DuD
Datenschutz und Datensicherheit

Information Security Management

Vom Prozess zur Umsetzung

Dörte Neundorf, Holger Petersen

IT-Sicherheitsmanagement ist ein zentraler Teil einer proaktiven Risiko-Steuerung. Dörte Neundorf und Holger Petersen stellen in ihrem Beitrag die Elemente eines Sicherheitsmanagements vor und beschreiben eine in der Praxis bewährte Vorgehensweise zum Aufbau eines IT Security Management Prozesses.

Dr. Dörte Neundorf

Security Consultant bei der Secorvo Security Consulting GmbH. Arbeitsschwerpunkt: Public Key Infrastrukturen, E-Mail-Sicherheit, IT-Security-Management und Awareness für IT-Sicherheit.
E-Mail: neundorf@secorvo.de

Dr. Holger Petersen

Security Consultant bei der Secorvo Security Consulting GmbH. Arbeitsschwerpunkt: Sicherheitsanalysen und Reviews, Digital Rights Management Lösungen und IT-Sicherheitsmanagement.
E-Mail: petersen@secorvo.de

1 Motivation

Informationen sind wichtige Geschäftsgüter. In fast allen Unternehmensbereichen werden sie zur Abwicklung oder zur Unterstützung von Geschäftsprozessen zwingend benötigt. Ohne effiziente Informationsverarbeitung – innerhalb und außerhalb der IT – sind heute viele Aufgaben nicht mehr oder nur noch mit starken Einschränkungen zu bewältigen.

Lange reichte es aus, besonders sensitive Informationen einzeln speziell zu schützen, etwa durch einen dedizierten Server mit Verschlüsselungstechnologien oder durch spezielle Zugangskontrollen für bestimmte Räume. Doch durch die starke Integration der Informationsverarbeitung ist eine solche isolierte Betrachtung nicht mehr möglich. Werden Informationen von einer Vielzahl von Prozessen genutzt und verarbeitet, spielt die Sicherung von Integrität, Vertraulichkeit und Verfügbarkeit über ihren gesamten Lebenszyklus eine wichtige Rolle für das Unternehmen.

Die Informationssicherheit muss deshalb eben so ganzheitlich betrachtet werden wie die Informationsverarbeitung: als ein fortlaufender Information-Security-Management-Prozess für das ganze Unternehmen. Information Security Management (ISM) bezeichnet dabei die Planungs- und Lenkungsaufgabe eines durchdachten und gesteuerten Sicherheitsprozesses. Dieser ist Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen.

Der ISM-Prozess ist sehr komplex. In vielen Großunternehmen ist bereits ein ISM-Prozess implementiert und mit vielen Ressourcen ausgestattet. Aber auch für kleine und mittlere Unternehmen ist ein solcher Prozess sinnvoll und hilfreich – gerade dann, wenn Informationen einen wichtigen Teil des Geschäftserfolgs ausmachen – z. B. weil das Unternehmen hochkomplexe Produktionsvorgänge beherrschen muss oder das Marketing stark von einem effizienten Management der Kundendaten abhängt.

Im folgenden Beitrag werden ein etwas vereinfachter Ansatz des ISM-Prozesses vorgestellt und Hinweise gegeben, wie dieser organisatorisch und aus Prozesssicht in ein Unternehmen zu integrieren ist. Dabei wird besonderer Wert auf Tipps für die Praxis gelegt, die eine Umsetzung nach den Bedürfnissen und den Ressourcen des Unternehmens ermöglicht.

Ist Information Security Management gleichzusetzen mit IT-Security-Management? In vielen Fällen wird das ISM einen sehr großen IT-Anteil beinhalten, da die Informationen in IT-Systemen besonders bedroht sind und da die Maßnahmen für IT spezifischer und vielfältiger sind als für in anderer Form vorliegende Informationen. Je mehr Informationen auch in anderer Form vorliegen (z. B. Messergebnisse, Probeteile), umso mehr muss auch dieser Aspekt in das ISM aufgenommen werden. Und schließlich spielt auch der persönliche Umgang der Mitarbeiter mit den Informationen eine Rolle, z. B. auf Messen oder im Freundeskreis, ebenfalls ein wichtiger Bereich außerhalb der IT-Systeme. Insofern besteht eine enge Verbindung zwischen Informationssicherheit und IT-Sicherheit einerseits, aber auch zwischen Informationssicherheit und z. B. dem Werkschutz andererseits.

Damit das Information-Security-Management seiner Bedeutung gerecht werden kann, sollte es über das **Risikomanagement** im Unternehmen verankert werden. Im Rahmen des Risikomanagements werden u. a. operationelle Risiken gemanagt, zu denen ebenfalls der Bereich Informationssicherheit gehört.[13]

[13] Siehe Romeike, in diesem Heft.

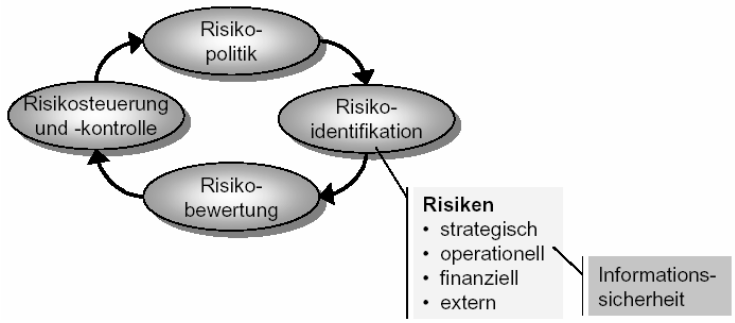

Abbildung 1: Risikomanagement-Prozess eines Unternehmens [RiNe02]

2 Der ISM-Prozess

Information-Security-Management (ISM) ist ein Prozess – also eine fortlaufende Verantwortlichkeit. **Ziel** des Prozesses ist das Management aller Maßnahmen der Informationssicherheit, um das Sicherheitsniveau auf ein angestrebte Niveau zu bringen und es dort zu halten sowie Informationen über den Status der Informationssicherheit und auftretende Probleme zu sammeln und darauf zu reagieren.

Für die Zusammenarbeit mit den anderen mit der Informationssicherheit befassten Organisationseinheiten und auch generell gilt: Information-Security-Management beinhaltet – neben den technischen und organisatorischen Aspekten – sehr stark die **Überzeugung** des Unternehmens als Ganzem und die der Mitarbeiter individuell von den Anliegen der Informationssicherheit. Insofern ist der Anteil der Kommunikations- und Integrationsaufgaben an der alltäglichen Arbeit des Information-Security-Management hoch.

Wird ein umfassender ISM-Prozess neu eingeführt, so wird sich häufig ein zweistufiger **Ablauf** ergeben:

- Im ersten Schritt erfolgt – mit u. U. recht großem Aufwand – der initiale Aufbau einer Sicherheits-Architektur [14] (entweder „from Scratch“ oder unter Nutzung bereits vorhandener Strukturen). Dies hat häufig Projektcharakter, ist also eine zeitlich begrenzte Aufgabe.
- Ist eine Architektur vorhanden, wird sie dann einer regelmäßigen Kontrolle, ständigen Weiterentwicklung und Verbesserung unterworfen. Dies ist der eigentliche Prozess des Information-Security-Managements

Beide Teile sind normalerweise Teil der Aufgaben der Organisationseinheit, die für das Information-Security-Management zuständig ist. Wichtig beim Aufbau eines ISM-Prozesses ist die Zuordnung der **Verantwortlichkeiten**. Initial gilt: Eine Sicherheitspolitik ist Voraussetzung eines sinnvollen ISM-Prozess. Ihre Festlegung ist nicht Aufgabe des Information-Security-Managements, da sie dessen Kompetenzen und Aufgaben erst festlegt. Anders formuliert: Nur wenn die Geschäftsleitung Informationssicherheit als Unternehmensziel definiert, in die anderen Unternehmensziele einordnet und elementare Randbedingungen (grundsätzlich tolerierbare Risiken, Budget, grundlegende Verantwortlichkeit) vorgibt, kann ein Information-Security-Management tatsächlich die gewünschten Ergebnisse erreichen.

Wichtig für den Erfolg ist auch eine geeignete **organisatorische Zuordnung** im Unternehmen: Das Information-Security-Management ist verantwortlich für die Informationssicherheit im Unternehmen oder Bereich – also für die Umsetzung der Vorgaben der Geschäftsleitung. Es ist daher meist direkt dem Vorstand zugeordnet – entweder als eigenständige Organisationseinheit oder innerhalb einer anderen Einheit, z. B. der Corporate Security.

Eine Zuordnung zur IT ist mehr und mehr unüblich. Damit geht man zum Einen Interessenskonflikten aus dem Weg und erhöht die gegenseitige Kontrollwirkung. Zum Anderen führt eine Betrachtung der Informationssicherheit aus IT-Sicht häufig dazu, dass Informationen und Risiken außerhalb der IT vernachlässigt werden und sich die Maßnahmen nur auf die IT konzentrieren.

Die **Revision** kontrolliert die Umsetzung der Maßnahmen und ggf. auch dessen Eignung zur Realisierung der strategischen Vorgaben. Inwieweit sie dabei die tatsächliche Umsetzung in den Fachbereichen überprüft oder lediglich das Information-Security-Management auditiert (das dann wiederum die Fachbereiche prüft), hängt von den spezifischen Gegebenheiten ab. Der **Datenschutzbeauftragte** wird – aufgrund seiner vom Gesetz vorgeschriebenen Aufgaben, die sich nicht mit den Anforderungen an das Information-Security-Management decken – meist nicht dem Information-Security-Management zugeordnet.

Trotz dieser organisatorischen Trennung ist eine enge **Zusammenarbeit** zwischen Information-Security-Management, Revision und Datenschutz wünschenswert. Erfahrungsgemäß fördert eine klare Zuordnung und Abgrenzung der Verantwortlichkeiten die Effizienz der Zusammenarbeit. Des Weiteren wird das Information-Security-Management eng mit Fach- und IT-Abteilung zusammenarbeiten; inwieweit die Einrichtung von Bereichsbeauftragen für Informationssicherheit sinnvoll ist und ob diese der IT oder dem Information-Security-Management zugeordnet werden, ist wieder nach unternehmensspezifischen Bedürf-

Abbildung 2: Information-Security-Management-Prozess

[14] Unter der Sicherheitsarchitektur eines Unternehmens ist die Gesamtheit aller in den Unternehmensbereichen realisierten Sicherheitspolicies und der daraus abgeleiteten Sicherheitsmaßnahmen zu verstehen. Im Rahmen dieses Gesamtkonzepts werden zudem die Verantwortlichkeiten festgelegt sowie die Prozesse definiert.

nissen zu entscheiden.[15]

Wir schlagen aus diesen Gründen folgendes Modell für den Information-Security-Management-Prozess vor. Es hat sieben Stufen (in Anlehnung an [BSI_GSHB]) wie in Abbildung 2 dargestellt:

- Durch die Geschäftsführung –verantwortlich für die Strategie – wird die **Sicherheitspolitik** festgelegt.
- Auf Basis der Sicherheitspolitik wird eine **Bedrohungs- und Risikoanalyse** durchgeführt, die Aufschluss über den Zustand und die Gefährdung der bestehenden (oder ggf. geplanten) Systeme und Strukturen gibt.
- Die Risikoanalyse ist Ausgangspunkt der Entwicklung von **Sicherheitskonzepten**, die Maßnahmen zur Senkung des Risikos auf ein akzeptables und sinnvolles Niveau erhalten.
- Die Fachbereiche führen die **Umsetzung** der Maßnahmen sowie entsprechende **Schulungen** und **Sensibilisierungen** durch. Sie berichten dabei an das Information-Security-Management über ihren Fortschritt und über Schwierigkeiten.
- Ebenfalls die Fachbereiche sind für den **Betrieb** der Informationssicherheit verantwortlich. Auch hier wird regelmäßig an das ISM berichtet.
- Das ISM übernimmt die **Steuerung** des Prozesses und reagiert damit auf die Ergebnisse der Umsetzung und die Berichte. Dadurch werden, wenn erforderlich, Änderungen in der Konzeption veranlasst.

Idealerweise beginnt ein ISM-Prozess tatsächlich mit der Festlegung der Strategie – in der Praxis ist ein Einstieg auch an anderer Stelle möglich. Häufig beginnt der Prozess mit dem Einsetzen des Steuerungselements ISM, dessen Aufgabe dann die Einrichtung des Gesamtprozesses ist.

Außerdem wird man in der Praxis im Allgemeinen nicht mit der Betrachtung des ganzen Unternehmens beginnen, sondern mit einem einzelnen Bereich. Nach und nach werden dann die weiteren Elemente der Architektur (vgl. Abbildung 3) ergänzt. U. U. wird dazu der in Abbildung 2 dargestellte Prozess einschließlich Rückkopplung („Regelung“) durch das ISM mehrfach durchlaufen und bei jedem Durchlauf der betrachtete Ausschnitt des Unternehmens vergrößert.

[15] Zur Gestaltung einer solchen unternehmensspezifischen Struktur siehe Bijok und Triedwindt, in diesem Heft.

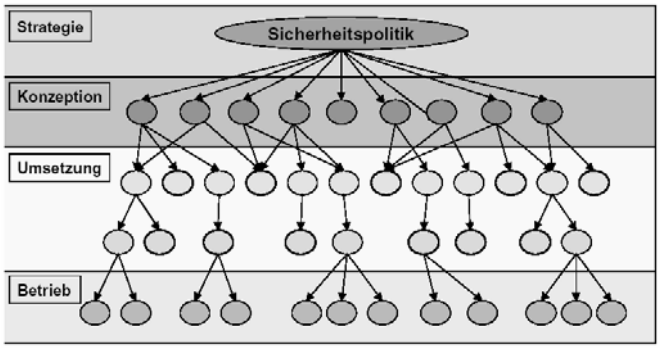

Abbildung 3: Darstellung einer Sicherheitsarchitektur

In den folgenden Abschnitten beschreiben wir die einzelnen Schritte in der idealisierten Reihenfolge. Wie ein „Seiteneinsteig“ in der Praxis aussehen kann, wird in Kapitel 3 diskutiert. Mit dem Thema Information Security Management beschäftigen sich auch einschlägige Standards [ISO 13335, ISO17799, IT_GSHB]. Eine gute Zusammenfassung über die Zielsetzung und die Inhalte dieser Standards gibt [D21_01].

2.1 Entwicklung einer Sicherheitspolitik

Voraussetzung eines Information-Security-Managements sind klare Vorgaben der Geschäftsleitung, nach denen sich der Management-Prozess richten kann und die eine Messlatte für das Erreichte bieten. Ohne solche Vorgaben ist kein umfassendes Management möglich. Natürlich kann man trotzdem Maßnahmen zur Informationssicherheit ergreifen, sie werden sich aber nach den Bedürfnissen der Anwender richten und damit in verschiedenen Fachbereichen unterschiedlich sein. Damit sind sie oft kaum vergleichbar und schlecht übertragbar, außerdem fehlt die zentrale Koordination. Damit wird das Ziel eines angemessenen und durchgängigen Sicherheitsniveaus im Unternehmen nicht erreicht.

Ohne eine demonstrative Unterstützung durch die Geschäftsleitung hat ein ISM kaum Möglichkeiten, die erarbeiteten Maßnahmen auch durchzusetzen: Die zentral festgelegten Maßnahmen können aus Sicht einzelner Teilbereiche durchaus – zumindest kurzfristig – eine Verschlechterung oder Verteuerung bringen oder schlicht ungewohnt sein. Daher ist eine Umsetzung ohne „Unterstützung von ganz oben“ recht unwahrscheinlich.

Trotzdem wird es in der Praxis manchmal nicht möglich sein, eine unternehmensweite Sicherheitspolitik durchzusetzen. Wird trotzdem ein ISM eingesetzt, ist es ratsam, dessen Verantwortungsbereiche und das verfolgte Ziel klar abzugrenzen. Dies könnten z. B. sein:

- nur bestimmte Bereiche (z. B. Entwicklung, Produktion, Forschung)
- nur bestimmte Aufgaben (z. B. Beratung, Vorschläge, Awareness)
- nur bestimmte Ziele (z. B. Steigerung der Sensibilisierung, Verfügbarkeit von Werkzeugen und Methoden)

wobei keine Widersprüche auftreten dürfen. Beispielsweise wäre das Ziel, Virenschutz auf allen Rechnern einzuführen, wohl unvereinbar mit der Aussage, dass sich der Zuständigkeitsbereich nicht auf die Forschung bezieht, oder eine Beratung aller Geschäftsbereiche in allen Fragen der Informationssicherheit kaum möglich, wenn keine Personalkapazität oder ein entsprechendes Budget zur Verfügung steht.

Auch hier gilt: Ein Information-Security-Management ist umso glaubwürdiger, wirkungsvoller und effizienter, je klarer die Ziele in der Sicherheitspolitik formuliert und kommuniziert werden und je realistischer sie sind.

Wenn der Beschluss gefallen ist, eine Sicherheitspolitik einzuführen, sollte eine

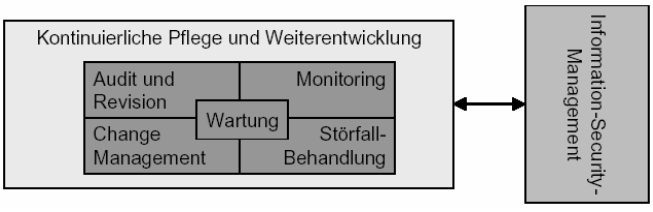

Abbildung 4: Aufgabenbereiche im laufenden Betrieb

Reihe von Anforderungen erfüllt sein, damit sie erfolgreich ist:

- Sie muss Verbindlichkeit vermitteln und muss daher von der Geschäftsleitung getragen und unterzeichnet sein.
- Die Formulierung der Sicherheitsziele und Strategien sollten knapp und präzise sein.
- Sie muss für alle Mitarbeiter des Unternehmens verständlich sein.
- Sie darf keine widersprüchlichen Aussagen beinhalten und muss konsistent mit anderen Policies im Unternehmen sein.
- Sie muss umsetzbar sein und sich an der Realität im Unternehmen orientieren.
- Sie muss in das Risiko-Management des Unternehmens passen und sich im Hinblick auf investierte Mittel und Ziele daran orientieren.

Hinweise zum Inhalt einer Sicherheitspolitik finden sich vielfältig in der Literatur, z. B. in [Kram02] oder [BSI_GSHB].

2.2 Bedrohungs- und Risikoanalyse

Liegt mit der Sicherheitspolitik die Rahmenvorgabe vor, ist der erste Schritt zur Umsetzung die Bedrohungs- und Risikoanalyse. Es wird eine Bestandsaufnahme aller Informationen durchgeführt und der Schutzbedarf ermittelt. Damit wird festgestellt, in welchen Bereichen ein besonders hoher Schutz erforderlich ist, z. B. weil die Informationen besonders relevant für den Erfolg des Unternehmens sind und deren Verlust oder bekannt werden das Unternehmen gefährden könnten.

Im Anschluss daran wird – auf Basis der existierenden Strukturen und ggf. der schon getroffenen Schutzmaßnahmen – ermittelt, wie hoch das Risiko ist und wo eine Risikosenkung erforderlich ist, um der Sicherheitspolitik zu entsprechen.

Die Risikoanalyse ist der konzeptionell aufwändigste Teil, da er eine komplette Bestandsaufnahme der relevanten Punkte und eine Beurteilung vieler „Einzelrisiken“ erfordert. Daher kann es sinnvoll sein, die Granularität der Risikoanalyse zu beschränken und z. B. nur die besonders kritischen Bereiche im Detail zu analysieren und für alle anderen einige generelle Grundschutzmaßnahmen anzuwenden.

2.3 Erstellung von Sicherheitskonzepten

Auf Basis der Ergebnisse der Risikoanalyse werden Sicherheitskonzepte entwickelt. Sie bestehen aus Maßnahmen, die die in der Risikoanalyse identifizierten Risiken auf ein tolerierbares Maß senken. Ein gutes Sicherheitskonzept beinhaltet eine Kosten-Nutzen-Analyse der verschiedenen Maßnahmen und wählt die unter diesem Blickwinkel wirkungsvollsten Maßnahmen aus. Aus der Kosten-Nutzen-Analyse ergibt sich meist auch eine Priorisierung und damit eine zeitliche Reihenfolge der Umsetzung der Maßnahmen.

Ein gutes, vollständiges und konsistentes Sicherheitskonzept ist die einzige Möglichkeit, eine tatsächliche Kontrolle über die mit der Verarbeitung von Informationen verbundenen Risiken zu erreichen und damit die Grundlage für ein zielorientiertes Management zu schaffen.

Das Sicherheitskonzept legt eine Sicherheitsarchitektur fest, die aus Strukturen und Maßnahmen auf allen Ebenen besteht. Dabei können Maßnahmen übergreifend für alle oder viele Bereiche gültig sein (z. B. die Vorgabe, vertrauliche Dokumente immer einzuschließen), aber auch spezifische für jeden Bereich oder sogar jedes System (z. B. die Vorgabe bestimmter technischer Eigenschaften). Daher ist eine Darstellung der Architektur in baumähnlicher Form hilfreich – hiermit kann man besonders gut erkennen, welche Abhängigkeiten bestehen und, wenn man z. B. zusätzlich eine Statuskennzeichnung einführt, wo Gründe für Verzögerungen liegen (vgl. Abbildung 3). Eine Gliederung kann auf der strategischen Ebene z. B. nach Geschäftsprozessen oder Bereichen erfolgen; in der betrieblichen Ebene wird man bis auf einzelne Systeme untergliedern.

2.4 Umsetzung der Sicherheitsmaßnahmen

Nach Erstellung des Sicherheitskonzepts beginnt die Detailarbeit: Die zahlreichen Maßnahmen müssen umgesetzt werden.

Da dies – abhängig von der Größe und Struktur des Unternehmens – meist nicht von einer Einheit, dem ISM, allein durchgeführt werden kann, sondern die Mitarbeit der Fachabteilungen und der IT-Abteilung erforderlich ist, ist der erste Schritt immer die Verteilung der Verantwortung, also die Klärung der Fragen:

- Wer ist für die Umsetzung der einzelnen Maßnahmen verantwortlich?
- Welche Rahmenbedingungen, Hilfsmittel und Freiräume gibt es dafür?
- Bis wann müssen sie umgesetzt sein?

Festzulegen ist außerdem die Berichtsstruktur: Wer informiert wen über den Status und bei Problemen? Bei der Festlegung ist die Effizienz der Verteilung zu beachten (wenn mehrere Abteilungen das Gleiche tun müssen, ist es sinnvoll, dies nur einmal zu tun und dann zu übertragen), außerdem eine ausreichende, aber nicht hinderliche Kontrolle der Umsetzung und ein kontrolliertes Wachstum (z. B. durch eine angemessene Priorisierung).

Hierdurch wird zum Einen das Sicherheitsniveau kontrolliert und es kann gleichmäßig gesteigert werden und zum Anderen wird verhindert, dass unwichtige Maßnahmen zuerst umgesetzt werden. Es hat sich bewährt, dass die Umsetzung der „lokalen“ Maßnahmen in der Verantwortung der Fachabteilungen oder Bereichsbeauftragten liegt. Da diese die spezifischen Gegebenheiten genau kennen, sollten die Maßnahmen des Sicherheitskonzept möglichst noch nicht die ganz konkrete Umsetzung festlegen, sondern nur den Rahmen abstecken, in dem die Sicherheitsmaßnahmen in lokalen Betriebskonzepten umzusetzen sind.

So wird man z. B. im Sicherheitskonzept eine bestimmte Authentisierungsstärke für ein System festlegen. Die Auswahl des konkreten Produktes jedoch sollte der Fachabteilung überlassen bleiben (ggf. unterstützt durch das ISM, falls dies sinnvoll ist).

Ziel dieser Stufe ist die Umsetzung der Maßnahmen – mindestens bis zu einer bestimmten Priorität – bis zu einem definierten Zeitpunkt, ggf. differenziert nach Bereichen. Dieses Ziel und die Mitwirkungspflicht aller – soweit sie besteht – muss klar kommuniziert sein.

Die Aufgaben des ISM sind neben dem initialen Anstoß und der Aufgabenverteilung die Koordination (Synergien finden und nutzen!), die Lösung von Problemen und eine allgemeine Kontrolle. Das ISM sollte außerdem die Stelle sein, bei der alle Statusinformationen zusammenfließen und die damit immer Auskunft über den Status geben kann. Dabei ist das ISM die Projektleitung „Umsetzung des Sicherheitskonzepts“.

2.5 Awareness: Schulung und Sensibilisierung

Die Maßnahmen zur Schulung und Steigerung der Sensibilität der Mitarbeiter für Belange der Informationssicherheit sind eigentlich Bestandteil der organisatorischen Umsetzung der Sicherheitsmaßnahmen. Andererseits sind sie aber so wichtig und auch klar abgegrenzt, dass sich eine separate Diskussion lohnt.

Der Bereich Awareness hat dabei mehrere Aspekte:

- Informationssicherheit hängt vom Verhalten aller ab.

Insofern müssen alle Mitarbeiter von der Bedeutung der Informationssicherheit und von der Notwendigkeit der eigenen Mitwirkung überzeugt werden. Dies beinhaltet zum Einen Informationstransfer – z. B. durch ein ausführliches Intranetangebot und den Einsatz von E-Learning, durch die Integration relevanter Aspekte in existierende Schulungen. Zum Anderen kann aber auch die Durchführung einer Kampagne für den entsprechenden Bereich sinnvoll sein – mit allen dort üblichen Mitteln (Plakate, Aufkleber, Preisausschreiben etc.), ggf. mit Unterstützung einer Werbeagentur. Diese Art **Sensibilisierung** ist – da sie viele andere Bereiche berührt – eine Querschnittsaufgabe und eine der zentralen Aufgaben des ISM.

- Selbst wenn die grundlegenden Ziele der Informationssicherheit von der Sicherheitspolitik durch die Geschäftsleitung festgelegt sind, muss die Geschäftsleitung selbst und das Management von der Qualität der abgeleiteten Konzeption und der Maßnahmen überzeugt werden und dem damit verbunden personellen und finanziellen Aufwand zustimmen.

Auch hier ist **Überzeugungsarbeit** notwendig – zum Beispiel möglichst praxisnahe Untersuchungen zum Return on Investment (ROI) der angestrebten Maßnahmen. Auch diese Überzeugungsarbeit ist meist eine Aufgabe des ISM.

- Schließlich müssen – im Rahmen der Umsetzung der Maßnahmen – Mitarbeiter in den neuen Prozessen und Techniken geschult werden.

Soweit die Maßnahmen einzelne Fachbereiche betreffen, wird auch die Verantwortung für die **Schulung** dort liegen. Das ISM sollte die Schulungen koordinieren, um Synergien auszunutzen und Schulungen gemeinsam durchzuführen, wenn dies möglich ist.

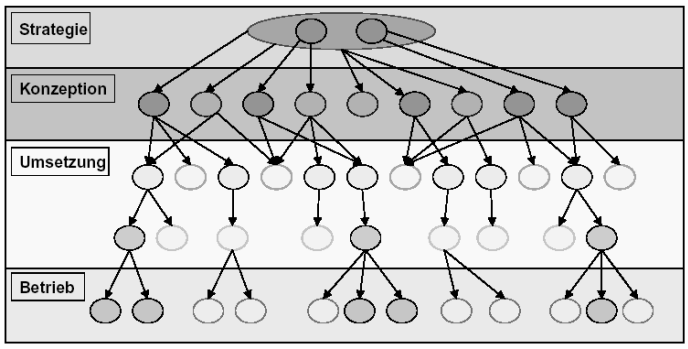

Abbildung 5: Beispiel für eine bestehende Sicherheitsarchitektur
(*dunkel: realisierte Konzepte, Maßnahmen und Systeme, hell: fehlende Teile*)

2.6 Informationssicherheit im laufenden Betrieb

Gehen wir einmal davon aus, dass ein Sicherheitskonzept erstellt und umgesetzt ist. Damit ist das Thema „Information-Security-Management" nicht erledigt, sondern es bleibt eine dynamische Aufgabe – deren Kontrolle und Weiterentwicklung Aufgabe des ISM ist.

Zuallererst müssen die Maßnahmen umgesetzt und beobachtet werden („**Monitoring**") – in der Verantwortlichkeit der Fachabteilungen und operativ Zuständigen. An der **Umsetzung** sind „alle" Mitarbeiter beteiligt, die Koordination und vor allem die „Motivation" liegt jedoch häufig beim ISM.

Trotz aller Maßnahmen werden sich – hoffentlich wenige – sicherheitskritische **Störfälle** nicht vermeiden lassen. Mit solchen Ereignissen muss geeignet umgegangen und es müssen ggf. erforderliche Gegenmaßnahmen ergriffen werden. Die getroffenen Maßnahmen müssen koordiniert und in die Sicherheitsarchitektur integriert werden. Hat sich im Rahmen des Sicherheitskonzepts ergeben, dass die Einrichtung eines speziellen CERTs (Computer Emergency Response Team)[16] sinnvoll ist, könnte dessen Betrieb Aufgabe des ISM sein.

Auch wenn keine Probleme auftreten, muss die Umsetzung der Maßnahmen regelmäßig im Rahmen eines **Audits** überprüft werden. Dabei ist zum Einen das Ziel, sich einschleifende Nachlässigkeiten möglichst rechtzeitig zu bemerken, zum Anderen aber auch, neue Probleme zu erkennen, bevor sie bedrohlich werden. Wichtig dabei ist, das der Auditor in seiner Rolle die Fachabteilungen unterstützt (und nicht bestraft), um eine offene, konstruktive Zusammenarbeit zu fördern. Ob das Audit vom ISM, von der Revision oder von der Fachabteilung durchgeführt wird, ist individuell festzulegen.

Ferner muss im laufenden Betrieb auf Veränderungen im Unternehmen – neue Systeme oder Organsiationseinheiten, Umstrukturierungen – reagiert und die Maßnahmen bzw. Teile des Sicherheitskonzepts angepasst werden (Teil des Change Managements).

Und schließlich ist auch die dem Sicherheitskonzept zu Grunde liegende Risikoanalyse in regelmäßigen Abständen zu aktualisieren. Wurden vielleicht neue Geschäftsprozesse etabliert, die aufgenommen und analysiert werden müssen? Hat sich die Kritikalität der bestehenden Prozesse verändert, z. B. weil ein bestimmtes Produkt für den wirtschaftlichen Erfolg des Unternehmens wichtiger geworden ist? Haben sich neue Risiken ergeben, die in den bisherigen Untersuchungen nicht berücksichtigt wurden? Aufgabe des ISM ist es dabei auch, einen Gesamtüberblick über das mit der Informationsverarbeitung verbundene Risiko zu haben.

Alle diese Änderungen müssen konsistent in allen Teilen der Sicherheitsarchitektur umgesetzt werden („**Change Management**").

3 Aufbau des ISM-Prozesses

In der Praxis ist die Informationsverarbeitung (Systeme, Anwendungen, Komponenten, Prozesse) im Unternehmen häufig über einen langen Zeitraum gewachsen. Der Aspekt der Informationssicherheit wurde dabei oft nur am Rande betrachtet. Daher ist in diesem Bereich mit einem „Wildwuchs"

[16] Zu den Aufgaben von CERTs siehe Fox, Gateway, DuD 8/2002; zur Organisation eines CERT in einem weltweit tätigen Konzern siehe Königshofen, DuD 11/2002.

von Richtlinien, Konzepten, etablierten Maßnahmen und Prozessen zu rechnen.

Möchte man in dieser Situation nachträglich einen Information-Security-Management-Prozess etablieren, so kann man selbstverständlich nicht „bei Null“ anfangen und alle bisherigen Systeme und Prozesse neu aufsetzen. Im Folgenden wird skizziert, wie man schrittweise zum Ziel gelangt.

Zunächst ist es wichtig, dass die Geschäftsführung den Aufbau des ISM unterstützt. Anschließend müssen die **Verantwortlichkeiten** und die **organisatorische Zuordnung** geklärt und die zuständigen Mitarbeiter informiert werden.

Der Information-Security-Management-Prozess orientiert sich an der in Kapitel 2 vorgestellten Vorgehensweise, jedoch wird der Berücksichtigung existierender Komponenten ein größeres Gewicht eingeräumt.

Abbildung 5 veranschaulicht den möglichen Ausgangspunkt, d. h. die bestehende Sicherheitsarchitektur. Dabei repräsentieren die ausgefüllten Kreise existierende Konzepte, Maßnahmen, Handbücher und Systeme, die leeren Kreise deuten fehlende Bestandteile an. Grundsätzlich sollte ein fehlender Baustein auf einer Ebene möglichst nur dann ergänzt werden, wenn der darüber liegende Baustein bereits vorhanden ist. Fehlt dieser ebenfalls, so setzt sich die Ergänzung nach oben hin bis zur Sicherheitspolitik iterativ fort.

Für ein **systematisches Vorgehen** sollte versucht werden, die Lücken Top-Down zu füllen, d. h. zunächst die fehlende Politik und fehlende Konzepte ergänzen und dann die daraus abgeleiteten Maßnahmen realisieren.

Pragmatisch kann man jedoch auch „in der Mitte“ der Architektur, z. B. mit einer fehlenden Maßnahme beginnen und von dort aus zunächst das zugehörige Konzept und ggf. die relevanten Aspekte der Sicherheitspolitik erarbeiten, um die Maßnahme möglichst schnell umsetzen zu können.

Diese Vorgehensweise birgt allerdings die Gefahr, dass

- die Konzepte und die daraus resultierenden Maßnahmen nicht in einer sinnvollen Reihenfolge, d. h. priorisiert nach ihrer Dringlichkeit, umgesetzt werden, sofern zu Beginn keine systematische Bedrohungs- und Risikoanalyse durchgeführt wurde. Dadurch kann es vorkommen, das in Bereichen mit einem hohen Risiko keine Maßnahmen ergriffen werden, während an weniger kritischen Stellen bereits umfassende Maßnahmen umgesetzt werden;
- konkurrierende Konzepte entwickelt werden, die sich nicht unter eine Sicherheitspolitik mit einheitlichem Sicherheitsniveau integrieren lassen;
- man nachträglich Widersprüche auf einem höheren Abstraktionsniveau erkennt und Kompromisse in Kauf nehmen muss, um die bisherigen Bemühungen nicht zu gefährden. Dieses kann langfristig auch höheren Aufwand bedeuten.

Ein Vorteil der pragmatischen Vorgehensweise ist der schnelle Erfolg bei der Umsetzung und der damit (zunächst) verbundene geringere Aufwand. Ferner wird es in einem sich schnell veränderndem Geschäftsumfeld immer wieder vorkommen, dass sich durch verändernde Rahmenbedingungen ständig Änderungsbedarf am Gesamtkonzept ergibt. Hierdurch kann bei einem Top-Down-Ansatz die Umsetzung wichtiger Maßnahmen maßgeblich verzögert oder blockiert werden.

4 Risikoanalyse und Sicherheitskonzept

Im Folgenden werden die Schritte der Risikoanalyse und bei der Erstellung des Sicherheitskonzepts detailliert beschrieben. Der Ablauf unterteilt sich in fünf Stufen (in Anlehnung an [BSI_SiHB]).

Stufe 1: Bestandsaufnahme

- **Erfassen der Geschäftsprozesse (1)**
  In diesem Schritt werden die für das Unternehmen bzw. den Geschäftsbereich relevanten und in die Analyse einzubeziehenden Geschäftsprozesse erfasst. Hier ist ein geeignetes Abstraktionsniveau zu wählen, um einerseits keine wichtigen Prozesse zu übersehen und anderseits den Analyseaufwand einzugrenzen.
- **Erfassen der Anwendungen und der zu verarbeitenden Informationen (2)**
  In diesem Schritt werden die den Geschäftsprozessen zu Grunde liegenden Anwendungen und die dort verarbeiteten Informationen erfasst.
- **Erfassen der bedrohten Objekte (3)**
  In diesem Schritt werden alle von den Anwendungen verwendeten Objekte erfasst, die Ziel eines Angriffs sein könnten. Objekte sind entweder materiell (Hardware, Datenträger, ...), logisch (Software, Daten, Kommunikation, ...) oder Personen.

Stufe 2: Schutzbedarfsfeststellung

- **Bewertung der Geschäftsprozesse (4)**
  In diesem Schritt werden die Geschäftsprozesse anhand relevanter Schadensarten (z. B. finanzielle Schäden, Rufschäden, Vertrauensverlust) hinsichtlich ihrer Schadenshöhe bewertet.
- **Bewertung der Anwendungen und der zu verarbeitenden Informationen (5)**
  In diesem Schritt werden die Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) für die Anwendungen und Informationen festgelegt. Die Bewertung des Schutzbedarfs erfolgt anhand der maximalen Schadenshöhe für die abhängigen Geschäftsprozesse.

Schadenshöhe	Definition
Unbedeutend	Es ist nicht zu erwarten, dass Störungen zu Schäden für das Unternehmen führen
Gering	Selbst mehrere Schäden dieser Art können vom Unternehmen gut verkraftet werden. Erst sehr viele solcher Schäden könnten die Existenz des Unternehmens bedrohen
Mittel	Erst bei mehreren Schäden dieser Größe wird die Existenz des Unternehmens bedroht
Groß	Ein Schaden dieser Höhe bedroht die Existenz des Unternehmens
Katastrophal	Ein Schaden dieser Höhe führt zum Zusammenbruch des Unternehmens

- **Bewertung der Objekte (6)**
  In diesem Schritt wird den Objekten ein Schutzbedarf zugeordnet, der sich aus dem Schutzbedarf der Anwendungen und Informationen ergibt.

Stufe 3: Bestandsaufnahme Maßnahmen (optional)

- **Erfassen der bestehenden Maßnahmen (7)**
  In diesem Schritt werden, soweit bereits vorhanden, bestehende technische und organisatorische Maßnahmen erfasst, die zum Schutz der Anwendungen und verarbeiteten Informationen eingesetzt werden.

Stufe 4: Bedrohungs- und Risikoanalyse

- **Bestimmung der Bedrohungen (8)**
  In diesem Schritt werden alle Bedrohungen bestimmt, die die Objekte gefährden können. Hierbei werden die bestehenden Maßnahmen, die zur Minderung der Bedrohungen dienen können, berücksichtigt.
- **Bestimmung der Schadenswahrscheinlichkeit (9)**

In diesem Schritt wird die Eintrittswahrscheinlichkeit geschätzt, mit der ein Schaden an einem Objekt voraussichtlich eintritt. Hierfür wird eine Häufigkeitstabelle eingesetzt. Diese ist an die Bedürfnisse des Unternehmens bzw. des Geschäftsbereiches anzupassen. Sie könnte z. B. wie folgt definiert werden:

Eintrittswahrscheinlichkeit	Häufigkeit (Beispiel)
Fast sicher	öfter als einmal pro Woche
Wahrscheinlich	öfter als einmal pro Monat
Möglich	öfter als einmal pro Jahr
Selten	öfter als einmal in 10 Jahren
Sehr selten	seltener als einmal in 10 Jahren

- **Bestimmung und Zusammenstellung der aktuellen Risiken (10)**
  In diesem Schritt wird aus Schadenshöhe und Eintrittswahrscheinlichkeit das Risiko abgeleitet. Ferner sollte festgelegt werden, welche Risiken tragbar und welche untragbar sind. (Abb. 6)

Stufe 5: Erstellung des Sicherheitskonzepts

- **Auswahl von Maßnahmen (11)**
  In diesem Schritt werden Maßnahmen ausgewählt, die die Risiken auf ein tragbares Maß verringern sollen. Hierbei werden die bestehenden Maßnahmen – soweit sinnvoll – berücksichtigt.
- **Bewertung der Maßnahmen (12)**
  In diesem Schritt wird untersucht, wie sich die Maßnahmen aufeinander, auf die Risiken, auf die Kosten und auf die operationellen Abläufe auswirken und ob das verbleibende Risiko tragbar ist.
- **Gesamtkosten-Betrachtung (13)**
  In diesem Schritt wird geprüft, ob ein angemessenes Verhältnis zwischen Kosten und Wirkung aller Maßnahmen vorliegt. Aufgrund des Ergebnisses dieses Schritts wird eine Empfehlung für die am besten geeigneten Maßnahmen ausgesprochen.

Zum **Abschluss jeder Stufe** wird das verantwortliche Management über die Ergebnisse informiert, da es diese mittragen muss. Insbesondere muss das Sicherheitskonzept nach der Stufe 5 verabschiedet werden, bevor es umgesetzt werden kann. Abbildung 7 fasst die Schritte graphisch zusammen.

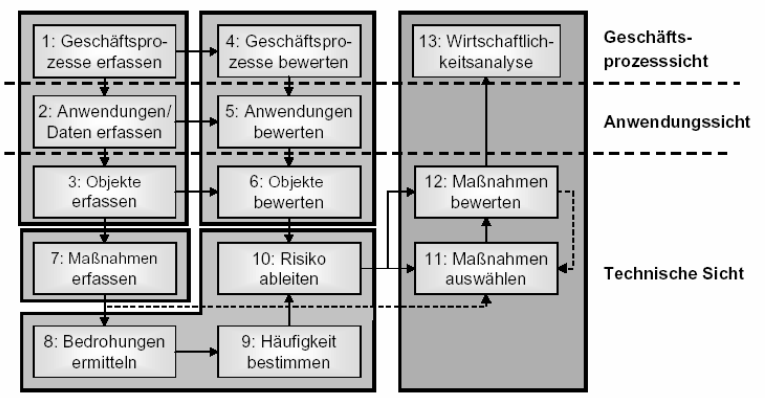

Abbildung 7: Vorgehensweise zur Risikoanalyse und Erstellung des Sicherheitskonzepts

		Schadenshöhe				
		Unbedeutend	Gering	Mäßig	Groß	Katastrophal
Eintrittswahrscheinlichkeit	Fast sicher	Mittel	Bedeutend	Hoch	Hoch	Hoch
	Wahrscheinlich	Gering	Mittel	Bedeutend	Hoch	Hoch
	Möglich	Gering	Mittel	Bedeutend	Hoch	Hoch
	Selten	Gering	Gering	Mittel	Bedeutend	Hoch
	Sehr selten	Gering	Gering	Mittel	Bedeutend	Bedeutend

Abb. 6: Risikomatrix

Referenzen

[BSI_SiHB] BSI, IT Sicherheitshandbuch, BSI 7105, 1992

[BSI_GSHB] BSI, Grundschutzhandbuch, Schriftenreihe zur IT-Sicherheit, Band 3, 2002

[D21_01] Initiative D21, IT-Sicherheitskriterien im Vergleich, Ein Leitfaden der Projektgruppe IT-Sicherheitskriterien und IT-Grundschutz-Zertifikat / Qualifizierung, Stand: 20.12.2001

[ISO 13335] ISO/IEC TR 13335 (1997): Guidelines for the management of IT Security (5 Teile)

[ISO 17799] ISO/IEC 17799 (2000): Code of practice for information security management.

[Kram02] G.Kramarz-von Kohout, Security Policy und Sicherheitsprozess – Ausrichtung und Gestaltung der Sicherheit in einem Unternehmen, DuD 26, (2002), S. 104-106.

[RiNe02] http://www.risknet.de/Risk_ Management/risk_management.html