Information Security Management Systeme

Christian Ludwig,
Matthias Siebke

Institut für Psychologie und Arbeitswissenschaft
Technische Universität Berlin

24. März 2010

Dies ist eine Einführung in Informationssicherheits-Managementsysteme (englisch: Information Security Management Systems; Abkürzung: ISMS). Es werden nur wenige grundlegende Kenntnisse über Sicherheitssysteme allgemein vorausgesetzt, um dem Inhalt folgen zu können.

Es wird gezeigt, wie mit einfachen Mitteln, vornehmlich dem Plan-Do-Check-Act Kreislauf, ein System zum Implementieren und Verifizieren von Sicherheitsmaßnahmen in der Informationstechnologie etabliert werden kann.

Dieses Dokument stellt einen ersten Schritt dar, um einen allgemeinen Überblick über ISMS zu bekommen.

Index-Begriffe: Information Security, IS, ISMS, ISO, ISO 9000, ISO 27001, ISM3

1 Einleitung

In Zeiten der fortschreitenden Technisierung dringen Computersysteme immer weiter in Organisationen vor. Die Technik soll den Arbeitsablauf der Mitarbeiter vereinfachen. Dazu werden Informationen in Computersystemen vorgehalten und in geeigneter Form in einzelnen Prozessschritten häppchenweise ausgegeben oder verändert. Mit dieser Methode gelingt es der Organisation einen Mitarbeiter mehr Informationen verarbeiten zu lassen, als es in der Vergangenheit ohne computergestützte Prozesse möglich war.

Informationen haben in unserer heutigen Gesellschaft einen sehr viel höheren Wert, als früher. Gerade im Hinblick auf eine angestrebte hundertprozentige Verfügbarkeit,

die überall und jederzeit gewährt sein soll oder der Nutzung von Informationen als geistiges Eigentum einer Organisation, hat man erkannt, dass diese Informationen schützenswerte Güter sind. Das Feld der Informationssicherheit strebt nach dem Schutz der in einer Organisation befindlichen Informationen und versucht mit Hilfe eines Managementsystems diesen Schutz zu formalisieren.

In den folgenden Kapiteln wird zunächst der Begriff des Informationssicherheits-Managementsystems genauer betrachtet. Dazu gehen wir auch auf die geschichtliche Entwicklung ein, um zu zeigen, warum diese spezielle Art der Managementsysteme notwendig geworden ist. Wir werden eine Taxonomie sehen und danach beispielhaft drei ISMS, den Standard ISO 27001, den BSI Grundschutz und den Standard ISM3, darstellen und vergleichen.

2 Begriffsklärung

Wenn man den Begriff *Information Security Management System* genauer betrachtet, fällt auf, dass er bereits eine Zusammensetzung aus mehreren einzelnen Begriffen ist. Wir werden die Bestandteile des Begriffs einzeln analysieren und am Ende zur vollständigen Bedeutung kommen, indem die Einzelteile wieder zusammen gefügt werden.

Zuerst klären wir den Begriff *Information*. Das Brockhaus-Lexikon beschreibt eine Information als

> Auskunft, Nachricht, Mitteilung, Belehrung; die formulierte Unterrichtung. ([1])

In der Informatik werden Informationen in der Regel als Daten kodiert und vorgehalten. In unserer Betrachtung müssen Informationen nicht zwingend als Daten in Rechnersystemen vorliegen, sondern es werden auch Informationen auf Papier sowie in den Köpfen der Menschen betrachtet

Information Security betrachtet demnach das Sichern aller Informationen einer Organisation. Dazu gibt es drei Schutzziele, die in der Informationssicherheit erreicht und aufrecht erhalten werden sollen ([2]).

1. Verfügbarkeit (englisch: availability)
2. Integrität (englisch: integrity)
3. Vertraulichkeit (englisch: confidentiality)

Häufig finden sich in der Literatur noch weitere Ziele, die sich jedoch in die oben genannten subsummieren lassen. Die hier vorgestellten Punkte bedeuten, dass auf eine Information immer dann zugegriffen werden kann wenn sie gebraucht wird (*Verfügbarkeit*), dass sie dann Unverfälscht ist (*Integrität*) und nur demjenigen zur Verfügung steht, der die notwendige Berechtigung hat sie zu erhalten (*Vertraulichkeit*).

Management Systeme existieren gleich mehrere in jeder Organisation. Ohne sie wäre sie nicht handlungsfähig. Sie sollen einen Regelkreis bilden, bestehend aus einer Zielsetzung, sowie der Realisierung mit anschließender Kontrolle. Schließlich soll auch eine Rückkopplung stattfinden, in der die Erfahrungen aus den vorigen Schritten reflektiert und Erkenntnisse für zukünftige Vorgehensweisen gewonnen werden können

([3], [4]). Damit kann das Management seiner lenkenden und kontrollierenden Funktion nachkommen.

Insgesamt kann man festhalten, dass mit einem *Information Security Management System* dem Management einer Organisation die Möglichkeit gegeben werden soll die Sicherheitsanforderungen der sich in der Organisation befindlichen Informationen zu definieren und durch geeignete Maßnahmen zu lenken. In den meisten Fällen strebt man dabei eine Erhöhung des Sicherheitsniveaus an.

3 Herkunft

Wir hatten bereits bemerkt, dass Informationen meist in Computersystemen abgelegt und verwaltet werden. Schauen wir uns also diese Computersysteme und die Gefährdung der darauf gespeicherten Informationen etwas genauer an.

In den frühen Tagen der Datenverarbeitung wurden Computer in Forschungseinrichtungen durch einen geschlossenen und kleinen Nutzerkreis bedient. Die Gefahren hier etwa böswillig Schaden anzurichten waren vergleichsweise gering, da jeder Nutzer namentlich bekannt war. Ferner lagen die meisten Informationen noch gar nicht in den Computersystemen vor. Die größte Gefahr ging jedoch in der Tat von unautorisiertem Zugriff auf den Rechner aus. Man ist dem durch Zugangskontrollsysteme und Zugangsbeschränkungen begegnet. Die Nutzung von Passworten ist seit dieser Zeit etablierte Praxis.

Während der Achtziger und Neunziger Jahre des zwanzigsten Jahrhunderts wurden Computersysteme immer preiswerter. Aufgrund des Vorteils ihrer enormen Rechenkraft haben sie schnell Einzug auch in Unternehmen gefunden. Informationen wurden immer öfter digital vorgehalten. Ein Austausch der Daten erfolgte via Disketten und später CD-ROMs. Die neue lauernde Gefahr waren nun Viren, welche sich mit den Medien verbreiteten. Als Gegenmaßnahme wurden Virenscanner etabliert.

Seit Mitte der neunziger Jahre des letzten Jahrhunderts gewinnt die Nutzung des Internets immer mehr an Bedeutung. Daten werden nun nicht mehr per Datenträger übergeben, sondern anonym im Netz verschickt. Hieraus ergeben sich gleich eine ganze Reihe neuer Sicherheitsprobleme. War es früher noch möglich die Herkunft von Daten zu verifizieren, wird dies heute zunehmend schwieriger. Aufgrund der Durchdringung des Internets in jede Lebenslage, hat sich eine Kultur des "always on" entwickelt. Menschen sind nun nahezu zu beliebiger Zeit erreichbar. Sie wollen ihre E-Mails jederzeit verfügbar haben. Durch Entwicklungen wie dem Smartphone – einem kleinen Computer in der Größe eines normalen Handys – ist dies nun auch möglich. Auch in Organisationen hat dieser Trend längst Einzug gehalten. War die IT-Infrastruktur eines Unternehmens vor einigen Jahren noch zentral an einem Ort, hat man es heute mit dezentraler Informationsverwaltung zu tun. Wir bekommen viele Informationen aus dem Internet oder zumindest über das Internet, zugespielt. Einige der sich hieraus ergebenden Gefahren sind Würmer, die sich auf Basis von Social Engineering durch das Internet verbreiten und von infizierten Rechnern sensible Informationen ins Internet verschicken.

Dadurch, dass dem Mitarbeiter einer Organisation nun mehr Informationen zur Ver-

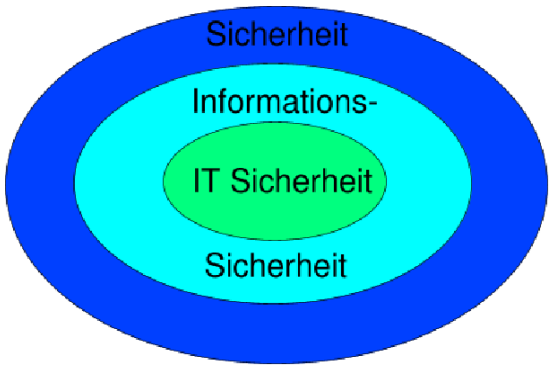

Abbildung 1: Darstellung der IT- und Informations-Sicherheit im Kontext der Gesamtsicherheit einer Organisation.

fügung stehen, steigt auch das Risiko, dass diese Informationen – meistens unbewusst – an unautorisierte Dritte weitergegeben werden. Dieser neu erkannten Bedrohung kann man nicht allein auf technischem Weg begegnen. Hier bedarf es zusätzlich organisatorischer Maßnahmen innerhalb des Unternehmens.

4 Taxonomie

Das Feld der Informationssicherheit ist historisch aus der IT-Sicherheit hervorgegangen. Hat man sich früher mit der IT-Sicherheit auf die Absicherung der technischen Systeme konzentriert, steht heute eher der Mensch im Fokus. Dieses Ziel, die Informationssicherheit, muss sich im Unternehmen in die gesamtheitliche Sicherheitsstrategie einpassen (Abbildung 1). Dazu muss sich eine Organisation ein selbst gestelltes Sicherheitsziel setzen und kontinuierlich darauf hinarbeiten. Dieses Sicherheitsziel sollte nach Erreichen auch aufrecht erhalten werden. Außerdem muss auf neuartige Bedrohungen reagiert werden können. All diese Anforderungen lassen sich auf verschiedenen Wegen erreichen. Dies führt uns zu den verschiedenen ISMS-Standards, die den Anspruch erheben, ein System bereitzustellen, welches die oben genannten Ansprüche erfüllt. Dabei lassen sich diese Standards in die folgenden Kategorien einteilen ([6]).

1. Prozessorientierte ISMS, z. B. CobiT, ITIL, CMMI, ISM3
2. Produktorientierte ISMS, z. B. Common Criteria
3. Controlorientierte ISMS, z. B. ISO 27001
4. Best-Practice orientierte ISMS, z. B. ISO 27002, ISF-SoGP
5. Risk-Management orientierte ISMS, z. B. CRAMM, ISO 27005, EBIOS

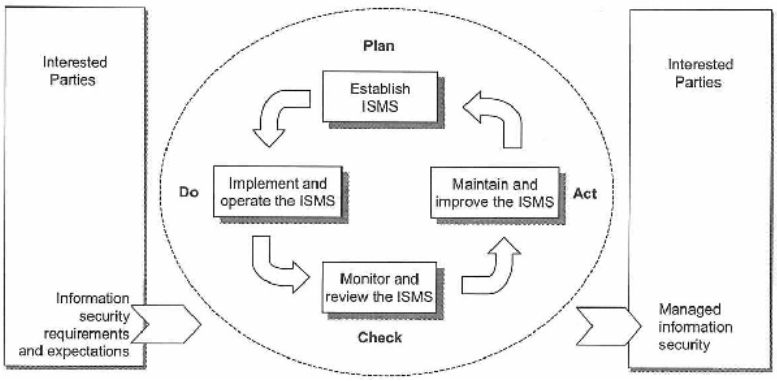

Abbildung 2: Darstellung des PDCA-Zyklusses in ISMS, Quelle: [7]

Diese Katalogisierung ist jedoch etwas unglücklich, da die einzelnen Kategorien nicht disjunkt sind. Es ist z. B. möglich einen best-practice orientierten Ansatz zu designen, der auf Prozessen basiert. Diese Kategorisierung zeigt nur die Herkunft der beispielhaft genannten Managementsysteme. Wie wir später noch sehen werden, gehören Controls ebenfalls zu einem prozessorientieren Ansatz dazu, wie Maßnahmen die auf best practices basieren. Man könnte daher die Kategorien best-practice orientiert, prozessorientiert und controlorientiert zusammenfassen.

5 Beispiele für ISMS

In nahezu allen Managementsystemen spielt der Plan-Do-Check-Act Zyklus eine zentrale Rolle. Bevor wir also detailliert auf einige ISMS eingehen, widmen wir uns erst einmal diesem Verfahren.

Abbildung 2 zeigt in schematischer Weise das Vorgehen beim Plan-Do-Check-Act Verfahren. Startpunkt des Zyklusses ist seine Initiierung, die, da es sich bei dem Verfahren um eine Hilfe für Management-Systeme handelt, durch das Management der Organisation erfolgen muss. Die Planungsphase wird erst betreten, nachdem die Organisation ein Defizit erkannt hat, das von den Notwendigkeiten oder den Erwartungen abweicht. Hierbei kann es sich z. B. um selbst gesteckte Ziele oder gesetzliche Vorschriften handeln.

In der *Plan*-Phase werden als erstes die Grenzen des Systems abgesteckt sowie Verantwortlichkeiten und Verfahren definiert. Innerhalb dieser Grenzen müssen dann Risiken erkannt, eingeschätzt und bewertet werden. Dies kann problematisch sein, da das System sehr groß sein kann. Hat man die Risiken erkannt, müssen geeignete Maßnahmen ergriffen werden. Diese werden in der *Do*-Phase meist in eigenen Projekten umgesetzt. In der darauf folgenden *Check*-Phase wird die Wirksamkeit der etablierten Maßnahmen abgeschätzt. Es werden Verbesserungen identifiziert, die in der *Act*-Phase als Korrekturmaßnahmen umgesetzt werden.

5.1 ISO 27001

Der Standard ISO 27001 ist aus dem "Code of Practice for Information Security" des Department of Trade and Industry der britischen Regierung im Jahr 1992 hervorgegangen ([8]). Das Dokument wurde 1995 durch das British Standards Institute in überarbeiteter Fassung erneut aufgelegt, diesmal als nationaler Standard BS7799. Später ist dieses Dokument zum internationalen Standard gereift, unter der Federführung der International Organisation for Standardisation (ISO). Es wurde im Jahr 2000 erst als Standard ISO/IEC 1799, und im Jahr 2005 als Standard ISO/IEC 27001 veröffentlicht. Es legt damit die Basis in einer Reihe von Standards im Bereich ISO/IEC 27000. Weitere Standards in dieser Reihe sind z. B. Leitlinien zur Implementierung (ISO 27003), Messmethoden (ISO 27004), Risikomanagement (ISO 27005) und Auditing (ISO 27006). In den nächsten Jahren wird es in diesem Bereich eine ganze Reihe neue – teilweise branchenspezifische – Standards geben, die ISO 27001 komplettieren. Ziel ist es die Sicherheit von Informationen in unterschiedlichen Organisationen vergleichbar zu machen und damit benchmarken zu können. Es soll ein Wettbewerb um gute Informationssicherheit am Markt entstehen.

ISO 27001 basiert auf dem Standard ISO 9001 ([7]) und erweitert diesen um Spezifika, die den Fokus speziell auf die Informationssicherheit legen. Es handelt sich um einen noch recht jungen Standard, die Adaption in Organisationen scheint gerade erst anzulaufen.

Wie schon erwähnt setzt ISO 27001 auf dem PDCA-Modell auf. Im folgenden werden wir auf die einzelnen Phasen des Modells eingehen und das Vorgehen in diesen Phasen, so wie es in ISO 27001 beschrieben ist, erläutern.

5.1.1 PDCA-Zyklus nach ISO 27001

Nachdem dem oberen Management einer Organisation die Notwendigkeit eines Managementsystems für Informationssicherheit durch interne oder externe Faktoren bewusst gemacht wurde, tritt man nach der Initialisierung des Prozesses in die *Plan*-Phase ein. Hier wird als erstes damit begonnen eine unternehmensweite ISMS-Policy zu erstellen. Diese Policy spiegelt die Unternehmensphilosophie wieder und dient als Grundlage für alle weiteren Entscheidungen. Im zweiten Schritt sind die Methoden zur Risikoeinschätzung und Bewertung festzulegen, sowie die zu schützenden Werte bzw. Informationen im Unternehmen (z.B. Forschungsdaten, Personalbögen, Server, etc.) zu identifizieren. Danach muss eine Bedrohungs- und Schwachstellenanalyse durchgeführt werden, um Risiko und Auswirkung einer Verletzung seiner Sicherheitsziele einschätzen zu können. In einem weiteren Schritt wird das vorhandene Risiko bewertet und anhand dieser Bewertung dann konkrete Maßnahmen zur Risikominimierung ausgewählt. Wichtig ist, dass am Ende dieser Phase das Restrisiko, welches ohne zweifel bleibt, durch das Management abgesegnet und getragen wird.

Mit den in der *Plan*-Phase beschlossenen Maßnahmen kann man nun in die Umsetzung (*Do*-Phase) eintreten. Hier sollte als allererstes festgelegt werden, mit welcher Priorität und in welcher Reihenfolge die Maßnahmen umzusetzen sind. Um das Umsetzen der beschlossenen Maßnahmen so effektiv wie möglich zu gestalten, ist also

ein Umsetzungsplan sowie die Definition von verantwortlichen Personen unabdingbar. Während des Implementierens der Maßnahmen werden parallel auch Methoden und Vorgehensweisen zur Überprüfung ihrer Wirksamkeit festgelegt, um später Aussagen über ihren Nutzen treffen zu können. Des Weiteren sollten in dieser Phase Awareness-Programme eingerichtet und Handlungsanweisungen zum Incident-Response gegeben werden. Aufgabe des Managements ist es die erforderlichen Ressourcen für die Umsetzung aller Maßnahmen bereitzustellen und freizugeben.

Der folgende Schritt, die *Check*-Phase, dient dem Überwachen und Kontrollieren der umgesetzten Maßnahmen. Das soll heißen, dass hier jetzt die Methoden zum Überwachen und Einschätzen der Wirksamkeit der Maßnahmen angewandt und ausgewertet werden. Sinn ist es eine Aussage über die Wirksamkeit der umgesetzten Maßnahmen treffen zu können, um anschließend eine wiederholte Risikoeinschätzung durchzuführen. Dazu sind die Berichte aus den Incident-Response Systemen sowie Ergebnisse aus internen oder externen Audits heranzuziehen. Aber auch das Management ist in dieser Phase gefragt. Seine Aufgabe ist es das gesamte ISMS zu beobachten und zu bewerten und anschließend Verbesserungen auszuarbeiten, die dann in der nächsten Phase umgesetzt werden.

In der letzten Phase des PDCA-Zyklusses, der *Act*-Phase, werden die identifizierten Verbesserungen implementiert, sowie die Korrektur- und Präventionsmaßnahmen dokumentiert. Sie dient also der Pflege und Verbesserung der einzelnen Maßnahmen aber auch des gesamten Managementsystems. Wichtig in dieser Phase ist, dass die Verbesserungen in die Organisation kommuniziert und eine Erfolgskontrolle anhand der Messmethoden und Messgrößen vorgenommen wird.

Bei größeren Änderungen können die *Do*-Phase und die *Act*-Phase als eigener PDCA-Zyklus aufgesetzt werden. Das hat den Vorteil, dass eine an sich komplexe Änderung an einem bestehenden System in kleine handhabbare Stücke herunter gebrochen werden kann. Allerdings dauert eine solche Abarbeitung in untergeordneten PDCA-Zyklen relativ lange. Die Umsetzung der allgemeinen Information Security Policy ist ein Beispiel für dieses Herunter brechen. Die Information Security Policy ist meistens eines der ersten Dokumente, die im Zuge der Implementierung eines ISMS nach ISO 27001 entsteht. Sie selbst beschreibt nur sehr allgemein wonach eine Organisation im Zuge ihrer Umsetzung dieser Policy strebt. Aus diesen Gedanken gehen viele Änderungsanforderungen oder auch Neuausrichtungen in einigen Bereichen hervor. Die Umsetzung jeder dieser Anforderungen kann man einen separaten PDCA-Zyklus vornehmen. Dieses Vorgehen kann man dabei auch rekursiv in den neu abgeleiteten PDCA-Zyklen etablieren. Dabei werden in den darunter liegenden Zyklen immer kleinere Änderungen betrachtet. Diese Änderungen lassen sich irgendwann mit einfachen Messmethoden und Messgrößen kontrollieren. In den übergeordneten Zyklen werden die Messmethoden und Messgrößen abstrakter. Schließlich hat man in der obersten Ordnung allgemeine Messgrößen, die die Sicherheit insgesamt beschreiben.

Ein weiteres wichtiges Augenmerk legt die ISO bei der Einführung und dem Betrieb eines Managementsystem für Informationssicherheit auf die Dokumentation. Hier wird nicht nur verlangt, dass alle wichtigen Erklärungen, wie beispielsweise die ISMS Leitlinie, vorhanden sind und alle Verfahren und Methoden die innerhalb des ISMS zur Anwendung kommen lückenlos dokumentiert werden, sondern auch, dass ein System

zur Lenkung der Dokumente etabliert sein soll. In solch einem System muss festgelegt sein in welcher Art und Weise die Dokumente kontrolliert, aktualisiert, veröffentlicht und vom Management abgezeichnet und freigegeben werden.

5.1.2 Controls

Man erkennt beim Analysieren des ISO 27001, dass sich das System sehr stark auf Messmethoden und Messgrößen stützt. Um verlässliche Aussagen über ein abstraktes Ziel wie Sicherheit zu bekommen, muss man verschiedene Anhaltspunkte haben, die in die Gesamtaussage eingehen. Dabei wird auf empirische Größen zurückgegriffen, denen eine Relevanz zur Aussage innewohnt. Bei ISO 27001 wird ein Problem oder eine Fragestellung mit Controls bewertet. Diese Controls sind die Messgrößen in meinem Gesamtsystem, was der gesamten Organisation entspricht, die den Grad der Zielerfüllung widerspiegeln. Die Auswahl der Controls gibt der Standard nicht vor. Es werden Empfehlungen als Best-Practice Ansatz gegeben, allerdings liegt die Bewertung eines Messwertes als geeignetes Control bei den durchführenden Personen.

Die Auswahl der Controls ist also enorm wichtig. Die Nutzung eines schlecht bewerteten Controls kann dazu führen, dass an dieser Stelle im System keine korrigierenden Maßnahmen ergriffen werden, obwohl es eigentlich notwendig wäre. Wie kann man aber Controls bewerten und schlecht passende Controls heraus filtern? Leider gibt es hierfür kein Patentrezept. Eine gute Herangehensweise ist es die identifizierten Controls in einer Gruppe von Experten zu diskutieren. Man sollte auch nicht nur ein Control für einen Sachverhalt heranziehen. Zu guter Letzt kann man die verschiedenen Controls, die das Ziel beschreiben gewichten. Es ist auch möglich einen regelmäßigen Review der Controls durchzuführen. Alle diese Maßnahmen dienen der Minimierung der entstehenden Fehler durch die Auswahl unpassender Controls.

Die Controls selbst dienen auch als Grundlage zur Performance-Messung des ISMS. Man kann daraus ableiten, wie schnell beispielsweise auf erkannte Unzulänglichkeiten in der Sicherheitsarchitektur reagiert wird. Damit ist eine Kontrolle des ISMS durch das Management möglich.

5.2 BSI Grundschutz

Ein weiterer Standard, der ein Modell zur Implementierung eines ISMS bereitstellt, ist der vom Bundesamt für Sicherheit in der Informationstechnik(BSI) herausgegebene BSI 100-1 ([5]). Dieser ist vor allem in Deutschland zu Hause und wird daher auch meist von deutschen Behörden implementiert.

Er sieht, wie alle anderen Standards auch, Sicherheit nicht als einen unveränderlichen Zustand an, der einmal erreicht bestehen bleibt. Vielmehr möchte man auch mit dem BSI 100-1 den ständigen Änderungen in einem Unternehmen und damit auch in der Sicherheit Rechnung tragen. Dazu setzt das BSI auch auf den bewährten PDCA-Zyklus. Abgebildet wird dieser Kreislauf hier auf zwei Bereiche: erstens auf den Lebenszyklus des Informationssicherheitsprozesses, der als übergeordneter Prozess zur Etablierung und Aufrechterhaltung des gesamten ISMS dient und zweitens auf den Lebenszyklus

des Sicherheitskonzeptes, welches alle Rahmenbedingungen, Konzepte und Handlungsanweisungen zur Umsetzung und Implementierung des ISMS beinhaltet. Dabei sind die einzelnen Handlungsschritte, die im Sicherheitskonzept vorgesehen und während der PDCA-Phasen ablaufen sollen, denen der ISO 27001 sehr ähnlich. Das BSI stellt daher auch eine Abbildung seiner Konzepte auf die Konzepte der ISO bereit, um zu zeigen, dass ein implementierter BSI 100-1 Standard auch konform zu den Anforderungen des ISO 27001 ist.

Das BSI geht allerdings noch ein Stück weiter. Führt die ISO nur sehr grobe Handlungsempfehlungen für die Umsetzung eines ISMS auf, so stellt das BSI mit seinen Standards BSI 100-2, BSI 100-3 und dem sehr umfassenden Grundschutzkatalog eine konkrete Implementierung der im BSI 100-1 vorgestellten Konzepte bereit. Dabei beschreibt die IT-Grundschutzvorgehensweise im BSI 100-2 im Detail jeden Schritt, der für die Umsetzung des BSI 100-1 notwendig ist. Mit dem BSI 100-3 (Risikoanalyse auf Basis des IT Grundschutz) gibt einem das Bundesamt ein konkretes Verfahren zur Risikoanalyse an die Hand, welches alle Anforderungen an ein solches Verfahren erfüllt. Der IT Grundschutzkatalog ist eine umfangreiche Sammlung von konkreten Handlungsempfehlungen zur Absicherung einer Vielzahl von IT- und Organisationskomponenten. Er soll genutzt werden um seine eigene Unternehmensstruktur nachzubilden und durch die Umsetzung der empfohlenen Maßnahmen schnell ein gewisses Sicherheitsniveau zu erreichen.

5.3 ISM3

Die Abkürzung ISM3 steht für *Information Security Management Maturity Model*. Es handelt sich dabei um einen Industriestandard, der von einem Konsortium aus Firmen des Bereichs IT-Consulting entwickelt wurde. Die neueste Version[1] stammt aus dem Jahr 2007. Die Entwicklung wird von der Community vorangetrieben und der Standard auch unter einer freien Lizenz, der Creative Commons, herausgegeben. Dies ermöglicht eine offene Weiterentwicklung des Standards. Neue Vorschläge aus der Community werden durch die Firmen des Konsortiums in den Standard integriert.

ISM3 erweitert den internationalen Standard ISO 9000 für Qualitätsmanagementsysteme. Es enthält ein Framework, in dem Verantwortlichkeiten innerhalb der Organisation genau festgelegt werden und ist daher kompatibel zu CobiT. Es wird ein prozessorientierter Ansatz verfolgt (siehe Kapitel 4). In einigen Konfigurationen ist ISM3 auch kompatibel zum bereits dargestellten Standard ISO 27001.

Das zugrunde liegende Modell des Standards basiert auf fest definierten Prozessen und daraus abgeleiteten Metriken. Die Grundlage der Prozesse bildet das Sicherheitskonzept der Organisation. In diesem gehen die unterschiedlichen Bedingungen der Fachbereiche und dessen Sicherheitsbetrachtungen ein. Alle Prozesse des ISM3 sind zu einem sehr detaillierten Grad vorgegeben. Es besteht nur sehr wenig Spielraum Prozesse an die Organisationsstruktur anzupassen. Unter anderem wird genau definiert welche Ein- und Ausgaben ein Prozess hat, welche Aktivitäten in ihm stattfinden müssen und welche Reichweite diese Aktivitäten haben. Es wird ferner angegeben wie oft

[1] zum Zeitpunkt als dieses Paper entstand war dies Version 2.11

der Prozess einem Review unterzogen werden muss und welcher Personenkreis an dem Prozess teilnehmen muss und wer die Ausführung zur Kenntnis nehmen muss. Jeder Prozess wird durch Handlungsanweisungen und Berichte genau dokumentiert, wobei auch die Dokumente und deren Inhalte genau vorgegeben sind. Zu jedem Prozess gibt es einen Besitzer, der die Ausführung überwacht und die dessen Aufsicht übernimmt.

ISM3 definiert als Sicherheitsziel verschiedene Reifegrade, von denen fünf Stück existieren. Diese Reifegrade unterscheiden sich nur in der Menge der umzusetzenden Prozesse. Dabei wird noch unterschieden, ob die Prozesse durch ihren Besitzer nur geführt werden, oder ob sie auch durch die Nutzung von Metriken verbessert werden.

Ein ISMS nach ISM3 wird durch einen Initialisierungsprozess in die Organisation implementiert. Darin wird ein Chief Information Security Officer definiert, der den gesamten Komplex der Information Security innerhalb der Organisation verantwortet. Es wird der zu erzielende ISM3-Level unter Berücksichtigung aller Regularien gewählt. Außerdem wird der zentrale Prozess des Dokumentenmanagements etabliert und die Arbeitsbereiche des strategischen, taktischen und operativen Managements erstellt.

Das strategische Management übernimmt die Führung und Koordination des ISMS. Es muss die benötigten Ressourcen für zur Verfügung stellen und verantwortet das Review aller ausgeführten Prozesse. Der wichtigste Prozess den ISM3 dem strategischen Management zuschreibt ist das Reporting an die Stakeholder. Daran erkennt man den klaren Einfluss, der von außen auf das Management wirkt.

Das taktische Management definiert die zu erreichenden Sicherheitsziele, die Metriken, welche in den Prozessen, Handlungsanweisungen und Berichten zu nutzen sind, sowie die Prioritäten nach denen das Sicherheitsziel angegangen wird. Hierzu ist ein Prozess definiert, der die Sicherheitsziele und die zu schützenden Objekte einer Organisation definiert und katalogisiert. das taktische Management kümmert sich auch um die Konformität des Sicherheitsziels mit geltendem Recht. Durch das taktische Management wird ein Asset- und Lifecycle-Management etabliert und Servicelevel ausgehandelt.

Das operative Management setzt die Änderungen des strategischen und taktischen Managements um. Die IT-Systeme werden hierbei über ihren gesamten Lifecycle hinweg betreut. Über die vorgegebenen Prozesse findet eine Incident- Prevention statt, sodass Sicherheitsvorfälle bereits im Vorhinein erkannt und verringert werden können.

6 Schlussbemerkung

Die Notwendigkeit eines Managementsystems für Informationssicherheit in Unternehmen ist unumstritten. Informationssicherheit kann man heutzutage nicht mehr nur durch die technische Absicherung der Computersysteme gewährleisten, sondern muss sie auf organisatorische Ebene angehen. Doch dies ist vielen Unternehmen noch nicht klar. So haben weltweit nur rund 6400 Unternehmen eine ISO 27001 Zertifizierung erhalten, davon 136 Unternehmen in Deutschland ([9]). Das zeigt zum einen, dass noch viel Handlungsbedarf in Richtung Informationssicherheitsmanagement besteht, zum anderen aber auch, dass in diesem Bereich zukünftig viel Potential zum Geld verdienen liegt.

Hier haben einige Firmen bereits diesen aufstrebenden Markt entdeckt. Die Firmen des Konsortiums um ISM3 machen einen solchen Eindruck. Sie geben Organisationen in ihrem Standard unterschwellig die Möglichkeit das gesamte Management der Informationssicherheit auszulagern an einen ihrer Partner. Sie brüsten sich auch damit anders zu sein, als ISO 27001, merken jedoch an, dass man auch in ihrem System Controls benötigt. Auf diese zentrale Eigenschaft jedoch gehen sie nur spärlich ein. Es entsteht der falsche Eindruck aus vordefinierten Prozessen an alles gedacht zu haben und das Thema Informationssicherheit vollständig im Griff zu haben.

Denn auch der Gesetzgeber stellt zunehmend die Anforderung an Unternehmen ein ISMS zu implementieren. So fordert die Bundesregierung beispielsweise mit dem Bundesdatenschutzgesetz die Absicherung personenbezogener Daten und mit dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ein Risikomanagement in Unternehmen, dass auch die IT-Sicherheit mit berücksichtigt.

Doch nicht nur durch gesetzliche Vorgaben können Unternehmen dazu gebracht werden ein ISMS einzuführen. Auch der immer stärker werdende Konkurrenzkampf führt dazu, dass Unternehmen eine Zertifizierung nach ISO 27001, BSI 100-1 oder ISM3 anzustreben. Denn solche Zertifizierungen können im Weltmarkt als Aushängeschild und schlussendlich auch als Wettbewerbsvorteil angesehen werden. Die verschiedenen Standards machen diesen Wettbewerbsvorteil dann vergleichbar und transparent. Dies geschieht allerdings nur auf einer sehr abstrakten Ebene. Wir haben gesehen, dass der Standard ISO 27001 nur sehr diffuse Handlungsempfehlungen und Definitionen vorgibt. So muss man viel Arbeit darin investieren, die richtigen Maßnahmen zum Erreichen seiner Sicherheitsziele zu identifizieren und geeignete Controls auszuwählen. Der Ruf nach einem handfesten Maßnahmenkatalog, der detailliertere Handlungsempfehlungen enthält, wird daher immer lauter. Eine zu genaue Vorgabe von Maßnahmen, wie es das BSI mit seinen Grundschutzbausteinen tut, kann jedoch auch dazu führen, dass solche Maßnahmen nicht mehr nur als Empfehlung gesehen werden. Ein Unternehmen sollte sich immer im Klaren darüber sein, dass es niemals alle Ansprüche abdecken kann und somit für spezielle Bedürfnisse immer individuelle Maßnahmen getroffen werden müssen. Es ist zwar immer besser einen vorgefertigten Maßnahmenkatalog abzuarbeiten, als gar keinen Schutz zu haben, doch diese Kataloge sollten niemals als Checkliste angesehen werden, deren Abarbeitung dann ausreicht um geschützt zu sein.

Doch auch mit Hilfe der besten Managementsysteme lässt sich keine Erhöhung der Sicherheit in ein Unternehmen bringen, wenn nicht jeder Mitarbeiter ein Bewusstsein für sicheres Handeln hat. Derzeitige ISMS decken diesen Aspekt nur dürftig ab. Zukünftig sollten ISMS also nicht nur mit umfangreicheren Bibliotheken aus Maßnahmen und konkreteren Methoden zur Risikobewertung aufwarten, sondern auch den Sicherheitskulturgedanken mit aufnehmen. Ein angestrebtes Niveau an Informationssicherheit ist nur zu erreichen und anschließend auch zu halten, wenn sich alle, vom Top Manager bis zum einfachen Mitarbeiter, der Notwendigkeit bewusst sind täglich Sicherheit zu leben.

Literatur

[1] dtv Brockhaus Lexikon in 20 Bänden, 1988

[2] Allen, Julia H., "The CERT Guide to System and Network Security Practices", Addison-Wesley, 2001

[3] International Organisation for Standardization, "ISO 9000: 2000: Quality Management Systems – Fundamentals and Vocabulary", 2000

[4] International Organisation for Standardization, "ISO 9001: 2000: Quality Management Systems – Requirements", 2000

[5] BSI – Bundesamt für Sicherheit in der Informationstechnik, "Informationssicherheit und IT-Grundschutz: BSI-Standards 100-1, 100-2, 100-3", 2008

[6] ISM3 Consortium, "ISM^3 – INFORMATION SECURITY MANAGEMENT MATURITY MODEL", v2.11, 2007

[7] International Organisation for Standardization, "ISO 27001: 2005: Information Security Management Systems – Requirements", 2005

[8] Webseite http://www.pc-history.org/17799.htm, "The History of ISO 17799 and ISO 27001", abgerufen am 06.02.2010 21:30

[9] Webseite http://www.iso27001certificates.com/, "International Register of ISMS certificates", abgerufen am 22.11.2009 17:00