Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher und Jan W. Meine
Meine Verlag – Wissenschafts-, Sach- und Fachbuchverlag, Magdeburg

Eine DIN für IT-Sicherheit?

Dr. Hubert Feyrer

Es wird ein Überblick über zentrale Begriffe sowie existierende Gesetze und Normen für den Bereich IT-Sicherheit gegeben. Dem folgt eine Vorstellung des Informationssicherheitsmanagements nach ISO 27001, inklusive Betrachtung der technischen und organisatorischen Maßnahmen, aber auch der Integration des Faktors Mensch und des Managements von Risiken. Es wird gezeigt dass hier nicht nur eine DIN für IT-Sicherheit vorliegt, sondern ein internationaler Standard, der alle Bereiche der Informationssicherheit abdeckt.

Zitationsvorschlag: **mjs:Feyrer:DIN**

Einführung

Täglich erschüttern Medienberichte über Unfälle, Sabotage und Angriffe mit IT-Anteil - bis hin zum Cyberkrieg - die Medien. Spätestens seit der Bankrotterklärung der Antiviren-Industrie[1], dass diese viele Viren prinzipiell nicht erkennen kann, ist damit eine gesteigerte IT-Bedrohungslage gegeben. Aufgrund dieser Bedrohungen besteht Bedarf an vermehrtem Schutz und Sicherheit.

Diese können aber nicht einfach per Download installiert werden, und für die Einführung von IT-Sicherheit kommt die Frage nach einem bewährtem, standardisiertem Verfahren auf, quasi einer »DIN für IT-Sicherheit«.

In wieweit dies machbar ist, beziehungsweise welche Aspekte betrachtet werden müssen und welche Methoden angewendet werden können um diese zu adressieren, zeigt dieser Text.

Begriffe

Bevor auf das Kernthema eingegangen wird sollen die relevanten Begriffe definiert und abgegrenzt werden. Wichtig ist dies, da manche der verwendeten Begriffe oft im alltäglichen Sprachgebrauch verwendet werden, ohne den klaren Fokus festzumachen.

Information als Wert

Bevor von »IT« – oder vollständig »Informationstechnologie« – und deren Sicherheit gesprochen wird, soll hier zuerst der dabei zentrale Begriff der »Information« und dessen Bedeutung für den vorliegenden Themenbereich erläutert werden.

Was sind Informationen? Wissen liegt in den Ausprägungen von deklarativem Wissen (Fakten) und prozeduralem Wissen (Abläufen, Prozessen) vor[2]. In Abgrenzung zu reinen, »ungerichteten« Daten und Fakten ist bei Informationen die Zielrichtung bzw. der Anwendungsbereich entscheidend – der Zweck des Einsatzes. Der Informationswissenschaftler Reiner Kuhle definierte Information als »Wissen in Aktion«[3].

Informationen existieren in verschiedenen Arten und Ausprägungen, und je nach Anwendung kommt ihnen ein bestimmter Wert und damit auch ein inhärenter Schutzbedarf zu.

Deklaratives Wissen ist oft in Fakten wie Bauplänen, Fertigungsverfahren oder chemischen Formeln gebunden, die nicht selten Geschäftsgeheimnisse darstellen.

Aber auch personenbezogene Daten wie Adressen oder Einkaufsgewohnheiten sind hier gemeint, ebenso wie weit sensiblere Daten, etwa zu Gehalt oder Gesundheit.

Finanzdaten können sowohl persönliche Daten sein, als auch im Unternehmensumfeld wichtige Angaben enthalten. Zahlungs- und Buchungsvorgänge erlauben Rückschluss auf Geschäftsvorgänge, Erwerb und Einsatz von Betriebsmitteln, und auf Geschäftspartner sowie dem allgemeinen finanzielle Zustand eines Unternehmens. Der Schutzbedarf aus unternehmerischer Sicht ist hier offensichtlich.

Aber auch interne Abläufe, Prozesse und

1 Hypponen (2012)

2 Bloom (1956)

3 Kuhlen (1995) S. 34

Verfahren stellen wertvolle Informationen dar. Diese können Produktions- und Fertigungsabläufe, Herstellung von Produkten, aber auch Aufbauorganisation und Nachrichtenwege umfassen. Welche Bedeutung diesen Informationen inne liegt zeigt das weltweite Patensystem, in dem genau diese Informationen geschützt werden sollen.

IT – Informationstechnologie

Von Informationen und Wissen in Prozessen zu deren Bearbeitung: »IT« – Informationstechnik – stellt heute die zentrale Technik zur maschinellen Verarbeitung von Informationen bereit.

Vorrangig geschieht dies unterstützend in Geschäftsprozessen aus denen Informationstechnologie heute nicht mehr wegzudenken ist. Zudem besteht in manchen Anwendungsgebieten, zum Beispiel der ganzen IT-Branche, die Informationstechnik selbst der zentraler Geschäftsinhalt, neben der Unterstützungsfunktion zur Prozessautomatisierung.

Offensichtlich umfasst »IT« Computer, Datenbanken und Speichersysteme sowie darauf basierende Software, Betriebssysteme und Anwendungen.

Zudem gelten heute Netzwerke zwischen Computersystemen als essenzieller Teil der IT, da Systeme nicht mehr isoliert betrieben werden, sondern der mit der Kommunikation einhergehende Austausch von Informationen wichtig ist. Der Paradigmenwechsel von der Elektronischen Datenverarbeitung (EDV) hin zur Informationstechnologie (IT) illustriert dies.

Bei der Betrachtung von IT sollte man aber weitere Komponenten nicht aussen vor lassen. Für moderne Rechenzentren, die die »Cloud« darstellen, sind Gebäude, die IT- und Kommunikationssysteme umfassen und schützen ebenso wichtig wie die Personen, die mit Informationen und Systemen als Anwender oder Administrator arbeiten. Selbstverständlich umfasst der Personenkreis wiederum auch das Management, das die Strategie von Unternehmen vorgibt, und damit letztendlich wieder, wie Informationen angewendet und genutzt werden.

Nicht vergessen werden sollte bei »IT« ausserdem auch klassische Speichermethoden auf Papier und sonstigen tragbaren Datenträgeren wie Disketten, CDROMs/DVSs und USB-Sticks. Deren Aufbewahrung und Entsorgung sollte ebenso mit der nötigen Sorgfalt begegnet werden wie das Sichern von Daten, um diese im Notfall wieder herstellen zu können.

Sicherheit

Dies bringt uns zum Thema »Sicherheit«. Der Wortursprung liegt im lateinischen und meint »sorglos« bzw. »ohne Sorgen«, und die Grenzen sind hier fließend: was heute noch als sicher angesehen wird wird morgen kritisch bewertet. In der Tat ist der Zustand der »Sicherheit« sehr relativ, und orientiert sich an existierenden bzw. als solches angesehenen Bedrohungen und letztendlich am damit akzeptiertem Risikoniveau. Dieses ändert sich mit der Zeit, und so ist »Sicherheit« als kontinuierlicher Prozess zu verstehen[1,2].

Wie sich die Bedrohungslage im einzelnen gestaltet und welches Risikoniveau als akzeptabel angesehen wird sollte ei-

1 Müller und Neidhöfer (2008) S. 60ff

2 Wikipedia (2012b)

gens mittels Risikoanalyse ermittelt und in einem eigenen Risikomanagement behandelt werden. Viele der Risiken und Bedrohungen im Unternehmen betreffen heute IT-Systeme, entsprechend sollten diese im Risikomanagement bedacht werden.

IT-Sicherheit

IT-Sicherheit meint die Sicherheit von IT-Komponenten. Gemäß Ulichs MTO-Konzept wirken aber neben der Technik auch Organisation und Menschen auf eine gemeinsam zu erfüllende Aufgabe wie etwa dem Schutz von Informationen vor Bedrohungen[1]. Entsprechend ist die Sicherheit von Informationen und sie verarbeitenden Komponenten weiter zu fassen als nur in »IT-Sicherheit«:

»IO-Sicherheit« betreffend die organisatorische Sicherheit von Informationen bzw. »IM-Sicherheit« für die menschlichen Aspekte sind als Begriffe heute nicht definiert, stellen aber genau die ergänzenden Aspekte für die Sicherheit von Informationen dar, die die IT-Sicherheit bildet. Letztendlich sind also zur Sicherung von Informationen - zur Gewährleistung von Informationssicherheit - alle drei Aspekte des MTO-Konzeptes anzuwenden. Abbildung 1 illustriert dies.

Begrifflich seien hier für die »IM-Sicherheit« die etablierteren Begriffe »Sensibilisierung für Informationssicherheit« bzw. »Security Awareness« genannt[2].

Als Abgrenzung zur IT-Sicherheit soll hier der Begriff »Informationssicherheit«

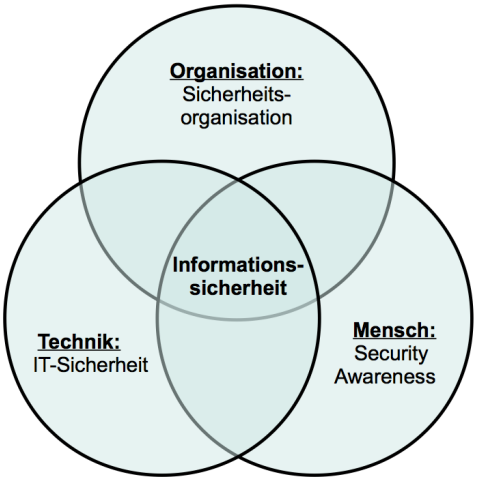

Abbildung 1: Aspekte der Informationssicherheit nach dem MTO-Konzept

genutzt werden, da dieser alle Aspekte der Sicherheit von Informationen umfasst. Da dies mehr als nur Technik ist, ist »Informationssicherheit« als Obermenge von »IT-Sicherheit« zu sehen.

DIN

Nach der Herleitung und Verzahnung des Begriffes »IT-Sicherheit« mit dem übergeordneten Begriff der Informationssicherheit hier abschliessend ein Wort zum im Titel benutzten Begriff »DIN«.

Dies steht für »Deutsches Institut für Normung«, ursprünglich für die hier relevante Diskussion »Normenausschuss der deutschen Industrie«, entsprechend findet sich auch oft die Abkürzung »Deutsche Industrie-Norm«. Hinsichtlich dieses Artikels ist dabei Folgendes im Fokus:

»Deutsch«: Im Alltagsgebrauch wird

1 Ulich (2005)

2 Mitnick (2002) S. 249ff

»DIN« auch als internationaler Qualitätsmaßstab vergleichbar zu »Made in Germany« verwendet. Dies ist wichtig, da der Standard (zumindest) von Unternehmen im deutschsprachigen Raum umzusetzen sein soll. Dies soll durch keine Sprachbarriere erschwert werden soll. Umgekehrt darf ein entsprechend formulierter Standard auch eine größere Verbreitung als nur die DACH-Region besitzen, solange die Akzeptanz und damit die Sicherstellung der Umsetzung davon nicht beeinträchtigt wird.

»Industrie«: Umgesetzt werden bzw. als Hilfe dienen sollte ein entsprechender Standard dem ursprünglichen Wortsinn der DIN nach der Industrie, also Unternehmen des produzierenden Gewerbes. Darüber hinaus umfasst dies ebenso auch weitere Wirtschaftszweige wie Dienstleister, Handel, Banken und Handwerk. Im Idealfall ist eine mögliche Norm für Informationssicherheit wiederum nicht auf einen Wirtschaftszweig beschränkt, sondern auch für den öffentlichen Bereich und nichtkommerzielle Einrichtungen wie Non-Government-Organizations einsetzbar.

»Norm« bezeichnet üblicherweise einen als Massstab dienenden, festgeschriebener Standard oder dokumentierte »Best Practice«, die ein bestimmtes Vorgehen beschreiben. Die Schriftform ist hier wichtig, da nur bei geschriebenen Regelungen sichergestellt werden kann, dass diese geschult, umgesetzt und letztendlich auch geprüft werden kann. Als Quelle dient üblicherweise ein wirtschaftsnaher Verband der sich auf die Etablierung und Einhaltung der Norm verständigt. Es sollen hier aber auch Gesetze nicht ausgeschlossen werden, da hier zwar die Quelle eine andere ist, der restliche Rahmen jedoch äquivalent ist.

Sich hier nur auf reine Normen des Deutschen Instituts für Normen zu beschränken wäre also zu kurz gegriffen, entsprechend weit gefasst ist der Fokus der im Folgenden betrachteten Normen und Gesetze.

Normen und Gesetze

Reglementierungen, die den Umgang mit Informationssicherheit adressieren, gibt es in Form diverser Normen und Gesetze. Auf der Suche nach *der* Norm für Informationssicherheit sollen diese als nächstes beleuchtet werden.

BSI IT-Grundschutz

Das Bundesministerium für Sicherheit in der Informationstechnik (BSI) bietet mit dem »IT-Grundschutz« eines der ältesten Vorgehensmodelle für den Bereich IT-Sicherheit an[1]. Die sehr umfangreiche Sammlung von Szenarien und Empfehlungen in den sogenannten »IT-Grundschutz-Katalogen« zeigt Gefährdungen auf und listet auch gleich umfangreiche Schutzmaßnahmen um diesen zu begegnen.

Kennzeichnend für den IT-Grundschutz des BSI ist, dass das Verfahren keine dedizierte Risikoanalyse als Grundlage verwendet. Stattdessen wird von einer »durchschnittlichen« Bedrohungslage ausgegangen, die die jeweiligen Umstände des Unternehmens nicht berücksichtigen. Zur Absicherung gegen diese durchschnittliche Bedrohungslage liefern die Grundschutz-Kataloge sehr umfangreiche Maßnahmen bezüglich Per-

1 Bundesministerium für Sicherheit in der Informationstechnik (2012)

sonal, Technik, Organisation und Infrastruktur.

Mangels Risikoanalyse ist nicht klar welche Werte vorrangig geschützt werden müssen, was in der Praxis dazu führt dass meist eine sehr lange Maßnahmenliste existiert, und der Standard des BSIs dadurch sehr umfangreich einzuführen ist[1].

IT-Grundschutz ist heute primär im öffentlichen Bereich zu finden. Internationale Unternehmen finden den IT-Grundschutz in einer englischen Übersetzung des auf Deutsche Massstäbe zugeschnittenen Standards, in Deutschland ist die Umsetzung im öffentlichen Dienst weit verbreitet. Eine Verpflichtung zur Umsetzung des IT-Grundschutzes gibt es per se nicht.

BDSG – Bundesdatenschutzgesetz

Anders sieht dies beim Bundesdatenschutzgesetzt (BDSG) aus. Als Gesetz in Deutschland geltend und aufgrund vieler fragwürdiger Vorfälle bei Gebrauch und Weitergabe von Daten und Informationen wird hier der Umgang mit personenbezogenen Daten adressiert.

Dies betrifft nach einer initialen Definition was unter personenbezogenen Daten zu verstehen ist deren Speicherung, Verarbeitung und Weitergabe, aber auch das Vorgehen zu Prüfung und Auditierung sowohl für öffentliche Stellen als auch nicht-öffentliche Unternehmen. Die Dokumentation erfolgt dabei praxisüblich in sogenannten "Verfahrensverzeichnissen", die die jeweiligen Umstände und Maßnahmen mehr (internes Verfahrensverzeichnis) oder weniger (öffentliches Verfahrensverzeichnis) detailliert aufzeigen.

Seit einer Revision des Gesetzes im Jahr 2003 werden im Anhang speziell anzuwendende technische und organisatorische Maßnahmen gelistet, die zu adressieren sind[2]. Diese umfassen neun Punkte. Diese sind der Zutritt zu Gebäuden und Systemen, Berechtigungen innerhalb von Anwendungen, den Schutz der Daten bei Weitergabe vor Zugriffen dritter, dass Eingabe, Verarbeitung und Löschung nachvollziehbar sind, den Schutz gegen Verlust und die Auflage dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden[3].

Bei Verarbeitung von Daten im Auftrag sind diese Maßnahmen auch von Seiten des Auftraggebers speziell vom Auftragnehmer einzufordern und ggf. durch Audits zu prüfen.

In der Praxis werden durch die oft allgemeinen Formulierung des BDSG Fragen aufgeworfen, jedoch nicht beantwortet. Diese zu erörtern und das BDSG in deren Sinne zu interpretieren ist Aufgabe der vom Gesetz in ihrer Funktion bestimmten Datenschutzbeauftragten, die für fast jedes Unternehmen zu bestimmen sind. Letztendlich wird im Gesetz auch das Verfahren bei Verstössen in den Bussgeldvorschriften geregelt.

International

Bisher wurden Normen bzw. Gesetze gelistet, die sehr stark auf Deutschland fokussiert sind. Aber auch in anderen Län-

1 Wikipedia (2012a)

2 Bundesministerium der Justiz (2009) Anhang zu Paragraph 9

3 Bundesministerium der Justiz (2009) Paragraph 11

dern bzw. international existieren heute bereits Vorgaben.

SOX – Sarbanes Oxley Act

Auch in den USA erlagen Unternehmen und deren Vorständen diversen Skandalen, unter anderem die Firma Enron im Rahmen des Börsencrashes um die Jahrtausendwende. Um dem in Zukunft besser begegnen zu können wurden durch den »Sarbanes Oxley Act« (kurz: SOX) 2002 ein Gesetz in den USA eingeführt, das die Berichterstattung von Unternehmen des Finanzsektors verbessern soll[1].

Da Unternehmen der hier relevanten Größenordnung meist auch international tätig sind hat SOX auch internationale Relevanz, zumindest bei der Pflege von Geschäftsbeziehungen mit den USA. Entsprechend existieren auch Verordnungen wie die der US-Wertpapier- und Börsenaufsichtsbehörde, die die Umsetzung des Gesetzes näher regeln[2].

Informationssicherheit ist hier nicht der primäre Fokus, es werden jedoch Anforderungen an die IT gegeben, um Themen wie Weitergabe und Speicherung von Daten sowie revisionssichere Protokollierung von Ereignissen sicherzustellen. Letztere sollen die nachträgliche Manipulation von Informationen verhindern.

Basel II / III – Bankenaufsicht

Ebenfalls aus dem Bankenumfeld stammten die Vorschriften des Basler Ausschuss für Bankenaufsicht, bekannt als Basel II[3] bzw. Basel III[4], die aufgrund von EU-Richtlinien für alle Banken und Finanzdienstleister vorgeschrieben sind.

Inhaltlich werden ähnlich wie beim Sarbanes-Oxley-Act primär finanzielle Abläufe geregelt, aber auch hier spielt die IT eine wichtige unterstützende Rolle. Hinzu kommt, dass mit Basel III Mindestanforderungen an ein Risikomanagement (MaRisk) definiert wurden[5], also zumindest Banken sich mit diesem Thema explizit auseinander setzen müssen.

PCI – Payment Card Industry

Im internationalen elektronischen Zahlungsverkehr sind heute Kreditkarten nicht mehr wegzudenken. Entsprechend hoch ist die Missbrauchsquote, und damit der Bedarf an Schutz. Die Payment Card Industry (PCI) hat dazu mehrere Standards definiert, die diesen bieten sollen.

Der »PCI Data Security Standard« (PCI-DSS) beschreibt den sicheren Ablauf des Zahlungsverkehrs, aber auch wie Missbrauch zu erkennen und zu behandeln ist. Da Kreditkarten oft in eigenen Terminals für die PIN-Eingabe verwendet werden und auch dort in der Vergangenheit viel Missbrauch betrieben wurde wird dies speziell im »PIN Transaction Security« (PCI PTS) Standard beschrieben. Neben der Bezahlung mit der physikalischen Karte ist elektronischen Geschäftsverkehr der Online-Zugriff mit Hilfe der Kartennummer üblich. Auch hier besteht ein breites Feld an möglichen

1 U.S. Government (2002)

2 SEC (2005)

3 Deloitte (2005)

4 Klauck und Stegmann (2012)

5 Ehrmann (2012)

Fehlern und Angriffsmöglichkeiten, dem der »Payment Application Data Security Standard« (PCI PA-DSS) begegnet.

Alle drei Standards sind auf die Sicherheit von Finanzdaten und die sie verarbeitende Systeme ausgelegt. Diese muss für den Erhalt der PCI-Zulassung auch regelmäßig durch Audits nachgewiesen werden.

HIPAA – U.S. Gesundheitswesen

Nicht nur im Bankenumfeld wird aufgrund von Misswirtschaft und unklarer Nachweislage der Ruf nach mehr Regulierung laut. Auch im Gesundheitswesen bestehen hier Begehrlichkeiten, und was in Deutschland mit dem Thema »Elektronische Gesundheitskarte« diskutiert wird, das ist in den USA bereits seit langem durch den »Health Insurance Portability and Accountability Act« (HIPAA, United States Congress 1996) von 1996 umgesetzt.

Das Gesetz behandelt zum einen die Übertragbarkeit von Krankenversicherungen bei Arbeitgeberwechsel als auch die Infrastruktur für eine elektronische Abrechnung aller Gesundheitsrelevanten Transaktionen. Ähnlich wie im Finanzbereich bestehen hier weitreichende Anforderungen an Unterstützung durch die IT, zudem kommen durch den erhöhten Schutzbedarf von Gesundheitsdaten weitere Anforderungen an die Sicherheit von Speicherung, Übertragung und Verarbeitung von Daten.

SAS70 & ISO 19011 – Auditierung

Nicht nur im Umfeld von Banken und staatlichen Einrichtungen wurde früh erkannt, dass Vorschriften gut sind, Kontrolle jedoch besser. Entsprechend ist Kontrolle auch heute ein elementares Managementinstrument, um die nachhaltige Umsetzung von Vorschriften sicherzustellen, und um Abweichungen zu erkennen und zu korrigieren.

Wie konkret bei der Vorbereitung, Durchführung und Nachverfolgung von Audits vorzugehen ist ist unter anderem im Statement on Auditing Standards Nr. 70 für Service Organisationen (SAS70, AICPA 1992) bzw. im Leitfaden zur Auditierung von Managementsystemen in der ISO Norm 19011[1] beschrieben. Obwohl hier kein direkter Bezug zu Informationssicherheit bzw. IT-Sicherheit besteht, sind diese Normen relevant für die Überprüfung, ob Vorschriften und Normen eingehalten werden, und wie dies bestimmt wird.

ITIL – IT Infrastructure Library

Die »IT Infrastructure Library« (ITIL, OGC 2012) bietet eine Sammlung (Library) von bewährten Standard-Vorgehen für IT-Dienstleistungen. Ausgehend von der Service-Politik werden »Best Practices« für Design, Umsetzung, Betrieb und Verbesserung vorgeschlagen.

Das Thema IT-Sicherheit ist nicht primär im Fokus, obwohl auch hier durch die Umsetzung z.B. von Asset Management, Configuration Management, Incident Management und eine solide Basis für ein aufbauendes Management von Informationssicherheit etabliert werden kann.

1 ISO/IEC (2011a)

COBIT – IT-Governance

Wo ITIL den Fokus auf IT-Dienste und deren Lebenszyklus hat gehen die »Control Objectives for Information and Related Technology« (COBIT, ISACA 2012) noch einen Schritt weiter und verstehen sich als Vorgaben für die IT-Governance, also die Steuerung der gesamten IT.

Als prozessorientierter Ansatz existieren Abbildungen auf diverse Standards wie ITIL für den Betrieb von IT-Diensten und ISO 27001 für das Management von Informationssicherheit (s.u.), aber auch weitere Regelungen wie Basel II/III und der Sarbanes Oxley Act können bei Bedarf integriert werden. Als solches versteht sich COBIT eher als Über-Standard für den Bereich IT-Governance, der auch die Informationssicherheit abdeckt. Rein für den hier angesprochenen Bereich ist COBIT jedoch viel zu weit gegriffen, um einen stabilen IT-Betrieb und eine optimale Unterstützung von Geschäftsprozessen durch Informationstechnik sicherzustellen verdient COBIT jedoch sehr wohl Beachtung.

ISO 2700x – Informationssicherheit

Mit der Umsetzung von COBIT ist auch der internationale Standard für das Management von Informationssicherheit ISO 27001[1] mit abgedeckt. Da COBIT aber wesentlich mehr als nur Informationssicherheit abdeckt ist gerade dieser Standard für die vorliegende Diskussion höchst relevant.

Historisch ging die Norm aus den British Standards BS 7799-1 und -2 hervor, wurde dann als ISO 17799 international anerkannt und 2007 in die Normen ISO 27001 und ISO 27002 aufgeteilt. Eine Übersetzung ins Deutsche und die Anerkennung als DIN Norm erfolgte 2008 als DIN ISO/IEC 27001, entsprechend liegt hier eine DIN vor die auch international gültig ist. Neben 27001 und 27002 existiert eine Reihe weiterer Normen die Details regeln, eine Übersicht ist in der frei zum Download erhältlichen ISO 27000 enthalten.

Aufgrund ihrer Bedeutung für den Bereich der Informationssicherheit soll diese Normenreihe im Folgenden näher betrachtet werden.

Vorstellung der Norm

Zentraler Bestandteil der Normenreihe ist die Norm 27001, es gibt jedoch eine Reihe angegliederter Normen von 27000 an aufwärts. Die Norm 27001 beschreibt ein sogenanntes »Informationssicherheits-Managementsystem« (ISMS). Wer mit Qualitätsmanagement nach ISO 9001 vertraut ist wird sich hier rasch zurecht finden: Es wird nicht nur beschrieben wie man »sicher« wird, sondern wie man diesen Zustand auch erhält bzw. verbessert.

Generell folgt das Aufsetzen und der Betrieb des ISMS nach dem Deming-Zyklus, der sich in die vier in Abbildung 2 gezeigten Teile Plan, Do, Check und Act gliedert[2].

Plan: Erster Schritt der Planung ist, den Gültigkeitsbereich (»Scope«) hinsichtlich der betrachteten Unternehmensteile, Abteilungen und Standorte festzulegen. Hier muss keine Breite von 100% über

1 ISO/IEC (2005)

2 Deming (2000)

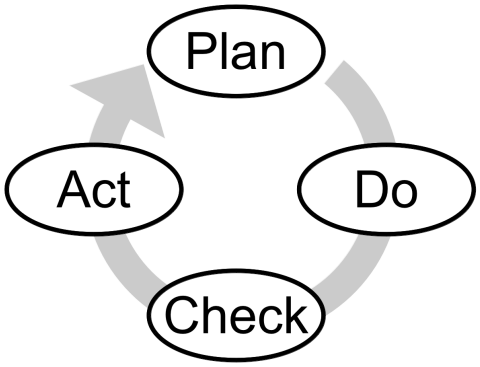

Abbildung 2: Das Managementsystem für Informationssicherheit entspricht dem Deming-Zyklus

alle Bereiche im ersten Schritt angestrebt werden, eine vollständige Abdeckung eines kleinen Teilbereichs wie Rechenzentrumsbetrieb oder die Entwicklungsabteilung ist durchaus normgerecht. Beeinflusst wird diese Auswahl zwischen dem Wunsch, möglichst alle Bereiche vollständig abzudecken und dem damit verbundenen Aufwand. Diese Möglichkeit, den Scope selbst zu wählen ist ein wichtiger Aspekt der ISO 27001.

Hat man sich auf den zu sichernden Bereich des Unternehmens geeinigt, so ist als nächstes die angestrebte Tiefe festzulegen. Idealerweise bei 100% liegend bietet die Norm auch hier Bereitschaft zur Diskussion - wer z.B. keine eigene Softwareentwicklung betreibt wird die entsprechenden Teile (»Controls«) kaum erfüllen können. An dieser Stelle sollte mit Vorsicht agiert werden, da hier zwar Aufwand bei der Umsetzung vermindert werden kann, eine unverhältnismässige Einschränkung jedoch Auswirkungen auf das Sicherheitsniveau hat, was nicht nur bei Audits negative Ergebnisse nach sich ziehen, sondern auch das ganze Bestreben in Frage stellen kann.

Nachdem der Gültigkeitsbereich festgelegt wurde ist dieser einer Risikoanalyse zu unterziehen. Im ISO 27001 Standard wird dazu kein bestimmtes Vorgehen gefordert. Als Orientierungshilfe kann die Norm ISO 27005 herangezogen werden, es existieren jedoch Alternativen, wie weiter unten aufgezeigt. Basierend auf der Risikoanalyse ist bekannt, welche Werte am meisten bedroht sind, und in welcher Reihenfolge Gegenmaßnahmen umgesetzt werden müssen, um ein akzeptiertes Risikoniveau zu erhalten.

Do: Um »sicher« zu sein genügt es nicht, nur die in der Risikoanalyse identifizierten Bedrohungen abzustellen. Informationssicherheit hat viele technische und organisatorische Aspekte, die zwingend erfüllt sein müssen. Zu finden sind die 133 Controls im Anhang A der Norm ISO 27001. Dieser normative Anhang ist zwingend umzusetzen (soweit nicht ausgenommen, wie oben beschrieben). Wer die Beschreibungen im Anhang A zu knapp findet und mehr Erklärungen benötigt findet diese in der ISO 27002 beschrieben. Mehr zu den 133 Controls im Anhang A später.

Neben der Umsetzung der Maßnahmen aus der Risikoanalyse und der vorgeschriebenen Controls ist auch periodisch der Status des ISMS zu erfassen, und basierend auf diesem die nächsten Schritte einzuleiten, was dann wiederum zu neuen Planungen führt.

Zentraler Bestandteil des ISMS ist, dass Regelungen für das Unternehmen getroffen werden, und diese auch schriftlich festgehalten werden. Darüber hinaus sind auch Aufzeichnungen über

die Durchführung einzelner Aktionen zu machen, um nachweisen zu können dass diese wirklich umgesetzt wurden.

Die Norm fordert hier entsprechenden Umgang mit bzw. die

Lenkung von Dokumenten und Aufzeichnungen. Bei der Umsetzung droht hier die Gefahr, dass man in Dokumenten und Formularen ertrinkt - Erfahrung mit den unternehmenseigenen Prozessen, wo diese protokolliert werden und wie entsprechende Reports erzeugt werden können helfen hier, den Aufwand überschaubar zu halten.

Was die Umsetzung des ISMS betrifft schreibt die Norm auch vor, dass dieses vom Management beauftragt werden muss: Ein Beschluß des IT-Leiters, seinen Bereich »sicher« zu machen wird wenig bringen, wenn der Rest des Unternehmens nicht am selben Strang zieht, oder die Unternehmensleitung nicht die entsprechenden Ressourcen bereit stellt. Das vom Standard geforderte »Management Commitment« stellt sicher, dass hier alle Abteilungen einbezogen werden.[1]

Nach der Beauftragung wird das Management weiter regelmässig eingebunden: Es sind periodische ISMS-Reports mit vorgegebenen Inhalten über den Stand der Informationssicherheit zu erstellen, und es wird gefordert dass sich das Management auch mit diesen auseinandersetzt und entsprechende Maßnahmen zur Umsetzung beschliesst. Auch wenn Empfehlungen der Informationssicherheit nicht zur Umsetzung beschlossen werden – etwa weil der Status Quo als ausreichend oder die Umsetzung als zu kostspielig erachtet wird – so wird dieser Beschluss dennoch in der Managementbewertung – der Bewertung der Informationssicherheit durch das Management – festgehalten. Sollten später Fragen aufkommen, können die so dokumentierten Entscheidungen nachvollzogen werden.

Check: Die Managementbewertungen stellen sicher, dass das Management über den Stand des ISMS unterrichtet ist. Aber entspricht das ISMS damit auch der Norm? Dies zu prüfen ist eine getrennte Aufgabe, die regelmässig - üblicherweise jährlich - durch sogenannte interne Audits festgestellt werden. Intern, weil ein Mitarbeiter des Unternehmens sie durchführen kann. Voraussetzung ist, dass er über das nötige fachliche (IT) und organisatorische (ISMS) Wissen verfügt, und dass nicht der eigene Tätigkeitsbereich auditiert wird. Ein IT-Leiter der gleichzeitig ISMS-Beauftragter ist, tut gut daran, einen Mitarbeiter von außerhalb der IT zu bitten, diese zu auditieren. Unterstützen können hier interne Stellen wie Revision, Datenschutzbeauftragter oder auch externe Berater.

Act: Das Ergebnis des Audits ist die Feststellung, welche Normforderungen erfüllt sind und welche noch Verbesserungspotential aufweisen. Diese transparent zu machen und strukturiert abzuarbeiten führt zu einer kontinuierlichen Verbesserung des Systems. Da die Verbesserungen wieder neue Planungen erfordern beginnt damit der Kreislauf des Systems von vorne.

Risikomanagement ist obligatorisch

Aufbau und Einführung eines Risikomanagements sind zur Umsetzung der ISO 27001 Norm vorgeschrieben. Wie ein-

1 Man beachte, dass beim Thema Sensibilisierung auch das Management einzubeziehen ist. Die ISO 27001 fordert dies explizit.

gangs erwähnt ist das Verfahren nicht näher spezifiziert, hier hat man freie Hand solange das Vorgehen angemessen ist.

Das in der ISO Norm 27005 beschrieben Verfahren bietet sich im Kontext der ISO 27001 an[1], es existieren jedoch eine Reihe weiterer Vorgehensmodelle die alternativ eingesetzt werden können. Zu nennen sind hier OCTAVE des US-CERT[2] und die Special Publication 800-30 des US-National Institute of Standards and Technology (NIST)[3]. Die beiden Normen unterscheiden sich primär bei der Ermittlung der bedrohten Werte. Wenn statt nationaler Vorgehen internationale Standards bevorzugt werden bietet sich die ISO 31000 für ein allgemeines Risikomanagement ohne Fokus auf IT-Sicherheit an[4]. Für spezielle Anwendungsgebiete wie den Finanzsektor existieren – wie eingangs für den Bereich der Standards illustriert – auch eigene Vorschriften für die Durchführung des Risikomanagements. Als Beispiel sind hier die Mindestanforderungen an das Risikomanagement (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht zu nennen, die wiederum auf Basel II zurückgehen.

Grundlage jeder Risikoanalyse ist, dass Bedrohungen erkannt werden, die die Werte des Unternehmens beeinträchtigen könnten. Werte ergeben sich dabei aus dem in der Planungsphase festgelegten Gültigkeitsbereich und den damit verbunden Geschäftsprozessen. Sie umfassen neben den offensichtlichen Werten der Betriebsmittel wie Rechnern auch unentbehrliche Personen, Gebäude, Geistiges Eigentum wie Quellcode und Patente, Kommunikationsverbindungen und nicht zuletzt die Finanzen des Unternehmens.

Für jeden dieser Werte wird ermittelt wie wichtig er im Verhältnis für das Unternehmen ist und welche unterschiedlichen Bedrohungen auf ihn mit welcher Eintrittswahrscheinlichkeit einwirken können. Entsprechend werden mögliche Maßnahmen zur Verminderung des Risikos, zur Versicherung gegen Bedrohungen oder zu deren Akzeptanz festgelegt. Maßnahmen, die Bedrohungen vermindern, werden für die Umsetzung des ISMS notiert und dort strukturiert abgearbeitet.

Risikoanalyse, Risikobehandlung und die Maßnahmenverfolgung sind Bestandteil des Risikomanagements, das wahlweise nur für den Bereich IT bzw. IT Security gemacht werden kann, alternativ aber auch an ein bestehendes Kontrollsystem abgeschlossen werden kann, das weitere Teile des Unternehmens abdeckt.

Maßnahmen der ISO 27001

Neben den in der Risikoanalyse identifizierten Themen schreibt die Norm eine Reihe von Maßnahmen vor, die zwingend umzusetzen sind. Diese 133 Kontrollpunkte sind in Anhang A der Norm gelistet, der etwas ungewöhnlichen Nummerierung folgend in den Kapitel A.5 bis A.15, die Kapitel A.1 bis A.4 existieren nicht.

Den Inhalt hier vollständig wiederzugeben würde den Rahmen sprengen, deshalb hier nur eine Zusammenfassung mit ausgewählten Beispielen, um einen Eindruck des geforderten Sicherheitsnive-

1 ISO/IEC (2011b)

2 Alberts und Dorofee (2002)

3 NIST (2002)

4 ISO/IEC (2009)

aus zu vermitteln.

Festlegung der Sicherheitsleitlinie (A.5)

Die Sicherheitsleitlinie beschreibt in sehr allgemeinen Worten und in relativ kurzer Form den Stellenwert der Sicherheit für das Unternehmen, auf welcher Basis diese umgesetzt und kontrolliert wird und auch wie Verstösse geahndet werden. Sie muss schriftlich festgelegt werden, was auch die Kommunikation mit Mitarbeiter, Kunden und Geschäftspartner erleichtert.

Die entsprechende Verankerung in der Unternehmenspolitik stellt auch sicher, dass das Unterfangen vom Management getragen wird.

Organisation der Informationssicherheit (A.6)

Die Verantwortlichkeiten für den Betrieb des ISMS müssen festgelegt werden. Zudem ist auch darzulegen, mit welchen externen Gruppen und Behörden zusammengearbeitet wird.

Weiterhin ist zu bedenken, wie der Umgang mit Kunden am Unternehmensgelände geregelt wird, etwa ob eine Besucherliste geführt wird, ob sich Besucher frei bewegen dürfen, ob Besucherausweise ausgestellt werden und wie mit Besuchern verfahren wird die sich nicht ausweisen können oder die in nicht für sie freigegebenen Bereichen angetroffen werden.

Management der organisationseigenen Werte (A.7)

Beispiele umfassen hier die Inventarisierung aller Werte wie etwa bei Asset und Configuration Management in ITIL, die Dokumentation der Zuständigkeiten für die Werte wie IT-Systeme inklusive Festlegung wer für den Rest wie Gebäude und Personal verantwortlich ist.

Informationen sind entsprechend ihrer Vertraulichkeitstufe z.B. nach öffentlich, intern oder vertraulich bzw. geheim zu klassifizieren, und Handlungsanweisungen für Speicherung, Druck, Übertragung per Post und E-Mail, Kennzeichnung und Entsorgung (Papier!) sind festzulegen und wie alle Regelungen allen Mitarbeitern kenntlich zu machen.

Personelle Sicherheit (A.8)

Sicherheit lebt nicht von Vorschriften, sondern wird durch alle Mitarbeiter umgesetzt. Um hier vorzubeugen sind Regelungen für die Personalabteilung zu prüfen. Dazu ist gegebenenfalls eine Sicherheitsüberprüfung für Mitarbeiter in sensiblen Positionen vorzuschreiben, sicherzustellen dass alle neuen Mitarbeiter über die Sicherheitsrichtlinien unterrichtet werden und eine Verschwiegenheitserklärung unterschreiben, und dass Verstösse geahndet werden.

Bei internem Arbeitsplatwechsel muss darauf geachtet werden dass Benutzerrechte entzogen werden und Arbeitsmittel zurückgegeben werden, ebenso wenn Mitarbeiter das Unternehmen verlassen.

Physische und umgebungsbezogene Sicherheit (A.9)

Der Zutritt zu Gebäuden und Rechnerräumen muss geregelt werden, ebenso die Sicherheitszonen, Schließanlagen und Prüflisten für Schlüsselvergaben. Besondere Bereiche wie öffentliche Zugänge und Lieferzonen müssen speziell betrachtet und reguliert werden um möglichen Eindringlingen zu begegnen. Diese Forderung entspricht der Zutrittskontrolle des Bundesdatenschutzgesetzes.

Auch die Lagerung von Betriebsmitteln muss bedacht werden (Diebstahl, Sabotage), ebenso wie die Trassenführung von Versorgungsleitungen und Wartungspläne für Infrastruktur wie etwa Strom, Wasser, Klima und Notstrom.

Betriebs- und Kommunikationsmanagement (A.10)

»Dokumentierte Betriebsprozesse« sind leider auch im Jahr 2012 mancherorts immer noch ein Fremdwort für die IT. Hier kann ITIL helfen, auch was die Koordination von Änderungen und deren Dokumentation und Nachvollziehbarkeit betrifft. Dies betrifft sowohl die eigenen Mitarbeiter als auch die von Dienstleistern – nur weil eine Aufgabe an Dritte vergeben wird entfällt nicht die eigene Kontrollpflicht! Entsprechend sind die Anforderungen bezüglich Informationssicherheit an Dienstleister in Verträge aufzunehmen und im Rahmen von Audits regelmässig – mindestens jährlich – zu prüfen. Die Kapazitäten von Systemen sollten überwacht und regelmässig kontrolliert werden, um Engpässe frühzeitig zu erkennen. Schutz gegen Viren und sonstigen Schadcode ist zu installieren – auch Systeme hinter Firewalls können von innen befallen werden.

Daten sind regelmässig zu sichern, die erfolgreiche Sicherung ist zu prüfen und regelmässige Restore-Tests sind durchzuführen.

Die Sicherheit von Netzdiensten ist durch Firewalls bzw. Deaktivierung sicherzustellen, Speichermedien aller Art sollten bedacht verwendet und bei Bedarf fachgerecht entsorgt werden. Dies betrifft explizit die Entsorgung von Papier sowie alten Festplatten.

Werden Informationen via physikalischem Datenträger oder via Netzwerk übertragen, so sind entsprechende Vorschriften zu treffen, die die Vertraulichkeit der Informationen berücksichtigt. Zum Beispiel sollte festgelegt werden ob geheime Daten beim Versand per E-Mail verschlüsselt werden müssen und wenn ja wie. Und ob mögliche Dienstleister diese Anforderungen nachkommen können. Webserver und sonstige öffentliche Dienste und Informationen sind adäquat gegen Missbrauch, Abfluss und Manipulation zu schützen, bei Anwendung elektronischer Transaktionen wie Bestell- und Bezahlvorgängen ist besonders auf Maßnahmen gegen Missbrauch zu achten.

Es ist festzulegen welche Aktionen wie zu protokollieren sind, und wie sichergestellt wird dass diese nachträglich nicht manipuliert werden können – siehe SOX und Basel II/III.

Zugangskontrolle (A.11)

Die relativ lapidare Normforderung ist hier, dass unberechtigte Zugriffe verhindert werden müssen. Erreicht wird dies, in dem berechtigte Zugriffe do-

kumentiert werden, und regelmässig ein Soll/Ist-Abgleich zwischen Systemen und Dokumentation erfolgt. Bei Vergabe von Rechten muss entsprechend die Dokumentation aktualisiert werden.

In der Praxis betrifft dieses Thema alle eingesetzten Systeme und alle Benutzer was sehr schnell ausufern kann. Für eine effiziente Umsetzung ist der Stand der Systeme automatisiert in einer Darstellung zu extrahieren, die der Dokumentation entspricht. Diese Forderungen entsprechen der Zugriffskontrolle des Bundesdatenschutzgesetzes.

Darüber hinaus sind eindeutige Benutzeraccounts zu verwenden, und Regelungen zur Geheimhaltung von Passworten zu treffen. Herausforderungen bestehen hier, wenn Systeme keine getrennten Benutzerkennungen erlauben, wie etwa der administrative Benutzer `root` unter Unix. Hier kann der Zugriff über ein entsprechendes Tool zur Passwortverwaltung geregelt werden, das dann die Zugriffsrechte abbildet.

Zudem sollten auch Policies betrachtet werden, die Benutzer anhalten, Informationen und Dokumente nicht unbeaufsichtigt auf dem Schreibtisch liegen zu lassen, und den Bildschirm bei Verlassen des Arbeitsplatzes zu sperren. Letzteres kann technische dadurch unterstützt werden, indem entsprechende Defaults für den Screensaver hinterlegt werden.

Neben der Identifikation von Benutzern ist auch der Zugang zum Netzwerk zu kontrollieren, unberechtigte Zugriffe per Firewall zu behandeln und zu protokollieren. Unberechtigte Benutzeranmeldungen am Betriebssystem sind zu erkennen und ebenfalls zu protokollieren.

Die Auswertung der Protokolle kann dann z. B. im Rahmen der ISMS-Managementreports geschehen.

Beschaffung, Entwicklung und Wartung von Informationssystemen (A.12)

Wenn Fachanwendungen extern beauftragt oder intern entwickelt werden, dann sollte das Thema Sicherheit bereits in der Konzeption berücksichtigt werden. Dazu gehört, dass eingegebene Daten geprüft werden (SQL Injections, Buffer Overflows, etc.) und auch die Ausgabe auf Plausibilität geprüft wird.

Werden Nachrichten zwischen Systemen ausgetauscht sind diese zu sichern, die entsprechenden kryptographischen Methoden und das Vorgehen zur Behandlung von Schlüsseln ist festzulegen.

Die Sicherheit von Systemdateien wie dem Betriebssystem, Testdaten und dem Quellcode ist sicherzustellen, vor allem wenn mit externen Dienstleistern gearbeitet wird. Wer würde schon den Live-Abzug aller Kundendaten als Testdaten an einen Dienstleister geben?

Änderungen an Systemen und Programmen sind nachvollziehbar zu dokumentieren, und Herstellerinformationen zu Schwachstellen verwendeter Programme, Systeme und Komponenten sollten regelmässig betrachtet werden.

Umgang mit Informationssicherheitsvorfällen (A.13)

So wie die Feuerwehr einen grossen Teil ihrer Zeit mit Vorbeugung gegen Brände verbringt wird auch beim ISMS viel Augenmerk auf die Vermeidung von sicherheitsrelevanten Vorfällen gelegt. Lei-

der ist dies nie 100% perfekt, und genau dann macht sich ein effizientes Training zum Umgang mit Sicherheitsvorfällen bezahlt.

Meldeketten und Verantwortlichkeiten müssen definiert sein, inklusive Alternativen wenn die primären Wege (Mail-Server ist down?!) oder Personen (IT-Leiter ist im Urlaub) betroffen sind.

Die Vorgehen für Standardprobleme sind vorab zu dokumentieren und zu üben, im Ernstfall sollten Beweise für mögliche strafrechtliche Verfolgungen gesammelt werden.

Sicherstellung des Geschäftsbetriebs (A.14)

Dem Stellenwert von Informationen gemäß muss der Ausfall von IT-Systemen in einer eigenen Notfallplanung dokumentiert, regelmässig geübt und laufend verbessert werden.

Der Ausfall der Systeme kann dabei verschiedenste Gründe haben, etwa Hardware-Ausfall, Naturkatastrophen oder Sabotage. Prozeduren für den Befall mit Viren sollten etabliert sein, ebenso wie mit dem Verdacht auf Manipulation durch Mitbewerber umgegangen wird. Die Szenarien gehen aus der Risikoanalyse hervor, sich passend abzusichern und für den Ernstfall gewappnet zu sein ist keine kleine Aufgabe.

Dieses Thema entspricht dem IT Service Continuity Management von ITIL bzw. der Verfügbarkeitskontrolle des BDSG.

Einhaltung von Vorgaben (Compliance) (A.15)

Verstöße gegen Gesetze, Patente und vertragliche Auflagen können weitreichende Folgen haben. Angefangen von Bußgeldern über Haftstrafen für die haftenden Mitglieder des Vorstandes bis hin zum Reputationsverlust besteht hier eine breite Palette an Bedrohungen. Der Bezug zur IT- bzw. Informationssicherheit ist hier oft nicht direkt ersichtlich, jedoch inhärent gegeben wenn zum Beispiel Auflagen des BDSG nicht eingehalten werden, eigene Produkte gegen bestehende Patente Dritter verstossen oder man sich das Lastenheft des Auftraggebers bei einem Softwareentwicklungsprojekt nicht bis ins letzte Detail durchgelesen hat und auf Regresszahlungen verklagt wird. Je nach Geschäftsumfeld sind die Auflagen hier sehr unterschiedlich, weshalb auch die Identifikation der anwendbaren Gesetze und Regelungen hier zentral ist.

Hierzu gehört selbstverständlich auch das Urheberrecht, gegen das Mitarbeiter nicht verstossen sollten - die Duldung durch den Arbeitgeber bringt diesen in Bedrängnis!

Faktor Mensch

Wie bereits beschrieben ist zur Einführung eines ISMS im Unternehmen nicht nur eine lange Reihe von technischen und organisatorischen Schritten nötig. Vor allem die Mitarbeiter, die dieses dann leben sollen sind der entscheidende Faktor für den Erfolg. Um diesen nicht dem Zufall zu überlassen adressiert die ISO 27001 auch die Sensibilisierung für Informationssicherheit in diversen Berei-

chen.

Als Hauptverantwortlich für die Informationssicherheit wird das Management festgelegt. Dieses bestimmt die Sicherheitspolitik des Unternehmens. Die operative Umsetzung darf zwar deligiert werden, aber spätestens bei der Managementbeurteilung ist die Geschäftsführung wieder eingebunden. Die organisatorischen und technischen Regelungen, die die Informationssicherheit gewährleisten, werden allen Mitarbeitern kommuniziert. Zusätzlich erfolgt gemäß Norm eine eigene Sensibilisierung für alle Mitarbeiter, damit sich diese den aktuellen Gefahren bewusst sind. Je nach Anzahl und Tätigkeitsfeld der Mitarbeiter ist die Sicherstellung von Security Awareness eine anspruchsvolle Aufgabe, die Umsetzung entsprechender Kampagnen wird mittlerweile von einer Reihe von Dienstleistern angeboten.

Als Unternehmen hat man vielerlei Geschäftskontakte, sowohl zu Kunden als auch zu Dienstleistern und sonstigen Geschäftspartnern. Diese sollten in das Managementsystem eingebunden sein - Kunden sollten wissen wem und wie sie Sicherheitsvorfälle melden, Geschäftspartner und Dienstleister sollten vertraglich zur Einhaltung der Sicherheitsvorgaben angehalten und laut Norm regelmässig überprüft werden.

Zertifizierung

Ein ISMS aus eigenen Antrieben zu betreiben ist gut, oft will dies aber auch nach außen dargestellt werden, und die Frage nach einer Zertifizierung kommt auf.

Um den Status Quo des ISMS periodisch festzuhalten schreibt der Standard Audits vor. Diese oben bereits beschriebenen internen Audits dienen zur Verbesserung des Systems, die Erkenntnisse gehen in die Verbesserung des Systems ein.

Spätestens wenn man eine Zertifizierung anstrebt ist dies extern zu beantragen, die entsprechenden Zertifizierungsaudits werden von diversen Unternehmen angeboten, TÜV, DQS und das BSI sind hier nur einige prominente Beispiele. Eine offizielle Akkreditierung der Zertifizierungsunternehmen ist zwar nicht zwingend notwendig, aber sehr sinnvoll um ein aussagekräftiges Zertifikat zu erhalten, das besagt dass die gängigen Standards sowohl hinsichtlich der Inhalte des auditierten Standards sowie auch des Vorgehens bei der Auditierung selbst eingehalten werden.

Software-Werkzeuge

Als letztes ein Wort zu Werkzeugen: hier hat der ISMS-Beauftragte die freie Wahl, die Normforderungen »per Hand« auf Papier oder in Textverarbeitung und Tabellenkalkulation zu dokumentieren, oder ein Werkzeug zu benutzen. Beides hat seine Vor- und Nachteile.

Vorgefertigte Werkzeuge folgen einer bestimmten Denkschiene, die erst verstanden und umgesetzt werden muss, bevor der Mehrwert zutage tritt. Dies ist insofern nicht-trivial, da oft schon die Umsetzung der vielen Normforderungen jeweils eine eigene Herausforderung ist, die die eigentliche Aufgabe nicht einfacher machen. Bei umfangreicheren Managemtsystemen mit vielen Standorten und Mitarbeitern ist ein toolgestützter Ansatz jedoch von Vorteil wenn sichergestellt werden kann, dass alle Bereiche

abgedeckt sind.

Die Frage »Tool oder nicht« kann nicht pauschal beantwortet werden sondern sollte durch Betrachtung von Scope, Auflagen zur Nachweispflicht und nicht zuletzt auch dem Preis potentieller Tools beantwortet werden. Letzterer variiert sehr: Mit Verinice ist eine etablierte Open Source Lösung kostenlos verfügbar, die viele Belange abdeckt. Kommerzielle Werkzeuge für den Bereich Governance, Risk & Compliance (GRC) gehen jedoch eher mit Kosten im vier- bis fünfstelligen Bereich zuzüglich Beratungskosten einher, da sich die Vorgehensmodelle eben nicht immer offensichtlich erschließen.

Als Inspiration für mögliche Werkzeuge sei hier auf entsprechende Listen im Internet[1] sowie die Bewertungen von Forrester[2] und Gartner[3] verwiesen.

Fazit

Wo ist sie nun, die DIN für IT-Sicherheit?

Ein zeit- und ordnungsgemäßer IT-Betrieb sollte die Anforderungen von Datenschutz (BDSG) und der IT Infrastructure Library (ITIL) als Grundlagen umsetzen, ein dediziertes Informationssicherheitsmanagement kann dann relativ einfach in der Praxis umgesetzt werden.

Als Einstieg bietet das BDSG eine erste Richtschnur, die die Grundabsicherung von Systemen und Informationen sicherstellt. Obwohl an manchen Stellen sehr allgemein formuliert und damit Raum für Interpretation erlaubend, bietet das BDSG doch mit Verfahrensverzeichnissen, der Behandlung der Auftragsdatenverarbeitung und einer überschaubaren Liste an technischen und organisatorischen Maßnahmen.

Es ist zu erwarten dass dieses Gesetz in den kommenden Jahren um Kontrollmechanismen erweitert wird, die kontinuierlich den Status des Datenschutzes erfasst und diesen verbessert. Ob damit der Übergang zu einem »Bundesinformationschutzgesetz« einher geht darf mit Spannung erwartet werden. Äusserungen des Bundesinnenministers Hans-Peter Friedrichs, dass zukünftig IT-Angriffe zu melden seien, bestätigen diese Bewegung[4].

Speziell für den Bereich IT-Sicherheit bzw. Informationssicherheit kommen damit zwei »Normen« in Frage: der IT-Grundschutz des BSI, und die internationale Norm ISO 27001.

IT-Grundschutz ist als rein deutsche Empfehlung des BSI zu verstehen, jedoch auch hier mit Abstrichen: Zum einen wird keine strukturierte Risikoanalyse durchgeführt, und so möglicherweise zentrale Sicherheitsaspekte nicht betrachtet. Zum anderen ist der Standard im Ursprung primär auf die öffentliche Verwaltung zugeschnitten - die Umsetzung aller Vorgaben erscheint (mangels Risikoanalyse) als erstrebenswert, ist dadurch jedoch auch extrem umfangreich und trotzdem nicht notwendigerweise vollständig. IT-Grundschutz kann als historisch relevant betrachtet werden, was auch durch die Entwicklung unterstrichen wird, dass sich das BSI aktuell zur Zertifizierung von »ISO 27001 auf Basis von IT-Grundschutz« hin be-

1 Mosaic Security Research (2012)

2 Forrester (2011)

3 Roe (2011)

4 Welt Online (2012)

wegt. Losgelöst vom Verfahren des IT-Grundschutzes behalten die dazugehörigen Grundschutz-Kataloge ihre Bedeutung als wichtige Quelle für Bedrohungen, Gefährdungen und Maßnahmen.

Für die Feststellung und die Verbesserung der Informationssicherheit ist die ISO Norm 27001 (und verwandte) bereits heute als internationaler Standard etabliert. Verbunden damit ist auch ein Management-System, um den Status-Quo zu messen, halten und zu verbessern. Die ISO 27001 deckt die Bereiche, in denen der IT-Grundschutz des BSI Schwächen hat, vollständig ab, und stellt umgekehrt sicher, dass alle Gesetzlichen Anforderungen erfüllt werden - u.a. die des BDSG.

Im direkten Vergleich bietet die ISO 27001 also mehr als IT-Sicherheit, nämlich Informationssicherheit mit allen relevanten Aspekten, und mehr als »nur« eine DIN, nämlich einen internationalen Standard, und klare Aussagen zur Umsetzung und Anwendung.

Daher wir hier die DIN ISO/IEC 27001 als »DIN für IT-Sicherheit« zur Umsetzung empfohlen.

Über den Autor

Dr. Hubert Feyrer hat an der Hochschule Regensburg technische Informatik studiert und an der Universität Regensburg im Fach Informationswissenschaft promoviert. Parallel war er anfangs als System- und Netzwerkadministrator sowie später als Dozent an der Hochschule Regensburg, der Uni Regensburg und am Stevens Institut Technology in Hoboken, New Jersey, USA, tätig. Nach seiner Promotion arbeitete er in der freien Wirtschaft, zuletzt als technischer Leiter bei einem Hersteller von Sicherheitslösungen mit Sitz in München, wo er als technischer Leiter Teams in den Bereichen IT-Security und Datacenters leitete, Entwicklungen in den Bereichen Hard- und Software vorantrieb und die Bereiche IT-Compliance und ISMS/ISO 27001 aufbaute und betreute. Aktuell ist Dr. Feyrer als Chief Information Security Officer (CISO) und Risikomanager bei einem international agierenden Personaldienstleister der Automobilbranche tätig.

Literaturverzeichnis

AICPA. (1992). Statement on Auditing Standards No. 70: Service Organizations. Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). Zugriff am 19. August 2012, unter `http://umiss.lib.olemiss.edu:82/record=b1038093`

Alberts, C. & Dorofee, A. (2002). *Managing Information Security Risks: The Octave Approach*. Addison Wesley Longman, Amsterdam.

Bloom, B. S. (Herausgeber). (1956). *Taxonomy of educational objectives—Handbook 1: Cognitive domain*. McKay, New York, USA.

Bundesministerium der Justiz. (2009). Bundesdatenschutzgesetzt (BDSG). Zugriff am 19. August 2012, unter `http://www.gesetze-im-internet.de/bdsg_1990/`

Bundesministerium für Sicherheit in der Informationstechnik. (2012). IT-Grundschutz. Zugriff am 19. August 2012, unter `https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html`

Deloitte (Herausgeber). (2005). *Basel II: Handbuch zur praktischen Umsetzung des neuen Bankenaufsichtsrechts*. Schmidt Verlag, Berlin.

Deming, W. E. (2000). *Out of the Crisis*. MIT Press.

Ehrmann, H. (2012). *Risikomanagement in Unternehmen: Mit Basel III*. Kiehl, Herne.

Forrester. (2011). The Forrester Wave: Enterprise Governance, Risk, And Compliance Platforms, Q4 2011. Zugriff am unter http://www.forrester.com/rb/go?docid=57692&oid=1-JTWY7G&action=5

Hypponen, M. (2012). F-Secure, Helsinki, Finland. Zugriff am 19. August 2012, unter http://www.f-secure.com/weblog/archives/00002376.html

ISACA. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA. Zugriff am 19. August 2012, unter http://www.isaca.org/COBIT/Pages/default.aspx

ISO/IEC. (2005). ISO/IEC 27001: Information Security Management Systems (ISMS) standard. Geneva: International Organization for Standardization.

ISO/IEC. (2009). ISO/IEC 31000: Risk management. International Organization for Standardization. Geneva, Schweiz.

ISO/IEC. (2011a). ISO 19011: Leitfaden zur Auditierung von Managementsystemen. International Organization for Standardization. Geneva, Schweiz.

ISO/IEC. (2011b). ISO/IEC 27005: Information security risk management. International Organization for Standardization. Geneva, Schweiz.

Klauck, K.-O. & Stegmann, C. (Herausgeber). (2012). *Basel III: Vom regulatorischen Rahmen zu einer risikoadäquaten Gesamtbanksteuerung*. Schäffer-Pöschel, Stuttgart.

Kuhlen, R. (1995). *Informationsmarkt. Chancen und Risiken der Kommerzialisierung von Wissen*. UVK Universitätsverlag, Konstanz.

Mitnick, K. (2002). *The Art Of Deception*. Hoboken, NJ, USA: Wiley & Sons.

Mosaic Security Research. (2012). Governance, Risk & Compliance (GRC) Software Guide. Zugriff am 19. August 2012, unter https://mosaicsecurity.com/categories/13-governance-risk-compliance

Müller, K.-R. & Neidhöfer, G. (2008). *IT für Manager*. Vieweg+Teubner Verlag, Wiesbaden.

NIST. (2002). Risk Management Guide for Information Technology Systems. National Institute of Standards und Technology. Zugriff am 19. August 2012, unter http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

OGC. (2012). ITIL Homepage. Office of Government Commerce, United Kingdom. Zugriff am unter http://www.itil-officialsite.com/home/home.aspx

Roe, D. (2011). IBM, Oracle, SAP Make Gartner GRC Magic Quadrant Leaders, But Small Vendors Hold Their Own. CMSWire, San Francisco, USA. Zugriff am 19. August 2012, unter http://www.cmswire.com/cms/information-management/ibm-oracle-sap-make-gartner-grc-magic-quad

rant-leaders-but-small-vendors-hold-their-own-012127.php

SEC. (2005). Spotlight on Sarbanes-Oxley Rulemaking and Reports. U.S. Securities und Exchange Commission. Zugriff am 19. August 2012, unter http://www.sec.gov/spotlight/sarbanes-oxley.htm

Ulich, E. (2005). *Arbeitspsychologie*. Schäffer-Pöschel, Stuttgart.

Health Insurance Portability and Accountability Act (HIPAA). (1996). Zugriff am unter http://www.legalarchiver.org/hipaa.htm

U.S. Government. (2002). The Sarbanes-Oxley Act. U.S. Government Printing Office. Zugriff am 19. August 2012, unter http://www.gpo.gov/fdsys/pkg/CRPT-107hrpt610/pdf/CRPT-107hrpt610.pdf

Welt Online (Herausgeber). (2012). Friedrich erwägt neues IT-Sicherheitsgesetz. Zugriff am 19. August 2012, unter http://www.welt.de/newsticker/news3/article108650186/Friedrich-erwaegt-neues-IT-Sicherheitsgesetz.html

Wikipedia. (2012a). IT-Grundschutz — Wikipedia, Die freie Enzyklopädie. Zugriff am 19. August 2012, unter http://de.wikipedia.org/w/index.php?title=IT-Grundschutz&oldid=100859542

Wikipedia. (2012b). Sicherheit — Wikipedia, Die freie Enzyklopädie. Zugriff am 4. Juli 2012, unter http://de.wikipedia.org/w/index.php?title=Sicherheit&oldid=102196504