systemen die Security mitgeplant wurde. Der Ertrag ging dagegen auf 15 beziehungsweise 12 Prozent zurück, wenn erst bei der Implementierung und in der Testphase an die Sicherheit gedacht wurde. Wer sich erst in der Praxis um die Sicherheit der Software kümmerte, musste der Studie zufolge sechsmal höhere Kosten tragen. Es lohnt sich also frühzeitig in IS zu investieren.

3.3 Chancen des IS-Risikomanagements

Im Fokus jedes Unternehmens steht die Maximierung der Chancen bzw. die Minimierung der Gefahren. Um das zu gewährleisten, muss jedes Unternehmen seine Chancen und Risiken kennen und managen. Dies ist der Kern des Risiko- und Chancenmanagements (RCM) und zählt zu den wichtigsten Managementfeldern überhaupt. Deswegen muss es auch zum täglichen Geschäft eines jeden Geschäftsführers gehören. Das Managen von IS-Risiken fällt allerdings vielen Entscheidern in Unternehmen noch schwer. Dabei ist die IT inzwischen Basis fast aller und vor allem vitaler Geschäftsprozesse. Die Technikausfälle können daher sehr bedrohlich für ein Unternehmen werden.

Die Aufgabe des Risiko- und Chancenmanagements im Unternehmen besteht in erster Linie in der Existenzsicherung sowie der Absicherung der Unternehmensziele, der sogenannten Zukunftssicherung, unter leistungswirtschaftlichen, finanziellen und sozialen Aspekten, wobei die Risikokosten möglichst gering zu halten sind. Dabei versteht man unter Risiko jede negative und unter Chance jede positive Abweichung von der vorgegebenen Zielgröße. Innerhalb des Bereiches des IS-RCM kann man zwischen strategischen und operativen Risiken und Chancen unterscheiden.

Risikomanagement ist nicht nur eine lästige Pflicht, sondern vielmehr eine Chance.

Sehen Sie das IS-Risikomanagement nicht nur als lästige Pflicht, sondern vielmehr als Chance, denn diverse Erfahrungen und Untersuchungen zeigen, dass sich das kontinuierliche Messen und Bewerten von IS-Risiken lohnt und auch monetär auszahlt. Das IS-Risikomanagement deckt wirtschaftlichen Gefahren auf, weist aber auch auf Einsparmöglichkeiten in der Infrastruktur und Organisation hin, wie beispielsweise wenn und wie etwa die bisherige Notfallplanung optimiert werden kann. Neben einem höheren Sicherheitsniveau profitieren Unternehmen, die ein IS-RCM betreiben, auch vielfach von einer Prozessoptimierung in der IT. Durchgängige Sicherheits- und Risikokonzepte sind darüber hinaus sehr gut dazu geeignet, das Vertrauen von Geschäftspartnern und Banken in das eigene Unternehmen zu stärken.

Die "Risikokultur" ist oft unterentwickelt

Eine entwickelte Risikokultur, also das Bewusstsein der Mitarbeiter für Risiken sowie deren Identifikation und Steuerung, ist wesentliche Voraussetzung eines effizienten Risikomanagements. Dem einzelnen Mitarbeiter des jeweiligen Unternehmens soll die Risikopolitik als Verhaltenskodex dienen. Ausgehend von Ihnen, als Geschäftsführer und Management, wird das Risikobewusstsein im Unternehmen geschaffen und die Risikokultur gelebt.

Risiko- und Chancenmanagement (RCM) ist ein kontinuierlicher Prozess

RCM ist keine einmalige Aktion, sondern ein stetiger Prozess, der in dem üblichen PDCA-Zyklus betrieben werden sollte. Die Methodik des IS-Risikomanagements finden Sie im Anhang beschrieben.

3.4 Sicherheitsorganisation

Um das ISMS erfolgreich im Unternehmen zu etablieren und Informationswerte auch über Standorte hinweg angemessen zu schützen, müssen neben der Funktion des Informationssicherheitsbeauftragten (ISB) weitere grundlegende Instanzen für die Informationssicherheit innerhalb der Organisationsstruktur des Unternehmens definiert und implementiert werden. Im Unternehmen muss eine Informationssicherheitsorganisation abhängig von der Größe und Struktur des Unternehmens aufgebaut werden, die u.a.:

- die Arbeit des ISB über alle Ebenen der Organisation hinweg unterstützt;
- Risiken frühzeitig erkennt und angemessene Maßnahmen einleitet und nachverfolgt;
- die Kontrolle der Einhaltung von Policies und Richtlinien ermöglicht;
- Verbesserungsmöglichkeiten in den (ISMS-) Prozessen aufzeigt;
- an die Größe und Struktur des Unternehmens angepasst ist;
- es jederzeit ermöglicht den momentanen Zustand des ISMS zu ermitteln;
- Sicherheitsvorfälle aufdecken und angemessen untersuchen kann;
- in der Lage ist, zielgerichtete Sensibilisierungs- und Schulungsmaßnahmen zu initiieren.

Ohne eine etablierte Informationssicherheitsorganisation im Unternehmen fehlen:

- die Grundlagen zur Integration von Informationssicherheit in Geschäftsprozessen, d.h. die Basis für gelebte Sicherheit und den Schutz der Informationswerte des Unternehmens;
- wichtige Organe (z.B. Information Security Emergency Team, ISET) für den effektiven und effizienten ISMS-Betrieb und das Notfallmanagement;
- Multiplikatoren für Informationssicherheit an den Standorten (z.B. Informationssicherheitskoordinatoren);
- entscheidende Voraussetzungen zur Umsetzung des PDCA-Zyklus (Plan – Do – Check – Act) innerhalb der ISMS-Prozesse.

Generell gilt es zu beachten, dass der Informationssicherheitsbeauftrage (Chief Information Security Officer; CISO) als Stabsstelle direkt an den Vorstand / die Geschäftsleitung berichtet. Die nachfolgend aufgeführten Beispiele zeigen mögliche Varianten einer Informationssicherheitsorganisation für Unternehmen unterschiedlicher Größe und Struktur.

Großunternehmen (Top DAX-Unternehmen)

Großunternehmen sind in der Regel als "Global Player" international tätig und verfügen häufig über komplexe Organisationsstrukturen und heterogene IT-Infrastrukturtechnologien. Daher bedarf es einer global aufgestellten Informationssicherheitsorganisation mit klar definierten Verantwortlichkeiten und Aufgaben, um Informationssicherheit in die Geschäftsprozesse zu integrieren und so im gesamten Unternehmen zu verankern.

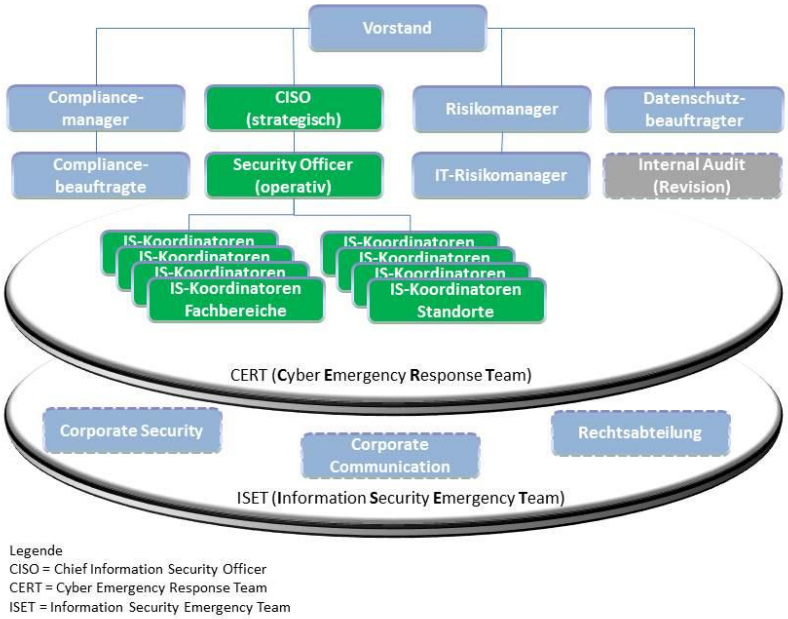

Abbildung 2: Beispielorganisation für Informationssicherheit (Großunternehmen)

Gehobener Mittelstand (>3000 MA – mittlere bis große Unternehmen)

Die Anforderungen und Problemstellungen im gehobenen Mittelstand entsprechen häufig denen der Großunternehmen. Jedoch sind im gehobenen Mittelstand die IT-Organisationen und –Budgets, was "Manpower" und absolute Beträge betrifft, in den meisten Fällen proportional weit schmaler ausgestattet.

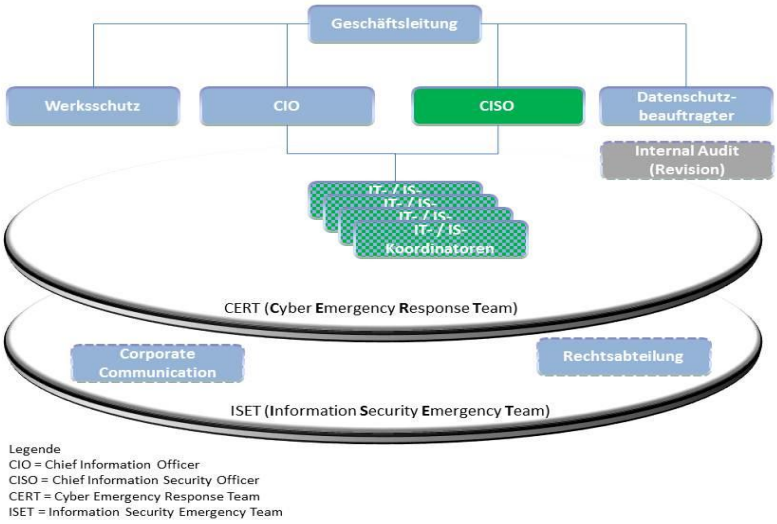

Abbildung 3: Beispielorganisation für Informationssicherheit (gehobener Mittelstand)

Darüber hinaus wird oft die Funktion für Informationssicherheitsmanagement vom IT-Leiter oder Datenschutzbeauftragten mit übernommen. Hier stellt sich neben der Personal- und Finanzthematik auch die Frage wie man ein sinnvolles und nachhaltiges Informationssicherheitsmanagement in der Praxis angeht.

Mittelstand (<3000 MA – kleine Unternehmen mit hohem Sicherheitsbedarf)

Auf Grund der zunehmenden Bedrohungslage durch Wirtschaftsspionage, Social Engineering oder Hacking gilt es für den Mittelstand Konzepte zu entwickeln, welche den Mangel an Kapazitäten und Knowhow im Bereich der Informationssicherheit und des Informationsschutzes beheben. Dies kann beispielsweise durch das Einbeziehen externer Informationssicherheits- und Datenschutzbeauftragter in die Sicherheitsorganisation des Unternehmens erfolgen. Dabei bleibt allerdings die Verantwortung für Informationssicherheit beim Unternehmen.

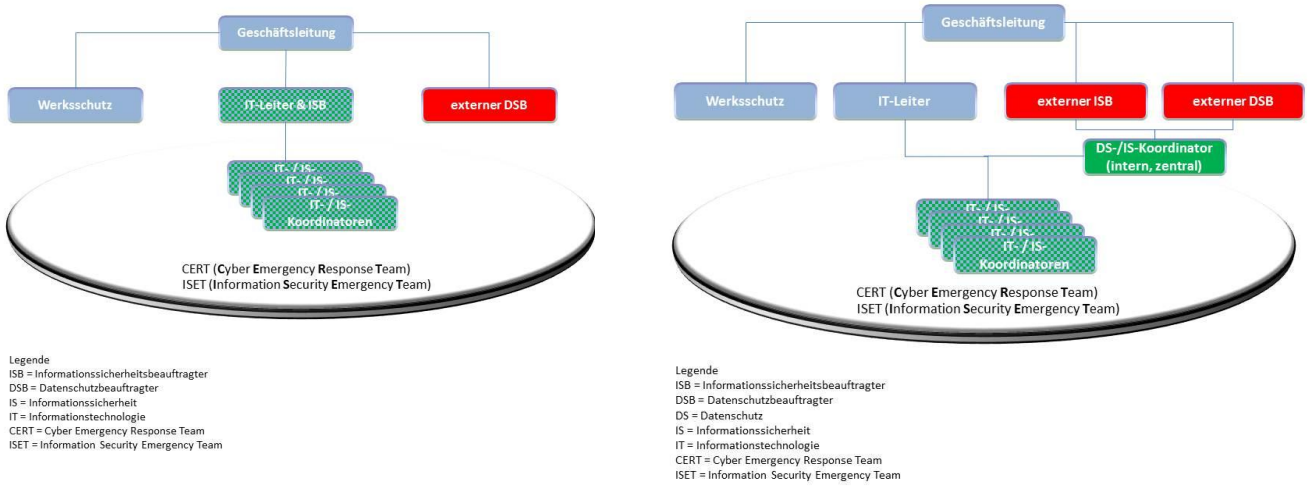

Abbildung 4: Beispielorganisationen für Informationssicherheit (Mittelstand)

3.5 Rollen und Verantwortlichkeiten

Informationssicherheit ist keinesfalls nur ein Thema der IT - vielmehr betrifft ein Informationssicherheitsmanagementsystem (ISMS) das gesamte Unternehmen, vom entscheidungstreffenden Management bis zu den informationsverarbeitenden Sachbearbeitern. Durch diesen übergreifenden Charakter ist es enorm wichtig, klar und deutlich die Verantwortung jedes Einzelnen im Sicherheitsprozess zu definieren und dieser Person die Verantwortung bewusst zu machen, denn nur so können die angestrebten Sicherheitsziele effizient und kostengünstig erzielt werden. Alle modernen Methoden zur Etablierung eines ISMS erkennen die Notwendigkeit und die Bedeutung von Rollen und Verantwortlichkeiten und geben Vorschläge für den Aufbau einer Informationssicherheitsorganisation. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) nennt beispielsweise in der Vorgehensweise zum IT-Grundschutz drei Grundregeln bei der Definition von Rollen im Informationssicherheitsmanagement:

- Die Leitungsebene hat die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung.
- Es ist mindestens eine Person (typischerweise Informationssicherheitsbeauftragter) zu benennen, die den Informationssicherheitsprozess fördert und koordiniert.
- Jeder Mitarbeiter ist gleichermaßen für seine originäre Aufgabe wie für die Aufrechterhaltung der Informationssicherheit an seinem Arbeitsplatz und in seiner Umgebung verantwortlich.

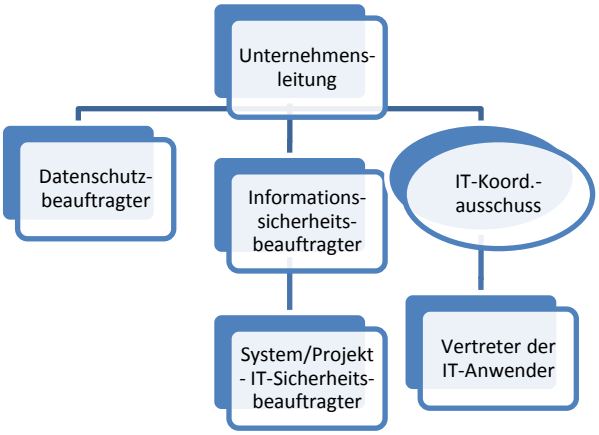

Abbildung 5: Aufbau einer Informationssicherheitsorganisation

Aufbauend auf dieser Grundlage gilt es eine Informationssicherheitsorganisation zu definieren, die den spezifischen Gegebenheiten des Unternehmens angepasst ist. Dabei gibt es kein Patentrezept wie Rollen und Verantwortlichkeiten aufzubauen sind, sondern nur Best-Practice Ansätze, die abhängig von der Unternehmensgröße, bewährte Rollen und deren Aufgaben und Verantwortlichkeiten vorschlagen.

Der IS-Beauftragte stellt den Hauptansprechpartner rund um das Thema IS dar. Er

- verantwortet alle erforderlichen Aktivitäten zur Etablierung, Implementierung und Aufrechterhaltung des ISMS;
- koordiniert insbesondere die Erarbeitung von Risikoanalysen und IS-Konzepten, die Einführung notwendiger Prozesse (z.B. Behandlung von Sicherheitsvorfällen) sowie die Sensibilisierung und Schulung der Mitarbeiter;
- überprüft die Realisierung und Wirksamkeit von IS-Maßnahmen und –Prozessen;
- führt regelmäßige interne Reviews durch und koordiniert externe Audits;
- berichtet der Unternehmensleitung den Status des ISMS;
- gewährleistet die Umsetzung von Verbesserungsmaßnahmen aufgrund erkannter Schwachstellen.

Gegebenenfalls können einzelne Aufgaben an System/Projekt-IT-Sicherheitsbeauftragte delegiert werden. Aufgabe des Datenschutzbeauftragten ist die Überwachung der Einhaltung von regulatorischen Vorschriften des Datenschutzes in allen Bereichen des Unternehmens. Dabei steht er in beratender Funktion der Unternehmensleitung, aber vor allem den Mitarbeitern zur Seite. Ein IS-Koordinierungsausschuss wird bei Bedarf temporär einberufen, um im Rahmen von größeren IT-Projekten das Zusammenspiel von Informationssicherheitsteam und den IT-Anwendern zu koordinieren.

3.6 Sicherheitsprozesse

Ist die Organisationsstruktur definiert, werden im nächsten Schritt die Prozesse des ISMS festgelegt und eingeführt. Bei der Definition der Prozesse ist es von Bedeutung welchen Rahmenbedingungen diese genügen sollen. Dabei ist z.B. zu beachten

- welche gesetzlichen Rahmenbedingungen eingehalten werden müssen;
- welche Anforderungen durch Kunden, Lieferanten und Geschäftspartner an das Unternehmen gestellt werden und welchen Einfluss diese auf den Sicherheitsbedarf haben;
- welche Sicherheitsstandards in der Branche generell üblich sind.

Nicht zuletzt durch den letzten Punkt wird deutlich, dass ein ISMS, das deutlich über die Anforderungen hinausgeht, sich auch negativ auf ein Unternehmen und dessen Wettbewerbsfähigkeit auswirken kann.

Der Sicherheitsbeauftragte ist für die ISMS-Compliance-Prozesse zuständig. Der Compliance-Prozess (ISMS-Prozess) wird im Regelfall mit einem Assessment begonnen. In dem Assessment werden der Untersuchungsbereich und die Anforderungen/Regelwerk festgelegt. Die Verantwortlichen bewerten die Anforderungen des Regelwerkes und legen Maßnahmen zur Überprüfung und Verbesserung an. Dieses Vorgehen wird in dem PDCA-Zyklus wiederholt.

Es sind die Prozesse zu definieren, zu beschreiben und die Verantwortlichkeiten zu bestimmen. Das Vorgehen sollte mit Hilfe von Beschreibungen und Prozessabläufen beschrieben und festgelegt werden.

Die weiteren Prozesse: Awareness, Business Impact Analyse (BIA), Business Continuity Management (BCM) (vgl. Anhang) etc. müssen entsprechend beschrieben und eingeführt werden.

Bei diesen Führungsprozessen ist besonders zu beachten, dass alle Rollen beschrieben und die Verantwortlichen benannt werden. Das Management hat die Entscheidungssicht, die Fachverantwortlichen die Beurteilungs- und Umsetzungssicht, die Mitarbeiter die Informationssicht und die Beauftragten die Überprüfungssicht.

3.7 Technische Sicherheit

Um Informationen erfolgreich vor Verlust und unberechtigtem Zugriff zu schützen und die Verfügbarkeit von IT-Systemen zu gewährleisten, ist neben der Schaffung organisatorischer und prozessorientierter Rahmenbedingungen auch eine technische Grundsicherung im Unternehmen erforderlich. Dies bedeutet zum einen die Absicherung der IT-Infrastruktur, aber auch die Implementierung von physischen Schutzmaßnahmen u.a. für das Betriebsgelände.

Einige wesentliche Werkzeuge zur Absicherung der IT-Infrastruktur und zum Schutz des Unternehmens vor Angriffen von außen und innen werden im Folgenden aufgeführt und kurz erläutert. Je nach Bedrohungslage und Ergebnis einer Risikobetrachtung können weitere technische Sicherheitsmaßnahmen wie z. B. Intrusion Prevention-Systeme oder aber auch der Schutz der Endgeräte nötig werden:

Firewall

Eine Firewall trennt Netze, so auch das Unternehmensnetzwerk vom Internet und bildet daher den äußeren Schutzwall eines IT-Netzwerks. Sie verhindert ein Eindringen unberechtigter Dritter in das Unternehmensnetzwerk. Voraussetzung hierfür ist, dass die Firewall-Einstellungen richtig konfiguriert sind und die Firewall einem kontinuierlichen Monitoring und Aktualisierungsprozess unterliegt. Die Wirksamkeit des Schutzgrades der Firewall sollte regelmäßig durch Penetrationstests überprüft werden, um so eventuell bestehende Schwachstellen zu erkennen und rechtzeitig entsprechende Maßnahmen zum Schließen der Sicherheitslücken zu implementieren.

Virenschutz und Patch-Management

Eine Virenschutzsoftware sichert die Betriebssysteme und Anwendungen der IT-Systeme und die darauf verarbeiteten Unternehmensdaten gegen den Befall von Viren, Würmern und Trojanern ab. Sie schützt so die Vertraulichkeit und Integrität von Daten und trägt zur Verfügbarkeit der Unternehmens-IT bei. Der Virenschutz kann nur dann einen hohen Wirkungsgrad erreichen, wenn er regelmäßig aktualisiert und alle IT-Systeme aktiv geschützt werden. Die Installation von aktuellen Sicherheitsupdates der Softwarehersteller für Betriebssysteme und Anwendungen erhöht den Schutz und die Verfügbarkeit der Unternehmens-IT zusätzlich. Die Wirksamkeit der internen Schutzmaßnahmen, wie beispielsweise des Patch-Managements, oder des Virenschutzes sollte regelmäßig durch interne Schwachstellscans überprüft werden.

Verschlüsselung und Kryptographie

Um Informationen vor unberechtigtem Zugriff zu schützen, müssen diese verschlüsselt werden. Nur das Verschlüsseln einer E-Mail gewährleistet die Vertraulichkeit des Inhalts. Wird die E-Mail zusätzlich noch signiert, kann dadurch die Authentizität des Absenders sichergestellt werden. Der Versand einer unverschlüsselten E-Mail bietet letztendlich den gleichen Schutz für den Inhalt, wie der Versand einer Postkarte. Auf mobilen IT-Endgeräten, wie Notebooks oder USB-Sticks werden oft sensible Unternehmensdaten mitgeführt. Hier muss darauf geachtet werden, dass auch diese Geräte verschlüsselt werden, um im Falle eines Verlusts die darauf befindlichen Unternehmensdaten vor unberechtigtem Zugriff zu schützen und so die Auswirkungen beispielsweise eines Diebstahls zu minimieren.

Berechtigungskonzept

Der Zugriff auf Daten in IT-Systemen wird über Berechtigungen gesteuert. Um sicherzustellen, dass nur autorisierte Benutzer einen Zugriff auf die entsprechenden Informationen erhalten, müssen Berechtigungen beim Informationseigentümer beantragt und von diesem freigegeben werden. Dieser Prozess sollte dokumentiert beispielsweise auf Basis eines Workflows erfolgen, um die Transparenz im Berechtigungsprozess zu gewährleisten. Außerdem sollte eine turnusgemäße Prüfung der Zugriffsberechtigungen durch den Informationseigentümer ein wesentlicher Bestandteil des Berechtigungskonzepts sein. Eine Prüfung kritischer Berechtigungskombinationen, beispielsweise in ERP-Systemen bildet eine weitere Grundlage für die Sicherheit der Geschäftsprozesse.

Datensicherung und Disaster Recovery

Zur Sicherstellung der Verfügbarkeit von Daten auf IT-Systemen müssen diese regelmäßig gesichert werden. Um die gesicherten Daten vor Verlust zu schützen, beispielsweise im Brandfall, sollten diese in einen von den

produktiven IT-Systemen (Daten) getrennten Brandabschnitt ausgelagert werden. Das gleiche gilt für die Sicherungsmedien. Um die Funktionalität der Datensicherung sicherzustellen, müssen regelmäßige Restore-Tests der Datenbestände durch die IT-Abteilung durchgeführt und dokumentiert werden. Diese Maßnahme bildet eine wichtige Grundlage im IT-Notfallmanagement und sollte um weitere Themen, wie beispielsweise Alarmierungspläne, Wiederherstellungspläne etc. erweitert werden, um bei Ausfall eines kritischen IT-Systems die Auswirkung auf den Geschäftsbetrieb auf ein Minimum zu reduzieren.

Physische und umgebungsbezogene Sicherheit

Da Informationen im Unternehmen nicht ausschließlich auf IT-Systemen verarbeitet werden, sondern auch in der Entwicklungsabteilung, in der Produktion oder im Vertrieb gilt es ganzheitliche Sicherheitskonzepte zu entwickeln, die auch die physische und umgebungsbezogene Sicherheit gewährleisten. Konkret bedeutet dies die Umsetzung von Schutzmaßnahmen wie Zutrittsschutz auf das Firmengelände, aber auch in Gebäude und Räumlichkeiten; das Tragen von Mitarbeiter- oder Besucherausweisen; Brandschutz; Einsatz einer Notstromversorgung für die IT-Systeme; sichere Entsorgung von Dokumenten und IT-Hardware oder die Installation einer redundanten Klimaanlage im Rechenzentrum. Es sollte darauf geachtet werden, dass die Schutzmaßnahmen speziell in den sensiblen Unternehmensbereichen, d.h. abhängig vom Schutzbedarf der dort verarbeiteten Informationen zuerst umgesetzt werden.

Neben den hier aufgeführten technischen Sicherheitsmaßnahmen gibt es viele weitere technische Informationssicherheitsmaßnahmen, die wie die organisatorische Sicherheit Ihren Bedürfnissen angepasst sein müssen. Eine gemanagte Informationssicherheit legt die Rahmenbedingungen der Organisation in Leitlinien, Richtlinien, Standards und den zugehörigen Konzepten fest. Es betrifft die Themen (Auszug):

- Informationssicherheitsleitlinie;
- Standard Anwender und Endgeräte;
- Standard Klassifizierung von Informationen;
- Standard Notfall- und Krisenmanagement;
- Standard Passwortsicherheit für Anwender;
- Standard Passwortsicherheit für Administratoren;
- Standard Netzwerksicherheit;
- Standard Serversicherheit;
- Standard Protokollierung;
- Standard Archivierung und Backup.

Gerade in größeren Unternehmen und Organisationen existiert oft die Einsicht, dass gegen "Sicherheitslöcher" vorgegangen werden muss. Nur, was sind die dringlichsten Aktionen gegen die gefährlichsten Risiken? Und wo soll man anfangen?

Wie Sie ganz einfach und vollautomatisch an Echtdaten aus der Produktion kommen, um die tatsächlich vorhandenen Risiken und potentiellen Verstöße gegen die gültigen Dienstanweisungen besser einschätzen und gegebenenfalls auch intern Ihren Handlungs- und möglichen Ressourcenbedarf untermauern können, möchten wir Ihnen an Hand folgender Projektskizze in Phasen exemplarisch darstellen:

Projektphase 1: "Einsammeln"
Vorhandene Risiken müssen identifiziert und in einer IST-Analyse zusammengefasst werden. Auf Basis dieses Datenmaterials erfolgt ein Abgleich mit allen bestehenden Richtlinien und Dienstanweisungen. Eine Schluss-Präsentation der Ergebnisse (eventuell mit einem Auditbericht) zeigt dann die Auswertung der Daten und die daraus resultierende Risikobewertung auf.

Projektphase 2: Ziele für Freiräume und das Sicherheits- und Systemmanagement definieren
Informationssicherheit muss nicht kompliziert sein, sollte jedoch die Unternehmenskultur abbilden und angemessenen Schutz flächendeckend ermöglichen. Rein organisatorische IT Sicherheitsmaßnahmen können nur dann wirksamen Schutz bieten, wenn diese technisch untermauert werden. Durch die Auswahl geeigneter Produkte und Technologien ist eine zusätzliche Arbeitsbelastung im Betrieb und in der Administration nicht zwingend notwendig.

Projektphase 3: Weicher Roll-Out
Viele Administratoren fürchten den Tag an dem eine strengere Sicherheitsrichtlinie in Kraft tritt und bestimmte, bislang geläufige Aktionen für die Benutzer unterbunden werden. Wenn etwa einem "VIP"-Nutzer bestimmte Berechtigungen entzogen wurden, dann ist mindestens ein Telefonat bei dem zuständigen Administrator vorhersehbar. Daher kommunizieren Sie mit dem User bereits während des weichen Roll-Outs im jeweils gewünschten Detaillierungsgrad, dies fördert zudem die Awareness der Anwender und schafft somit einen wichtigen Beitrag zur Sicherheitskultur im Unternehmen.

Projektphase 4: "Scharfschalten"
Sobald die Policy, die vorher "nur" gemeldet hat oder Daten über Art und Umfang von Transaktionen an die Zentrale geliefert hat, scharf geschalten ist, sollten Änderungen revisionssicher protokolliert werden.

4 ISMS-Normen und -Standards

4.1 ISO 27001

Die allgemeinen Anforderungen an ein Informationssicherheitsmanagementsystem werden in der Internationalen Norm ISO/IEC 27001 definiert. Die Norm geht auf den 1995 publizierten Britischen Standard BS 7799 zurück. Der Gedanke des Managementsystems und die Möglichkeit zur Zertifizierung eines ISMS kam im Jahre 1999 mit Teil 2 des BS 7799, aus dem 2005 die heutige ISO/IEC 27001 entstand.

Dem Wunsch nach einer internationalen Norm folgend, wurde aus Teil 1 des BS 7799 im Jahr 2000 die ISO/IEC 17799, die später in die heutige ISO/IEC 27002 umbenannt wurde.

ISO/IEC 27001 legt allgemeine Anforderungen an ein ISMS fest. Die konkrete Umsetzung wird bewusst offen gelassen. Daneben verfügt die Norm über mehrere Anhänge. Im normativen Anhang A werden in 11 Themengebieten insgesamt 133 Maßnahmen (Controls) zur Verfügung gestellt, die analog zu ISO/IEC 27002 strukturiert sind. ISO/IEC 27002 gibt dabei Anleitungen und Hinweise zur Umsetzung der Maßnahmen-Anforderungen aus ISO/IEC 27001 Anhang A. Die Anforderungen an das ISMS sind im sogenannten Management-Rahmen (Kap. 4 bis 8) der ISO/IEC 27001 formuliert.

In Analogie zu anderen Managementsystemen (z. B. Qualitätsmanagement nach ISO 9001) findet auch hier das "Plan-Do-Check-Act"-Modell (PDCA) Anwendung. Im Sicherheitsprozess wird die konkrete Umsetzung der Anforderung geplant, realisiert, überprüft und wenn notwendig angepasst/verbessert.

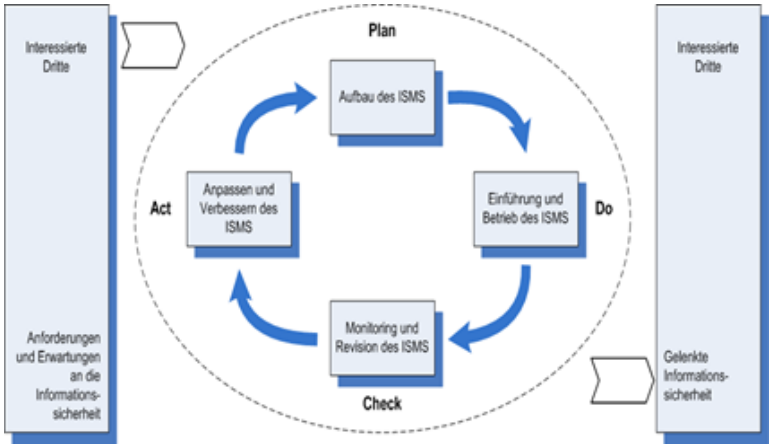

Abbildung 6: Managementsystem für Informationssicherheit

ISO 27001 verfolgt das Ziel des zuverlässigen und nachhaltigen Schutzes von Informationen als Werte einer Organisation vor Bedrohungen. Dabei ist es unerheblich in welcher Form die Informationen vorliegen. Es kann sich z. B. um gespeicherte Daten, Ausdrucke oder multimediale Inhalte handeln.

Gemäß dem beschriebenen PDCA-Modell bietet die Norm einen prozessorientierten Ansatz für Einrichtung, Betrieb, Überwachung und Aufrechterhaltung eines organisationsbezogenen Managementsystems für Informationssicherheit im Kontext der Geschäftsaktivitäten und Risiken.

In einem ersten Schritt muss hierfür der Geltungs- und Anwendungsbereich des ISMS abgegrenzt werden. Dieser entspricht nicht zwingend dem gesamten Unternehmen sondern kann auch einzelne Lokationen oder Geschäftsprozesse umfassen, wenn diese substantiell zum Unternehmenserfolg beitragen. Die Sicherheitsziele für den Anwendungsbereich werden definiert und in einer Sicherheitsleitlinie niedergeschrieben. Die Unternehmensleitung etabliert die Sicherheitsleitlinie als verbindliches Regelwerk und stellt darüber hinaus sicher, dass die Sicherheitsziele mit den Unternehmenszielen einhergehen.

Kern der Norm ist eine Risikoanalyse für den Anwendungsbereich des ISMS. In ihrem Verlauf wird zunächst der Schutzbedarf der Informationen unter Berücksichtigung aller Anforderungen ermittelt. Hierbei spielen gesetzliche oder vertragliche Regelungen, aber auch der Stellenwert der Information für das jeweilige Unter-

nehmen eine Rolle. Im Weiteren werden alle auf die Informationen wirkenden Bedrohungen, vorhandene Schwachstellen und bereits existierende Gegenmaßnahmen identifiziert. Die Maßnahmen aus ISO/IEC 27002 und zugehörigen Anforderungen aus Anhang A der ISO/IEC 27001 geben eine Auswahl an möglichen Gegenmaßnahmen vor. Aus der Kombination von Bedrohungen, Schwachstellen und Gegenmaßnahmen werden eventuelle Restrisiken abgeleitet und der Unternehmensleitung vorgelegt. Dem Management obliegt die Entscheidung, wie mit den verbleibenden Risiken umgegangen wird. Die Gesamtverantwortung für die Informationssicherheit und die damit verbundenen Risiken verbleibt beim obersten Management.

Wie auch im Qualitätsmanagement stellt der Standard Anforderungen an die Lenkung von Dokumenten und Aufzeichnungen. Für jedes Schriftstück müssen Verfasser, Revision und Änderungen, sowie Freigaben mit Datum nachvollzogen werden können.

Für den Anwendungsbereich des ISMS muss immer eine aktuelle Version der Definition des Anwendungsbereichs, der Sicherheitsziele, der Sicherheitspolitik, der Maßnahmenbeschreibungen sowie der unterstützenden Maßnahmen und Prozesse vorliegen. Darüber hinaus ist festzulegen, welche Risikoanalyse-Methode zur Anwendung kommt. Ihr Ergebnis und der Risikobehandlungsplan sind zu dokumentieren. Alle Maßnahmen, die gemäß der durchgeführten Risikoanalyse zur Anwendung kommen, müssen in der sogenannten "Erklärung zur Anwendbarkeit" (engl.: Statement of Applicability) aufgeführt und begründet werden. Auch alle Methoden, die zur Planung, Durchführung und Messung des ISMS herangezogen werden, sind zu dokumentieren.

Ein zentraler Punkt für den Erfolg eines Managementsystems für Informationssicherheit ist die Unterstützung durch das oberste Management. Hier zeigt sich einmal mehr, dass es sich bei Informationssicherheit nicht um eine primär technische Angelegenheit handelt. Die ISO/IEC 27001 fordert von der Unternehmensleitung ausreichende finanzielle und personelle Ressourcen zur Verfügung zu stellen und alle Mitarbeiter für die Belange der Informationssicherheit zu sensibilisieren. Das Managementsystem für Informationssicherheit muss durch die Unternehmensleitung kontinuierlich überprüft, bewertet und gegebenenfalls angepasst und verbessert werden. Dazu gehören auch regelmäßige Audits, die neben dem Managementsystem für Informationssicherheit gemäß Managementrahmen auch die anwendbaren Controls der ISO/IEC 27001 prüfen.

4.2 IT-Grundschutz

Einen weiteren Ansatz für ein Managementsystem für Informationssicherheit bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem "IT-Grundschutz". Dieser Ansatz ist laut BSI vollständig kompatibel zu ISO/IEC 27001 und berücksichtigt auch die Empfehlungen der ISO/IEC 27002. Die Methodik des IT-Grundschutz ist in vier IT-Grundschutz-Standards festgelegt. Der BSI Standard 100-1 beschreibt Managementsysteme für Informationssicherheit. Wie auch bei der ISO/IEC 27001 ist das Informationssicherheitsmanagement ein Prozess und Teil des unternehmensweiten Risikomanagements. Die praktische Umsetzung des IT-Grundschutzes wird in BSI Standard 100-2 dargestellt. Dieser Teil des Standards bildet den Kern der Vorgehensweise nach IT-Grundschutz. Eine Risikoanalyse auf der Basis von IT-Grundschutz ist in BSI Standard 100-3 beschrieben. Der BSI Standard 100-4 zum Notfallmanagement bietet darüber hinaus einen Ansatz für den systematischen Aufbau eines organisationsweiten Business Continuity Management.

Mit der IT-Grundschutz-Methodik will das BSI die Implementierung eines ISMS durch ein hohes Maß an Standardisierung vereinfachen. Für den definierten Anwendungsbereich (Informationsverbund) werden anhand der Geschäftsprozesse die dort verarbeiteten und zu schützenden Informationen ermittelt.

Im Rahmen der Strukturanalyse werden dann alle Ressourcen (Anwendungen, Infrastruktur, Netze, Server, Clients etc.) erfasst, von denen diese Geschäftsprozesse und Informationswerte abhängen. Gleichartige Ressourcen können dabei zu Gruppen zusammengefasst werden.

Im zweiten Schritt wird der zugehörige Schutzbedarf bestimmt. IT-Grundschutz unterscheidet zwischen drei Stufen des Schutzbedarfs bezogen auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit: "Normal", "Hoch" und "Sehr Hoch". Der Schutzbedarf der Informationen vererbt sich auf alle Ressourcen, die an ihrer Verarbeitung beteiligt sind; d.h. auf Anwendungen, von dort auf benötigte IT-Systeme und von dort wiederum auf die zugehörigen Räumlichkeiten und Gebäude.

Zur Abbildung des Informationsverbunds (Modellierung) existieren im IT-Grundschutz derzeit ca. 80 sog. IT-Grundschutzbausteine. Sie bestehen aus typischen objektspezifischen Gefährdungen und gefährdungsmindernden Maßnahmen. Für jeden Baustein wurde bereits in der Entwicklung eine Risikoanalyse durchgeführt, so dass eine Umsetzung der Maßnahmen ein ausreichendes Schutzniveau für den normalen Schutzbedarf darstellt. Diese Bausteine sind in fünf Schichten gegliedert: Schicht 1 enthält Bausteine mit übergreifenden Aspekten (z.B. Personal), Schicht 2 behandelt die baulich physikalische Infrastruktur (z.B. Serverraum), IT-Systeme sind auf Schicht 3 zu finden (z.B. Client unter Windows XP), Schicht 4 bedient Netze (z.B. VPN) und Schicht 5 Anwendungen (beispielsweise Datenbanken). Wie schon die Bausteine selbst sind alle Gefährdungen und Maßnahmen thematisch sortiert in den Gefährdungs- und Maßnahmenkatalogen der IT-Grundschutz-Kataloge zusammengefasst.

Hat die Schutzbedarfsanalyse für einzelne Bereiche des Informationsverbunds einen hohen oder sehr hohen Schutzbedarf ergeben, oder sind Ressourcen nicht durch IT-Grundschutzbausteine abgedeckt, müssen in einer erweiterten Sicherheitsanalyse und Risikoanalyse Gefährdungen und mindernde Maßnahmen ermittelt werden. Hierzu können die Gefährdungs- und Maßnahmenkataloge und die Vorgehensweise aus dem BSI-Standard 100-3 verwendet werden.

Ist der Informationsverbund vollständig abgebildet, werden alle Maßnahmen im Sicherheitskonzept konsolidiert. Der Sicherheitszustand und der Umsetzungsgrad der Maßnahmen wird im Rahmen des Basissicherheitschecks ermittelt. Für alle nicht oder nur teilweise umgesetzten Maßnahmen werden Umsetzungspläne entwickelt. Risikoanalysen, insbesondere deren Ergebnisse und verbleibende Restrisiken werden in einem Managementreport zusammengefasst, kommuniziert und sind von der obersten Leitung zu tragen.

Das BSI unterscheidet bei der Einstufung der Maßnahmen nach unterschiedlichen Priorisierungen. Alle Maßnahmen der Stufe A sind essentiell für die Sicherheit und daher vorrangig umzusetzen. Mit B gekennzeichnete Maßnahmen sind wichtig für den Aufbau einer kontrollierbaren Informationssicherheit und sollten daher auch schnellstmöglich umgesetzt werden. Hat das ISMS einen solchen Reifegrad auf Stufe A oder B erreicht, besteht bereits die Möglichkeit, diesen Meilenstein durch ein entsprechendes Testat eines unabhängigen, vom

BSI zugelassenen Auditors zu dokumentieren. Für eine Zertifizierung nach ISO/IEC 27001 auf Basis von IT-Grundschutz sind zusätzlich auch Maßnahmen der Stufen C (Zertifizierungsstufe) umzusetzen.
Außerdem enthalten die IT-Grundschutz-Kataloge noch mit Z gekennzeichnete Maßnahmen, die aufgrund von Risikoanalysen oder bei höheren Sicherheitsanforderungen zusätzlich herangezogen werden können. Mit W gekennzeichnete Maßnahmen dienen darüber hinaus vornehmlich der Wissensvermittlung.
Der BSI-Standard 100 zum IT-Grundschutz wie auch die zugehörigen IT-Grundschutz-Kataloge sind auf den Webseiten des BSI frei verfügbar. Die IT-Grundschutz-Kataloge werden typischerweise jährlich überarbeitet. Darüber hinaus publiziert das BSI zahlreiche Hilfsmittel, Studien und weitere Dokumente, die den IT-Grundschutz sinnvoll ergänzen und den Entwicklungen der Technik und Informationssicherheit Rechnung tragen.

4.3 COBIT

Die "Control Objectives for Information and related Technology" (COBIT) der Information Systems Audit and Control Association (ISACA) wurden erstmalig 1996 als Werkzeug für IT-Prüf- und Auditaufgaben veröffentlicht. Seitdem sind in den Folgeversionen systematisch zusätzliche Kontroll- und Managementaufgaben hinzugefügt worden. Die Bedeutung der IT für das Business des Unternehmens sowie der Wert von Unternehmensinformationen wurden in den Fokus gerückt und die Struktur von COBIT entsprechend optimiert. So präsentiert sich COBIT 5 seit April 2012 als ein umfassendes Framework, das Unternehmen dabei unterstützt, durch eine effektive Governance of Enterprise IT (GEIT) ihre Geschäftsziele zu erreichen und die erwünschten Mehrwerte zu generieren. Ziel ist dabei eine ganzheitliche, integrative und komplette Sicht auf Governance und Management der IT.

Alle wesentlichen ISACA Frameworks und Leitlinien, wie z.B. Val IT oder Risk IT, wurden in COBIT 5 integriert. Ebenso ist das Framework kompatibel zu etablierten internationalen Frameworks und Standards, z.B. ITIL, PRINCE2, ISO 27001, ISO 20000, ISO 38500 etc.).

Die aktuelle Version vermeidet nun die o.g. "Langform" von COBIT, da es die bisherigen "Control Objectives" in dieser Form nicht mehr gibt.

Die Kernelemente des COBIT 5-Frameworks sind:

- 5 Prinzipien;
- Enabler, bestehend aus Unternehmenswerten, Prozessen und Organisationsstrukturen;
- Lebenszyklusmodell zur Implementierung.

Die 37 COBIT-Prozesse sind in 5 Domänen strukturiert:

- Evaluate, Direct and Monitor (Governance-Ebene) (EDM)
- Align, Plan and Organize (APO)
- Build, Acquire and Implement (BAI)
- Deliver, Service and Support (DSS)
- Monitor, Evaluate and Asses (MEA).

Dazu bietet COBIT Ansätze zur Messung und Steuerung der Zielerreichung, unterstützt durch ein Reifegradmodell.

Aus dem Umfeld der Informationssicherheit existieren z.B. folgende Prozesse:

- APO13 Manage security
- BAI05 Manage organizational change enablement
- BAI08 Manage knowledge
- BAI09 Manage assets
- DSS04 Manage continuity
- DSS05 Manage security service.

Desweiteren existiert eine Publikation "COBIT 5 for Information Security", wo mit großer Sorgfalt und Ausführlichkeit die gesamte COBIT 5 Architektur in den Blickwinkel der IS gedreht wird. IS-relevante Inhalte werden mit Hilfe der Enabler gefiltert und um zahlreiche wertvolle und praxisnahe Anleitungen ergänzt.

Auch wenn COBIT und ISO/IEC 27001 auf unterschiedlichen Ebenen ansetzen, ergeben sich durch die starke Überschneidung erhebliche Synergieeffekte. Einerseits kann eine Zertifizierung nach ISO/IEC 27001 als Nachweis für eine Teilerfüllung von COBIT herangezogen werden, andererseits liefern die Steuerungs- und Messmethoden in COBIT wertvolle Werkzeuge für den effektiven Betrieb eines ISMS.

4.4 Informationssicherheitsmanagement in ITIL

Die IT Infrastructure Library (derzeit ITIL Edition 2011) ist der De-facto-Standard im IT-Servicemanagement. Er fasst 'Good Practices' für die Erbringung von Dienstleistungen durch den Betrieb einer IT-Infrastruktur zusammen. ITIL Edition 2011 basiert auf dem PDCA-Prozessmodell und deckt die einzelnen Phasen durch fünf Hauptprozesse ab. Die "Servicestrategie" (Service Strategy) bildet den Entwurf, die Entwicklung oder die Implementierung des IT Service Managements als strategische Ressource inklusive der Definition von Zielen und Richtlinien. Diese umfasst sowohl organisatorische Aspekte als auch die strategische Ausrichtung. Der Prozess "Service Design" stellt Methoden und Grundsätze bereit, um die strategischen Ziele in Service Portfolios (Service Angebot) und Service Assets (Ressourcen und Fähigkeiten) umzusetzen. In der Phase "Serviceüberführung" (Service Transition) werden neu designte und geänderte Services in den Betrieb überführt. Der "Servicebetrieb" (Service Operation) gewährleistet einen dauerhaft gleichbleibenden, effektiven und effizienten Betrieb der angebotenen Services. Der Prozess "Kontinuierliche Serviceverbesserung" (Continual Service Improvement) ermöglicht eine dauernde Verbesserung aller Services und Service-Assets um notwendige Korrekturmaßnahmen einzuleiten und eine dauerhafte Wertschöpfung zu erhalten.

Das Informationssicherheitsmanagement ist Bestandteil des "Service Design". Da sowohl ITIL Edition 2011 als auch die ISO/IEC 27001 auf dem gleichen Lebenszyklusmodell basieren fügen sie sich gut ineinander. ITIL 2011 verweist auf den Standard ISO/IEC 27001 für die Implementierung eines Informationssicherheitsmanagements. Zusätzlich werden die Anforderungen mit Fokus auf das Servicemanagement konkretisiert.

ITIL liefert also Best Practices auf allen Management-Ebenen der IT sowie auf allen Sachebenen beginnend bei der Geschäftsausrichtung, über die Servicegestaltung und Gewährleistung der Informationssicherheit bis hin zum Betrieb von Anwendungen und Infrastruktur und dem hiermit verbundenen Technologieeinsatz. Wichtig ist die Einbettung des Sicherheitsprozesses in die Prozesslandschaft des Unternehmens. Beispielhaft sind hier die Schnittstellen zu mehreren Prozessen kurz dargestellt.

Incident und Problem Management
Hier ist die Aufgabe des Sicherheitsmanagements, sicherheitsrelevante Vorfälle zu bewerten und an einer zukünftigen Vermeidung mitzuarbeiten.

Change Management
Beteiligung des Sicherheitsmanagements an der Beurteilung der Auswirkungen von anstehenden Änderungen auf Sicherheitsbelange.

Service Asset and Configuration Management
Hierbei liefert die Configuration Management Database (CMDB) / das Configuration Management System (CMS) aktuelle und vollständige Asset-Informationen. Auch sollte hier eine Klassifizierung der Assets hinsichtlich ihres Schutzbedarfes vorgenommen werden.

Service Level Management (SLM)
Gibt Unterstützung bei der Ermittlung von IS-Anforderungen. SLM dient ferner zum Festschreiben spezieller IS-Anforderungen in Service Level Agreements (SLA), Operational Level Agreements (OLA) etc. und kann ferner auch zur Pflege von IT-Services bzgl. deren IS-Funktionalität verwendet werden.

Availability und Capacity Management dienen der Berücksichtigung der Sicherheitsanforderungen bzgl. Verfügbarkeit und Kapazität beim Service-Design. Durch Analyse von Monitoring-Daten wegen auftauchender Anomalien lassen sich oftmals Rückschlüsse auf Sicherheitslücken ziehen.

IT Service Continuity Management wird oftmals in engem Zusammenhang mit der Business Impact Analyse (BIA) sowie mit dem Risk Assessment gesehen. Beispielsweise ist ein Notfallplan eine notwendige Voraussetzung für ein ISMS nach ISO 27001.

Financial Management dient als solide Grundlage für die Planung ausreichender Budgets für ein ISMS. Ferner dient es zur Ermittlung, Zuordnung und ggf. Verrechnung der Kosten von IS-Maßnahmen.

Somit ergänzen sich Informationssicherheitsmanagementsysteme und die IT Infrastructure Library (ITIL) in sinnvoller Weise.

Über die Anforderungen der ISO 27001 hinaus bietet die IT Infrastructure Library ferner Anregungen zur Bewertung der Effektivität und Effizienz an Hand von Messgrößen (Key Performance Indicators; KP), um eine Steuerung des Informationssicherheitsmanagements zu ermöglichen.

4.5 IS-Risikomanagement

Ein ISMS ist ohne ein Risikomanagementsystem gar nicht denkbar. Wie soll man – ohne sich seiner Risiken bewusst zu sein – wissen, welche Sicherheitsmaßnahmen man braucht und in welcher Priorität diese umzusetzen sind. IS-Risikomanagement muss in die bestehenden Unternehmensprozesse, wie IS-Management, Unternehmens- und IT-Strategie eingegliedert und angepasst werden sowie den Einklang mit dem operativen Betrieb finden.

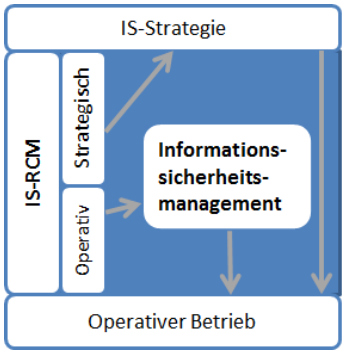

Abbildung 7: Zusammenhang zwischen ISM und IS-RCM

Der Standard ISO/IEC 27005 enthält Leitlinien für ein systematisches und prozessorientiertes Risikomanagement. Der Standard kann für Risikomanagement, das mit den Anforderungen der ISO/IEC 27001 kompatibel sein soll, genutzt werden. Der vollständige Prozess nach ISO/IEC 27005 ist in Abbildung 8 dargestellt.[3]

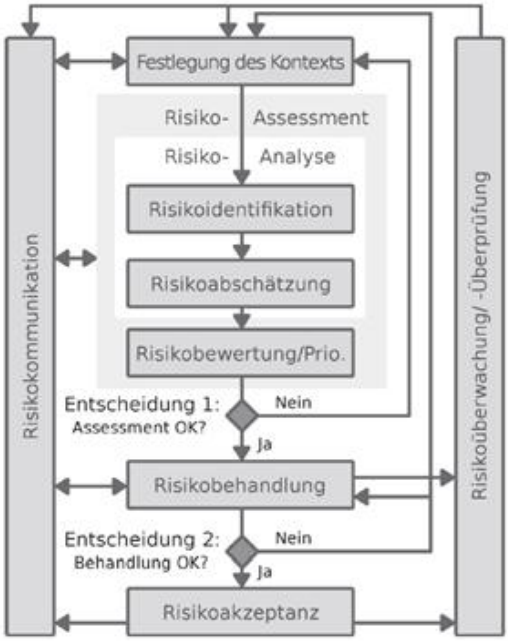

Abbildung 8: Der vollständige Risikomanagementprozess (Quelle: KLIPPER)

Neben ISO 27005 ist der BSI Standard 100-3 "Risikoanalyse auf Basis von IT-Grundschutz" eine sehr wichtige Grundlage für das Management von Sicherheitsrisiken, die gerade in der Risikoidentifizierung einen wert-

[3] KLIPPER, Sebastian: Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010. Vieweg+Teubner, 2011. – ISBN 9783834813602

vollen Dienst erweisen kann. Darüber hinaus gibt es für die Behandlung von Risiken in Organisationen zahlreiche weitere Standards und Vorgehensweisen, wie z.B. ISO 31000 oder das Risikomanagementframework COSO ERM des Committee of Sponsoring Organizations of the Treadway Commission (COSO). Ein Framework für das Management von IS-Risiken im Allgemeinen stellt das "Risk IT Framework" von ISACA dar. Auch mit dem "Risk Management Guide for Information Technology Systems" des NIST wurde ein standardisiertes Vorgehen zum IS-Risikomanagement beschrieben. Dabei erfolgt die Einschätzung eines IS-Risikos zumeist auf Basis der zu erwartenden Auswirkungen auf die Schutzziele (Integrität, Vertraulichkeit, Verfügbarkeit) und der daraus resultierenden Kosten bzw. des resultierenden Schadens.

Für die Berücksichtigung von Risiken und Chancen im Managementprozess ist die Bewertung ausschlaggebend, die sich vereinfacht in zwei Faktoren ausdrückt:

Die Höhe der Eintrittswahrscheinlichkeit (geschätzt und plausibel) und das Verhältnis von Risiko und Chance (nicht jedes Risiko und jede Chance ist würdig, gemanagt zu werden: z.B. "Firmenvernichtung durch einen Vulkanausbruch in Deutschland": denkbar, aber unrealistisch). Der Grad der Beeinflussbarkeit der Chance und des Risikos durch das Unternehmen und der dazu notwendige Aufwand.

Nur solche Risiken und Chancen, die aktiv beeinflussbar sind, werden in das Risiken- und Chancen-Portfolio aufgenommen. Solche, die davon wiederum in dem wirtschaftlich vertretbaren Ausmaß beeinflussbar sind, werden selbst gemanagt. Es existieren grundsätzlich vier klassische Risikobegegnungsstrategien und zwar:

1. Risikovermeidung – Verzicht auf die risikobehaftete Handlung. Allerdings vermeidet dies auch die Nutzung der eventuell verbundenen Chancen.
2. Risikominderung (aktives Reduzieren des Risikos) - Verringerung des möglichen eintretenden Schadens bzw. der Wahrscheinlichkeit des Eintritts oder beides gleichzeitig, um die Wahrscheinlichkeit des Gelingens zu erhöhen bzw. die Folgen abzumildern.
3. Risikotransfer (Überwälzen des Risikos) - Ein Dritter, z.B. Versicherung, übernimmt die Schadenauswirkungen bei Eintreten eines Risikos.
4. Risikoakzeptanz (Eingehen des Risikos) - Das Risiko wird ohne weitere Behandlung hingenommen.

Der Umgang mit Risiken erfordert einen klar strukturierten Managementprozess und eine durchdachte Risikokommunikation mit einem klaren Schwerpunkt auf die menschliche Komponente. Da selbst wenn formal alles richtig ist und man nach einem Sicherheitsvorfall jemanden zur Rechenschaft ziehen kann – das Ziel den Sicherheitsvorfall zu verhindern, wurde trotzdem verfehlt. Da nur Risiken die angesprochen werden, können im Risikomanagementprozess bearbeitet und abgesichert werden. Gerade der Prozess (Risikomanagementprozess) und somit der Weg bezeichnet das Ziel des Risikomanagements, der auch wie der PDCA-Zyklus als Regelkreislauf dargestellt wird (s. Abbildung).

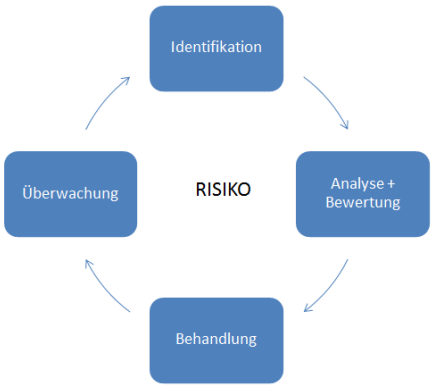

Abbildung 9: Prozesse des IS-RCM

4.6 Business Continuity Management

Für die Steuerung eines Unternehmens/einer Organisation ist es unabdingbar, im Rahmen des Business Continuity Managements (BCM) die Risiken von Unterbrechungen des Geschäftsbetriebs durch einen Notfall angemessen zu analysieren und zu behandeln.

ISO 22301 spezifiziert entsprechende Anforderungen zum Aufbau und Management eines effektiven und dokumentierten Business Continuity Management Systems (BCMS) und unterstützt damit Unternehmen bei BCM-Aufgaben.

Ein BCMS legt besonderen Wert auf folgende Aspekte:

- Verständnis der Anforderungen einer Organisation und der Notwendigkeit, eine Leitlinie und Ziele für das Business Continuity Management (BCM) zu etablieren;
- Implementierung und Betrieb von Maßnahmen zum Management von Unterbrechungen des Geschäftsbetriebs durch einen Notfall innerhalb der Organisation;
- Überwachung und Review der Leistungsfähigkeit eines BCMS;
- Kontinuierliche Verbesserung auf der Basis objektiver Messungen.

Als Managementsystem hat ein BCMS folgende Hauptkomponenten:

- Leitlinie;
- Rollen und Verantwortlichkeiten;
- Management-Prozess in der Struktur des PDCA-Modells;
- Audit-fähige Dokumentation;
- Weitere BCM-Prozesse, die für die Organisation relevant sind.

Durch die PDCA-Struktur ist ein BCMS nach ISO 22301 kompatibel zu anderen bekannten Managementsystemen wie ISO 9001, ISO 14001, ISO 27001 oder ISO 20000, was einen integrierten Aufbau und Betrieb innerhalb des Unternehmens ermöglicht.

ISO 22301 ist die erste internationale und zertifizierungsfähige BCM-Norm. Sie wird den derzeit geläufigen Standard BS 25999-2 ablösen. Zertifikate nach BS 25999-2 behalten noch bis Mitte 2014 ihre Gültigkeit. Analog zum BS 25999-1 wird voraussichtlich Anfang 2013 die ISO 22313 als Anleitung zur Umsetzung der ISO 22301 erscheinen.

Eine wichtige Komponente innerhalb des BCM-Prozesses ist die Business Impact Analyse (BIA). Hierbei werden die Auswirkungen von Geschäftsunterbrechungen auf Produkte und Dienstleistungen ermittelt und daraus Prioritäten für den Wiederanlauf abgeleitet. Dabei werden die kritischen Geschäftsprozesse und die zeitabhängigen Folgen ihres Ausfalls analysiert, ebenso wie Abhängigkeiten zwischen diesen Prozessen und erforderliche Ressourcen, um sie nach einer Geschäftsunterbrechung auf einem "Notbetriebsniveau" betreiben zu können.

Eine BIA liefert einen detaillierten Einblick in die Zusammenhänge zwischen den Risiken einerseits und den Auswirkungen eines Schadensfalls auf die Geschäftstätigkeit einer Organisation andererseits. Durch eine BIA können die Auswirkungen bei Ausfällen von Prozessen ermittelt werden; damit ist sie eine Grundlage für Notfall- und Wiederanlaufplanung. Als Ergebnis liefert eine BIA die max. tolerierbare Ausfallzeit pro betrachteten Prozess incl. seiner Ressourcen.

Im Folgenden wird das Vorgehen der BIA gemäß BSI-Standard 100-4: Notfallmanagement dargestellt. Dieser Standard vereint Elemente und Empfehlungen aus dem British Standard 25999 sowie dem ITIL Service Continuity Management mit den relevanten Maßnahmen aus den IT-Grundschutzkatalogen und enthält alle wesentlichen Aspekte für ein angemessenes Business Continuity Management.

Gemäß BSI Standard 100-4 untergliedert sich die Durchführung einer Business Impact Analyse im Wesentlichen in folgende, in der Abbildung 10 dargestellte Teilschritte:

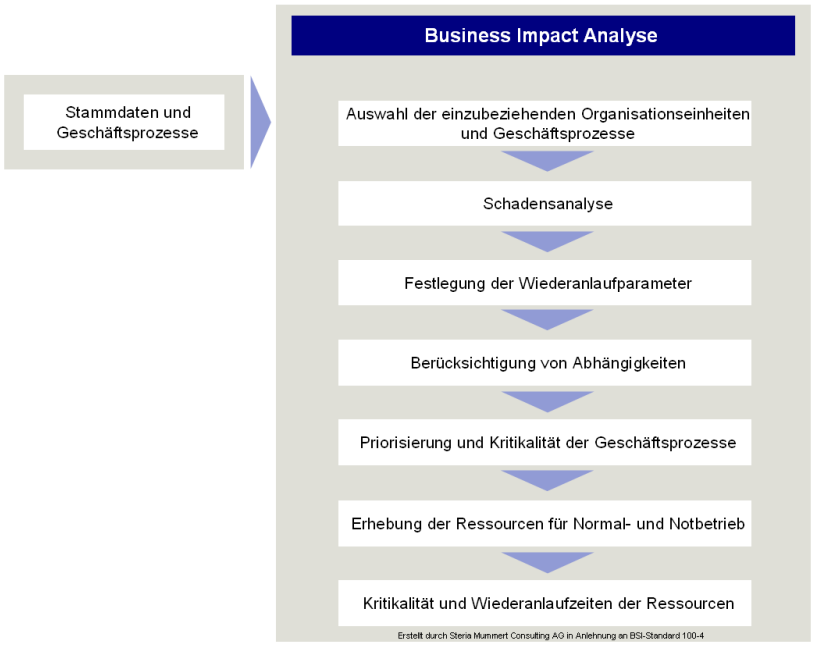

Abbildung 10: Ablauf Business Impact Analyse nach BSI 100-4

Stammdaten und Geschäftsprozesse

Es wird zunächst eine Übersicht aller relevanten Geschäftsprozesse der Organisation, möglichst mit den jeweils verantwortlichen Ansprechpartnern bzw. Prozessverantwortlichen, erstellt. Diese Erhebung sollte auch eine Verknüpfung der Prozesse mit den Unternehmenszielen sowie Querbezüge zwischen den Prozessen enthalten.

Auswahl der einzubeziehenden Organisationseinheiten und Geschäftsprozesse

Wird im Rahmen der Prozesserhebung ersichtlich, dass innerhalb des festgelegten Gültigkeitsbereichs des Notfallmanagements einige Geschäftsprozesse eine sehr geringe Bedeutung für das Erreichen der Geschäftsziele und der wertschöpfenden Prozesse des Geltungsbereichs besitzen, so können diese (unter entsprechender Argumentation) bei der weiteren Betrachtung ausgespart werden.

Schadensanalyse

In der Schadensanalyse wird der Schaden für den Geltungsbereich untersucht, der verursacht wird, wenn die Prozesse oder Ressourcen nicht wie vorgesehen zur Verfügung stehen. Dabei ist nicht nur die Höhe des Schadens, sondern insbesondere dessen zeitliche Entwicklung von Interesse. Für die Durchführung der Schadensanalyse müssen aussagekräftige Parameter (z.B. Schadenskategorien, Schadensszenarien, Betrachtungszeitraum) festgelegt werden. Als Ergebnis liefert die Schadensanalyse für jeden Prozess den Schaden, der sich aus dem Ausfall ergibt.

Festlegung der Wiederanlaufparameter

In Abhängigkeit von Schadenverlauf und zu erwartender Schadenshöhe wird definiert, wie hoch die maximal tolerierbare Ausfallzeit, die Wiederanlaufzeit und das Wiederanlauf-Niveau (d.h., welche Kapazität bezogen auf den Normalbetrieb ein vorübergehender Notbetrieb zumindest aufweisen sollte) für jeden Prozess ist. Die ermittelten Werte werden für den Geltungsbereich konsolidiert.

Berücksichtigung von Abhängigkeiten

Zur Ermittlung des Gesamtschadens müssen auch die Wechselwirkungen der Schäden zwischen den Prozessen bezogen auf die Ziele der Organisation betrachtet werden. Gegebenenfalls müssen die Wiederanlaufparameter angepasst werden.

Priorisierung und Kritikalität der Geschäftsprozesse

Anhand von zu definierenden Kritikalitätsstufen wird festgelegt, in welcher Reihenfolge die Geschäftsprozesse wieder anlaufen sollen.

Erhebung der Ressourcen für Normal- und Notbetrieb

Um sinnvolle Kontinuitätsstrategien entwickeln und Vorsorgemaßnahmen festlegen zu können, ist es notwendig, die von den kritischen Geschäftsprozessen genutzten Ressourcen zu identifizieren. Hierbei sind sowohl die Art der Ressourcen sowie die Relevanz der Ressourcen für den Normalbetrieb und den Notbetrieb zu erheben.

Kritikalität und Wiederanlaufzeiten der Ressourcen

Die Kritikalität und die Anforderung an den Wiederanlauf von Ressourcen leiten sich von der Kritikalität und den Wiederanlauf-Anforderungen der Prozesse ab, die diese Ressource nutzen. Bei dieser Festlegung ist auch zu berücksichtigen, dass eine Ressource von mehreren Prozessen genutzt werden kann, wodurch sich die Einstufung in der Regel erhöht.

Die in der Business Impact Analyse ermittelte Priorisierung der kritischen Prozesse und Ressourcen einer Organisation bilden die Grundlage für ein funktionierendes Notfallmanagement. In Notfall- und Wideranlaufplänen sollten Prozessen und Ressourcen mit höchster Kritikalität als erstes wiederhergestellt werden, um die negativen Auswirkungen des Ausfalls auf ein Minimum zu reduzieren.

5 Rechtliche Aspekte[4]

Ganzheitliche IS erfordert technisch-organisatorische Maßnahmen wie Handlungsanweisungen, Verfahrens- und Nutzungsrichtlinien sowie die Einhaltung rechtlicher Rahmenbedingungen. Ergänzt wird dies durch ein vorzugsweise zertifiziertes Risikomanagement einschließlich Mitarbeiterschulung, das durch die Entscheidungsträger eines Unternehmens bzw. einer Organisation umzusetzen ist. Dies dient auch der Vermeidung von Haftungstatbeständen.

Ganzheitliche Informationssicherheit umfasst:

- Organisatorische Sicherheit (Risikomanagement, Nutzungsrichtlinien, Kontrolle, Schulung);
- Rechtliche Sicherheit (Vertragsgestaltung, AGB, Vermeidung straf- und zivilrechtlicher Haftung bzw. Organisationsverschulden, Betriebsvereinbarungen);
- Technische Sicherheit (Archivierung, Backup, Firewall, Filter, Verschlüsselung, Authentifizierung);
- Wirtschaftliche Sicherheit.

Der BGH verwendet in Zusammenhang mit dem Haftungsrecht den Begriff "Verkehrssicherungspflichten": "Wer eine Gefahrenquelle eröffnet oder sich an ihr beteiligt, muss Dritte schützen und hierfür geeignete Schutzmaßnahmen ergreifen". Die IT-gestützten Kommunikationsvorgänge (z.B. in Intranet und Internet) eröffnen vielfältige Gefahren und sind demnach Gefahrenquellen im Sinne der Verkehrssicherungspflichten.
Diese Verkehrssicherungspflichten bestehen im Wesentlichen aus:

- Organisationspflichten bezüglich betrieblicher (technischer) Abläufe und
- Aufsichtspflichten des Arbeitgebers gegenüber seinen Mitarbeitern.

Eine vollständige Sicherheit kann im Rahmen der Verkehrssicherungspflichten nicht verlangt werden, jedoch solche Maßnahmen, die wirtschaftlich zumutbar sind. Vertraglichen Schutzpflichten richten sich nach den Verkehrssicherungspflichten. Solche Verkehrssicherungspflichten ergeben sich aus einer Vielzahl gesetzlicher und vertraglicher Bestimmungen sowie der Rechtsprechung, z.B.

[4] Zusammengestellt unter Verwendung von: SPEICHERT, Horst: IT-Rechtsleitfaden (http://www.bluecoat.de/leitfaden/IT-Rechtsleitfaden_BCS.pdf)

- "Garantenstellung" nach § 13 StGB: Straftaten können auch durch Unterlassen von Sicherungsmaßnahmen, Verletzung von Sorgfaltspflichten begangen werden;
- § 9 BDSG plus Anlage (Diese Vorschrift enthält die Grundsätze ordnungsgemäßer Datenverarbeitung, also Vorgaben für die technisch-organisatorische Datensicherheit.);
- bei Amts-, Berufs- und Privatgeheimnissen, § 203 StGB;
- bei Geschäfts- und Betriebsgeheimnissen, § 17 UWG;
- besondere Verschwiegenheitsverpflichtungen und strafbewehrte Garantenstellung für besonders sensible Daten.

Es ist ein technisches Sicherheitskonzept zu entwickeln, das Unbefugten Zugriff auf personenbezogene Daten verhindert. Im Einzelnen bedeutet dies:

- Authentifizierung;
- Festplattenverschlüsselung;
- Verfügbarkeitskontrolle (Virenschutz, Backup, sichere Archivierung);
- Weitergabekontrolle (Datensicherung, Verschlüsselung);
- Zugangskontrolle (Passwort, Firewall);
- Zugriffskontrolle (effektive, rollenbasierte Rechteverwaltung);
- Zutrittskontrolle (räumliche, physische Sicherung).

Die Vermeidung persönlicher Eigenhaftung ist für die handelnden Mitarbeiter, wie Leiter von IT-Abteilungen, Sicherheitsbeauftragte, Administratoren und sonstige IT-Verantwortliche entscheidend. Hierbei ist zu unterscheiden zwischen

- arbeitsrechtlicher Haftung (Abmahnung, Kündigung);
- strafrechtlicher Haftung (Geld- oder Freiheitsstrafe);
- zivilrechtlicher Haftung (Schadensersatz).

Abgeleitet aus dem Arbeitsvertragsverhältnis hat jeder Mitarbeiter arbeitsvertragliche Nebenpflichten (Schutz-, Mitwirkungs-, Geheimhaltungs- und Aufklärungspflichten). Sorgfaltsmaßstab ist ein "besonnener Mensch mit durchschnittlichen Fähigkeiten in der Situation des Arbeitnehmers". Bei leitenden Mitarbeitern gelten höhere Sorgfaltsanforderungen.

Schadensersatzansprüche des Arbeitgebers wegen Verletzung arbeitsvertraglicher Nebenpflichten sind in der Praxis in seltenen Fällen zwar möglich, aber wegen der Fremdbestimmtheit der Arbeitsleistung trägt der Arbeitgeber grundsätzlich das Unternehmensrisiko. Für Arbeitnehmertätigkeiten mit erhöhtem Risiko gelten deshalb (Rechtsprechung des BAG) die Grundsätze zur sog. schadensgeneigten Tätigkeit:

- für vorsätzliches/grobfahrlässiges Verhalten: volle Haftung des Mitarbeiters;
- mittlere Fahrlässigkeit: Schadensteilung zwischen Arbeitgeber und Mitarbeiter;
- leichte Fahrlässigkeit: keine Haftung des Mitarbeiters.

Diese Haftungserleichterung für den Mitarbeiter gilt grundsätzlich nur im Verhältnis zum Arbeitgeber. Im Verhältnis zu geschädigten Dritten besteht ein Freistellungsanspruch des Arbeitnehmers gegen den Arbeitgeber.

Für eine mögliche Strafbarkeit gilt dagegen der Grundsatz der vollständigen Eigenverantwortung. Ein Arbeitnehmer macht sich also selbst strafbar, die arbeitsvertragliche Haftungserleichterung ist nicht anwendbar. Auch ein "Befehlsnotstand" kann nicht angeführt werden.

Zur Vermeidung von Eigenhaftung kann ein verantwortlicher Mitarbeiter nachfolgende Maßnahmen zum Selbstschutz ergreifen:

- Gewissenhafte Aufgabenerfüllung;
- Hinzuziehung externer Berater;
- Lösungsvorschläge für Sicherheitsmängel erarbeiten, Projekte vorschlagen, angemessenes Budget beantragen;
- Regelmäßige Information der Geschäftsleitung über mögliche Risiken.

Als Reaktion bei Ablehnung vorgeschlagener Maßnahmen durch die Geschäftsleitung ist zu empfehlen:

- Risiken erneut aufzeigen;
- Vorgang des Vorschlags und der Ablehnung "protokollieren" bzw. dokumentieren;
- "Mitwisser" schaffen, z.B. durch E-Mail mit 'cc';
- schriftliche Bestätigung einfordern.

In erster Linie ist die Unternehmensleitung für ein effektives Risikomanagement verantwortlich, wozu auch das IS-Management zählt. Insbesondere müssen Gefahrenpotenziale erfasst, abgeschätzt und überwacht werden, damit Gefahren frühzeitig erkannt werden.

Der Umfang der Managementpflichten variiert je nach Gefahrenlage und Schadenspotenzial. Kommt die Unternehmensleitung ihren Pflichten nicht mit der gebotenen Sorgfalt nach, ergeben sich persönliche Haftungsrisiken der Verantwortlichen gegenüber dem Unternehmen oder gegenüber Dritten. Daher empfiehlt es sich, alle einschlägigen Veranlassungen zu dokumentieren.

6 Zusammenfassung

Permanente Effizienzsteigerungsanforderungen aufgrund der Herausforderungen der globalen Märkte erfordern effektive Geschäftsprozesse und abgesicherte Informationen. Die Werte eines Unternehmens sind neben Menschen, Infrastruktur und Kapital die Informationen. Ziel ist es, Prinzipien, Methoden und Werkzeuge zu finden, um Informationssicherheit zu beurteilen, zu rechtfertigen und optimal einzusetzen. Dabei sind die Kosten für Sicherheitsmaßnahmen und die Kosten für Schäden bzw. Schutzmaßnahmen so zu definieren, dass ein optimales Schutzniveau im Verhältnis zu dem Gesamtwert der zu schützenden Informationen vorhanden ist.

Die Einstufung sollte in Schutzklassen (Kapitel 3.1) erfolgen. Dabei ist nicht nur die Vertraulichkeit zu betrachten sondern auch die Verfügbarkeit und Integrität. Es wird viele Schutzmaßnahmen geben, die eine solche Betrachtung nicht benötigen sondern die Sicherheitsmaßnahmen nach den gegebenen Anforderungen umsetzen. Bei einer notwendigen Brandschutzanlage für ein Gebäude wird auch keine Kosten/Nutzen Betrachtung durchgeführt (die Auswirkungen einer späteren Nachrüstung können beim Großflughafenprojekt in Berlin betrachtet werden).

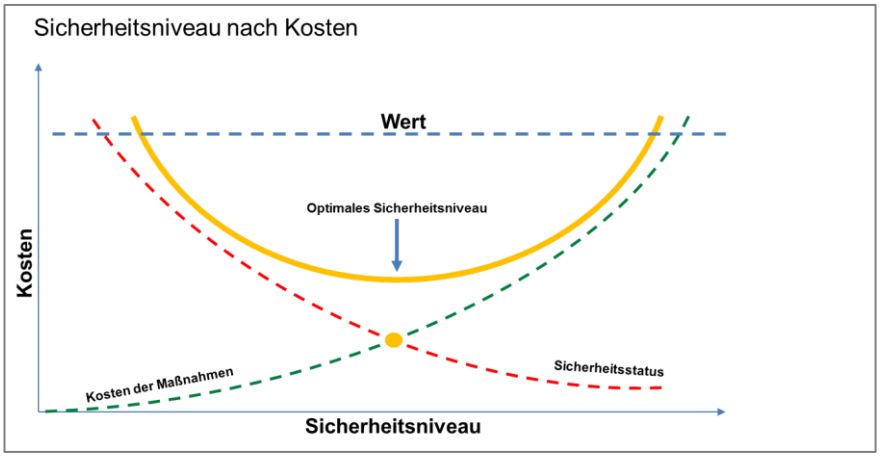

Abbildung 11: Darstellung des optimalen Sicherheitsniveaus

Mit dem Ansatz des ganzheitlichen Informationssicherheitsmanagementsystems wird herausgearbeitet, dass die Charakteristika von informationssichernden Maßnahmen genutzt werden können, um den Erfolg und den Nutzen im Vergleich zum klassischen "Es wird schon nichts passieren, es ist doch bisher auch nichts passiert" Vorgehen deutlich einfacher und schneller agieren zu können. Praxisrelevante Ergebnisse, Erkenntnisse und Handlungsempfehlungen für die Organisation werden permanent erarbeitet.

Die Methoden und praxiserprobten Vorgehensmodelle mit dem beschrieben Nutzen sind vorhanden und müssen nur umgesetzt werden.

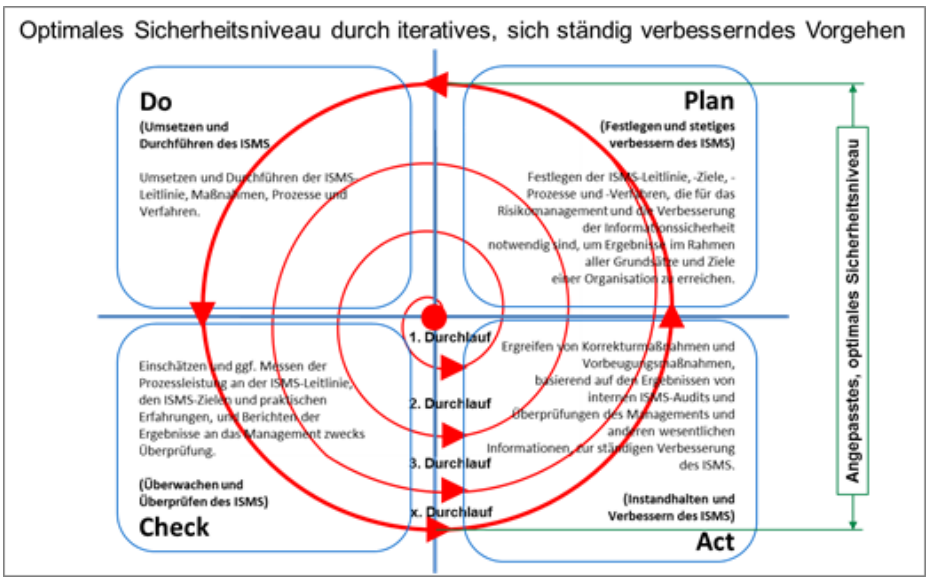

Abbildung 12: Informationssicherheitsphasen und Niveau

Das Vorgehen für das Informationssicherheitsmanagement ist in den dargestellten, internationalen Standards praxiserprobt vorhanden. Das Management kann kosteneffizient das Unternehmen nach gesetzlichen Vorgaben, den Anforderungen der Kunden und den eigenen Vorgaben ausrichten. Das optimale Sicherheitsniveau wird durch die konsequente Umsetzung der Plan-Do-Check-Act Methode erreicht. Sicherheit ist kein Projekt sondern ein Prozess. Erst durch einen eingeführten und gelebten Sicherheitsprozess wird das für die jeweilige Organisation optimale Sicherheitsniveau erreicht. Der Wettbewerbsvorteil wird sich im Unternehmenserfolg wiederfinden.

Es ist Zeit zu handeln, sonst handelt die Zeit!

Abkürzungsverzeichnis

BAG	Bundesarbeitsgericht
Basel II	Neue Baseler Eigenkapitalvereinbarung
BCM	Business Continuity Management
BDSG	Bundesdatenschutzgesetz
BGH	Bundesgerichtshof
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
BIA	Business Impact Analyse
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CMS	Configuration Management System
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
GRC	Governance, Risk and Compliance
ISMS	Information Security Management System/Informationssicherheitsmanagemtsystem
IS	Informationssicherheit
IS-Risiko	Informationssicherheitsrisiko
ISO	International Organization for Standardization
ITIL	IT Infrastructure Library
IT-RCM	IT-Risiko- und Chancen-Management
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KP	Key Performance lndicators
OLA	Operational Level Agreements
PDCA	"Plan - Do - Check - Act"
SLA	Service Level Agreements
SLM	Service Level Management
SOX	Sarbanes-Oxley Act
StGB	Strafgesetzbuch
UWG	Gesetz gegen den unlauteren Wettbewerb

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; Bereitstellung von Public-Key-Zertifikaten für sichere E-Mailkommunikation), des Expertenzertifikates "TeleTrusT Information Security Professional" (T.I.S.P.) sowie des Qualitätszeichens "IT Security made in Germany". Hauptsitz des Verbandes ist Berlin. TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI).

Kontakt:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
http://www.teletrust.de

TeleTrusT
Pioneers in IT security.