Friedhelm Chlopek

Wirtschaftliche Aspekte der IT-Sicherheit

Seminararbeit

BuK

IT Companion

Danksagung

Wenn man sich in meinem Alter entschliesst, sein Leben im Grunde neu zu beginnen, dann geht das nicht ohne die Unterstützung von anderen. In meinem Fall möchte ich zunächst und vor allem meiner Frau Lara danken.

Danke an all meine Dozenten, die mir dieses zweite Chance gegeben habe.

Danke auch an die Kommilitonen, die mich als doch deutlich älteren Menschen immer ernst genommen haben und die mir nie das Gefühl gegeben haben, nicht auch einer von Ihnen gewesen zu sein.

„An allem Unfug, der passiert, sind nicht etwa die Schuld, die ihn tun, sondern die, die ihn nicht verhindern."
Erich Kästner

Seminararbeit: Wirtschaftliche Aspekte der IT-Sicherheit

Text: Friedhelm Chlopek

Bildbearbeitung: Friedhelm Chlopek

Lektorat: Lara Maria Laubach

Satz: Friedhelm Chlopek

Friedhelm Chlopek, Jahrgang 1962, nahm 2011 im Alter von 48 Jahren noch einmal sein Studium an der Fachhochschule des Saarlandes imFachbereich Wirtschaftsingenieurwesen auf und beendete es 2012 erfolgreich.
Die vorliegende Seminararbeit wurde im Rahmen des Seminars „Aktuelle Themen der Wirtschaftsinformatik" geschrieben. Das Seminar wurde von Professor Dr. Daniel F. Abawi angeboten. Die Betreuung übernahm Andre Miede

Inhaltsverzeichnis

ZUSAMMENFASSUNG

Der wirtschaftliche Aspekt der IT-Sicherheit hängt von der Größe des Unternehmens ab. Sicherheit ist immer mehr als nur Technik. Zur Berechnung der Vorteilhaftigkeit der Investitionen werden die dynamischen Verfahren der Investitions-rechnung angewandt. Die Kontrolle erfolgt über die Techniken des Controllings. Man sollte IT-Sicherheit nicht outsourcen.

1. Einleitung

Dipl.- Wirtsch.-Ing. Georg Schütz, der an der HTW das Wahlpflichtfach Datenbankprogrammierung im Fachbereich Wirtschaftsingenieurwesen hält, hat eingangs seiner Vorlesung (Wintersemester 2011/12) ein sehr schönes Bild der Programmierung gezeichnet, wie sie normalerweise von Laien gesehen wird. Er benutze das Bild eines Eisberges, von man nur die Spitze sieht und nicht das wahre Ausmaß, das im übertragenen Sinne hinter der Arbeit und der Pflege einer Datenbank steht.

Dass wir die IT-Sicherheit brauchen, hat sich erst langsam und im Laufe der letzten Jahre durchgesetzt. In dieser Seminararbeit möchte ich versuchen, die IT-Sicherheit unter dem wirtschaftlichen Aspekt zu beleuchten.

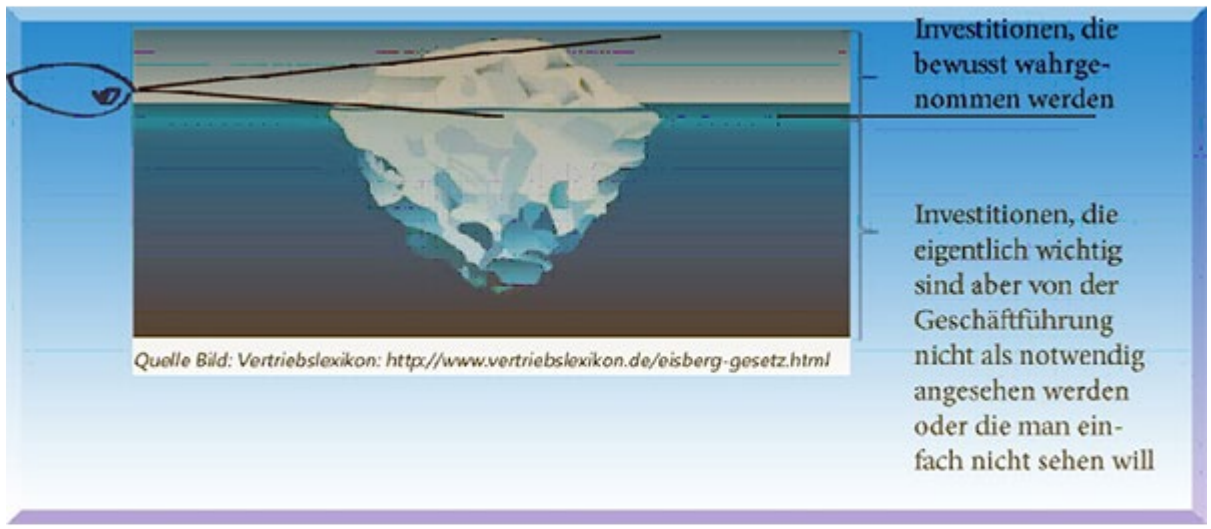

Abb. 1 Wahrnehmung der Kosten

1.1. Eingrenzung des Themas

Wenn man sich dem Thema „Wirtschaftliche Aspekte der IT - Sicherheit" nähert, dann stellt sich zwangsläufig die Frage, von welcher Sicherheit hier eigentlich die Rede sein soll. Sprechen wir von der Sicherheit, die gegen Angriffe von außen schützen soll? Oder geht es darum, die innere Sicherheit zu gewährleisten? Was soll geschützt werden? Ein Produkt? Ein Unternehmen? Aus diesen Fragestellungen ergeben sich schließlich die wirtschaftlichen Aspekte der IT-Sicherheit.

Ich möchte an dieser Stelle auf die BSI Lageberichte „Die Lage der IT-Sicherheit in Deutschland 2009" und „Die Lage der IT-Sicherheit in Deutschland 2011" hinweisen. Ich werde ihn an einigen Stellen dieser Arbeit zitieren. Im Bericht wird deutlich gemacht, „dass die aktuellen Gefährdungen wie Cyber-Angriffe, Angriffe auf mobile Endgeräte und Attacken, die auch außerhalb der klassischen IT greifen, eine Herausforderung für Politik, Wirtschaft und Gesellschaft bedeuten." [1]

Das Thema wird insofern eingegrenzt, als das ich im Folgenden über die IT-Sicherheit in Unternehmen schreibe werde. Zunächst werde ich unter dem Aspekt der IT-Sicherheit auf die Organisationsstrukturen und Unternehmensgrößen eingehen. Anschließend möchte ich die Gefahren bzw. Risiken benennen, die heute bekannt sind. Die Bewertung und die Steuerung der Gefahren werde

1 BSI Lagebericht 2011, https://www.bsi.bund.de/DE/Publikationen/publikationen_node.html

ich anschließend thematisieren. Im letzten Kapitel soll der wirtschaftliche Aspekt der IT-Sicherheit in einem Fazit zusammengefasst werden.

Wesentliche Informationen zum Thema IT-Sicherheit liefert das IT-Grundschutzhandbuch. Es beschreibt die Standardsicherheitsmaßnahmen für IT-Systeme. Im Fokus stehen die Infrastruktur, die Organisation, das Personal und die Technik. Darüber hinaus beschreibt es die sogenannte Notfallversorgung.

Ich selbst habe ein Unternehmen, die Basso & Kuster GmbH, als geschäftsführender Gesellschafter aufgebaut und über lange Jahre geleitet. Das in dieser Arbeit verwendet Beispiel entspricht dem, was damals tatsächlich geschehen ist. Insofern habe ich auch versucht, meine eigenen Erfahrungen zu diesem Thema in diese Arbeit einfließen zu lassen.

Die Grafiken wurden von mir selbst bearbeitet. Dafür habe ich die Programme der Adobe Creative Suite sowie den Open Source yEd Graph Editor genutzt.

Zum Schluss der Einleitung: Aus stilistischen Gründen verwende ich bei der Beschreibung von Personen die männliche Form. Gemeint sind damit aber stets Frauen und Männer.

2. ORGANISATIONSSTRUKTUREN FÜR DEN IT-BEREICH

2.1.Anwendung des IT-Grundschutzhandbuches.

Die Anwendung des IT-Grundschutzhandbuches findet in vier verschiedenen Schritten statt. Zunächst einmal geht es darum, überhaupt ein IT-Sicherheitssystem einzurichten. Diese sogenannte Initiierung umfasst das Einrichten eines IT-Sicherheitsmanagement und das Erstellen einer IT-Sicherheitsleitlinie für das Unternehmen.

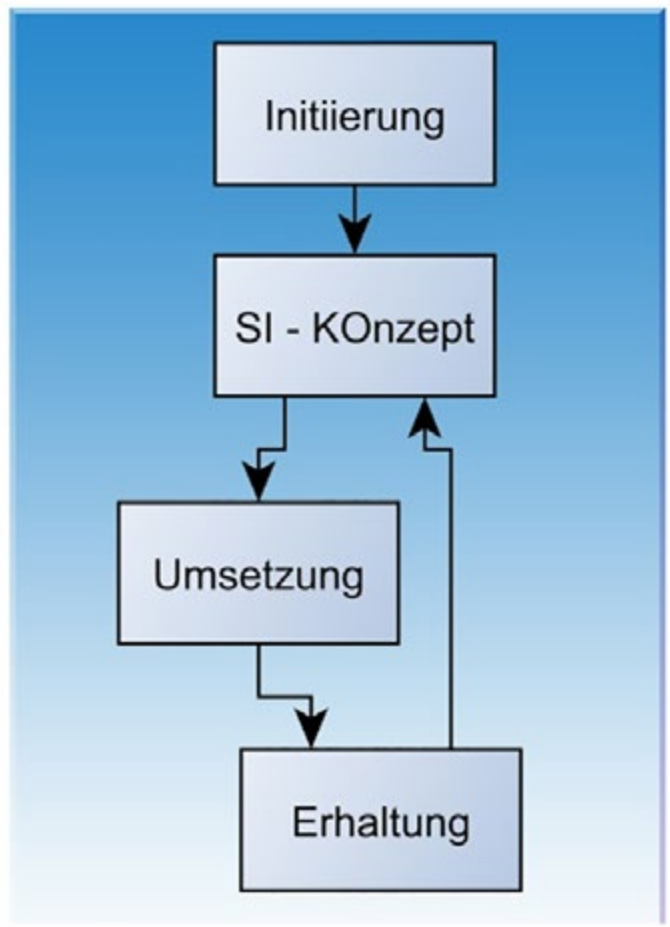

Abb. 2: „Ablauf zur Erstellung von SI-Konzepten" nach Prof. Dr.-Ing. Hannes Federrath Vorlesungsskript „Wie viel darf IT-Sicherheit kosten?", Seite 9.

Der Initiierung folgt das IT-Sicherheitskonzept. Das IT-Sicherheitskonzept sollte aus der IT-Strukturanalyse, der Schutzbedarfsaufstellung, der IT-Grundschutzanalyse (die durch eine Sicherheitsanalyse ergänzt werden kann) sowie einem Realisierungsplan bestehen. Im Realisierungsplan werden die Fragen nach den Verantwortlichkeiten, der Priorität der Maßnahmen, den Zeitpunkten, wann diese Maßnahmen beginnen und enden sollen sowie die Frage nach den zu Verfügung stehenden Ressourcen beantwortet. Zu den begleitenden Maßnahmen zählen die Schulungskonzepte sowie die Sensibilisierung der Mitarbeiter.

Die Umsetzung selbst beinhaltet schließlich die Gestaltung von technischen und organisatorischen Abläufen an den Arbeitsplätzen, das Anpassen der Aufgabenbeschreibungen sowie die Bereitstellung von Informationen für Schulungen und von Hilfsmitteln.

Im letzten Punkt, der Erhaltung, wird durch regelmäßige Prüfungen versucht, die oben beschriebenen Aufgaben auf ihre Richtigkeit und Aktualität hin zu prüfen. Die Aufrechterhaltung eines sicheren Betriebes erfordert einen Sicherungsprozess, der gegebenenfalls an aktuelle Geschehnisse angepasst bzw. korrigiert werden kann.

2.2. Organisationssystem

Um die Strukturen eine Organisation näher zu erläutern, ist es zunächst wichtig, eine Definition des Organisationssystems zu benennen, um dadurch eine Ableitung auf die Organisationstrukturen zu bekommen.

„Ein System ist eine gegenüber der Umwelt abgegrenzte Gesamtheit von Elementen, die durch Beziehungen untereinander verknüpft sind. Die Elemente (Stellen/Personen) sind also Teil des Systems, sie sind miteinander mehr oder minder eng verbunden. Einige Elemente unterhalten auch

Beziehungen zu externen Elementen (Umwelt wie Lieferanten, Kunden, Kapitalgeber etc.). Eng miteinander verbundene Elemente bilden Subsysteme (z.B. Abteilungen), die mit anderen Subsystemen innerhalb der Organisation Kontakt halten. Geschlossene Systeme verwehren Außenstehenden den Zutritt, offene Systeme gewähren ihn. Unternehmen als Spezialfall der Organisation sind zweckorientierte, offene, dynamische, soziotechnische Systeme, sie wandeln Inputs (Einsatzfaktoren) in Outputs um, wofür sie vom Markt honoriert werden, was ihre Lebensfähigkeit erhält." [1]

Die klassische Einteilung eines Unternehmens in die verschiedenen Verantwortungsebenen mit Hilfe eines Organigramms hat sich mittlerweile überall durchgesetzt.

Abb. 3: Beispiel eines Organigramms von Unternehmen

1 Wirtschaftslexikon 24net. http://www.wirtschaftslexikon24.com/d/organisationssystem/organisationssystem.htm

Am Beispiel des Organigramms von Abb.3 leiten wir nun die verschiedenen Ebenen ab, die wir zur Betrachtung unserer Organisationsstruktur hinsichtlich der IT-Sicherheit heranziehen wollen:

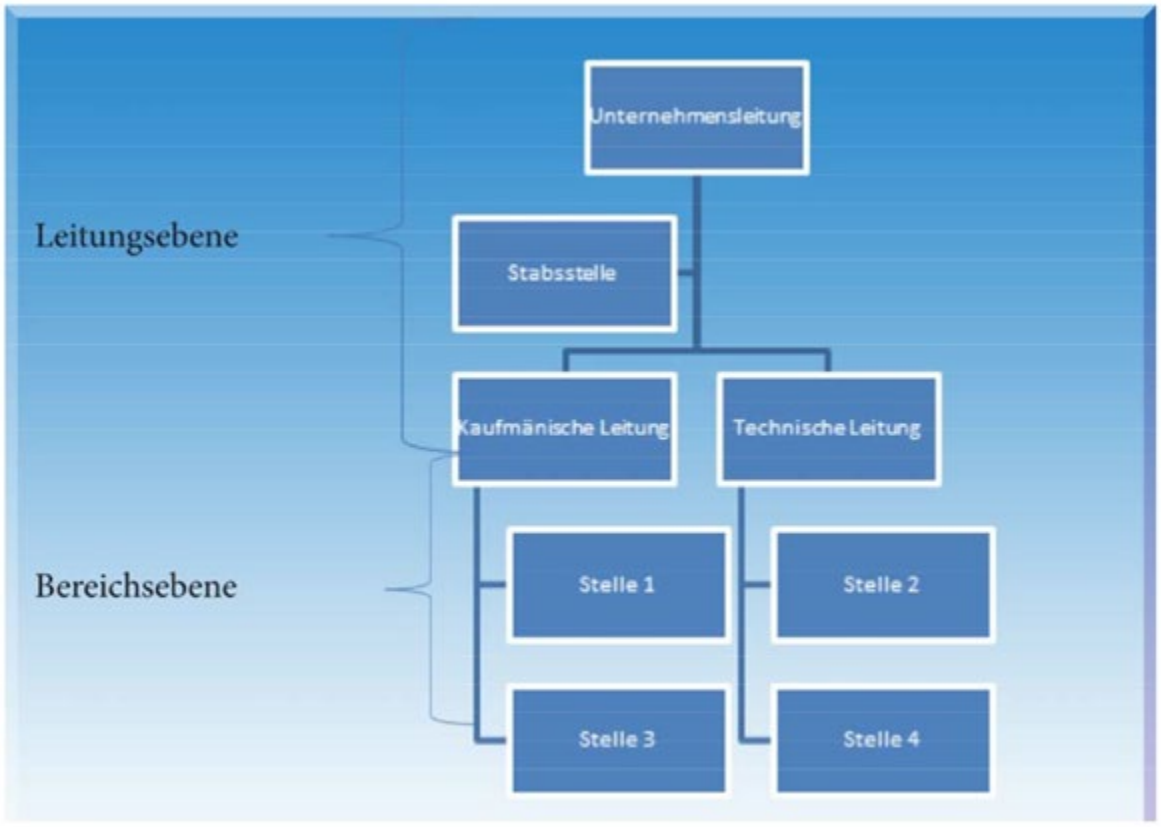

Abb. 4: Beispiel Organigramm mit den entsprechenden Ebenen

Wenn wir nun den Stellen auf der Bereichsebene Projekte zuordnen, haben wir auch die letzte Ebene, die wir für die nun folgende Betrachtung brauchen, die Projektebene.

3. INITIIERUNG

Betrachtet man die Organisationsstruktur für die IT-Sicherheit bei kleinen, mittleren und großen Unternehmen, wird deutlich: Je größer ein Unternehmen, desto größer ist der absolute Wert des finanziellen Budgets für die IT-Sicherheit.

3.1. Kleine Organisationen.

Um eine Größe für kleine Unternehmen festlegen, möchte ich aus dem Skript von Prof. Dr. Heimo H. Adelsberger von der Universität Duisburg /Essen zitieren: „Das Produkt SAP Business One wird von SAP als ERP-Lösung für kleine Unternehmen mit weniger als 100 Mitarbeitern und 30 Nutzern empfohlen. Durch Business One werden die Kernprozesse des Unternehmens, z. B. Finanzwesen, Kundenbetreuung und Vertrieb abgedeckt.“ [1]

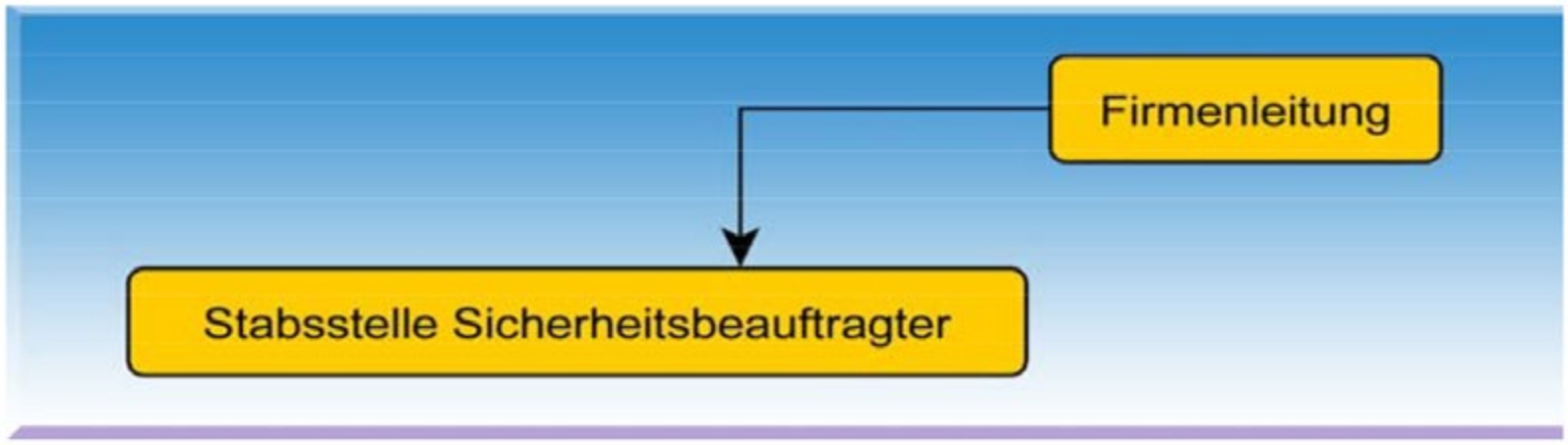

Abb. 5: Organisationsstruktur für IT-Sicherheit in kleinen Unternehmen

Wenn wir uns den Kreislauf für die Umsetzung und ständige Verbesserung von IT-Sicherheitskonzepten anschauen, haben wir in kleinen Unternehmen im Idealfall kleine und schnelle Strukturen. Das bedeutet natürlich auch, dass wir unter dem absoluten Kostengesichtspunkt nicht so hohe Kosten haben wie beispielsweise mittlere und große Unternehmen.

3.2. Mittlere Organisationen

„Das Produkt Business ByDesign wurde von SAP für kleine und mittelständische Unternehmen mit 100-500 Mitarbeitern entworfen. Es handelt sich um eine On-Demand-Lösung insbesondere für Unternehmen, die bisher keine integrierte Geschäftssoftware einsetzen.“ [2]

---

1 Prof. Dr. H.H. Adelsberger, Skript „Einführung in die ABAP“, S. 12

2 Prof. Dr. H.H. Adelsberger, Skript „Einführung in die ABAP“, S. 13.

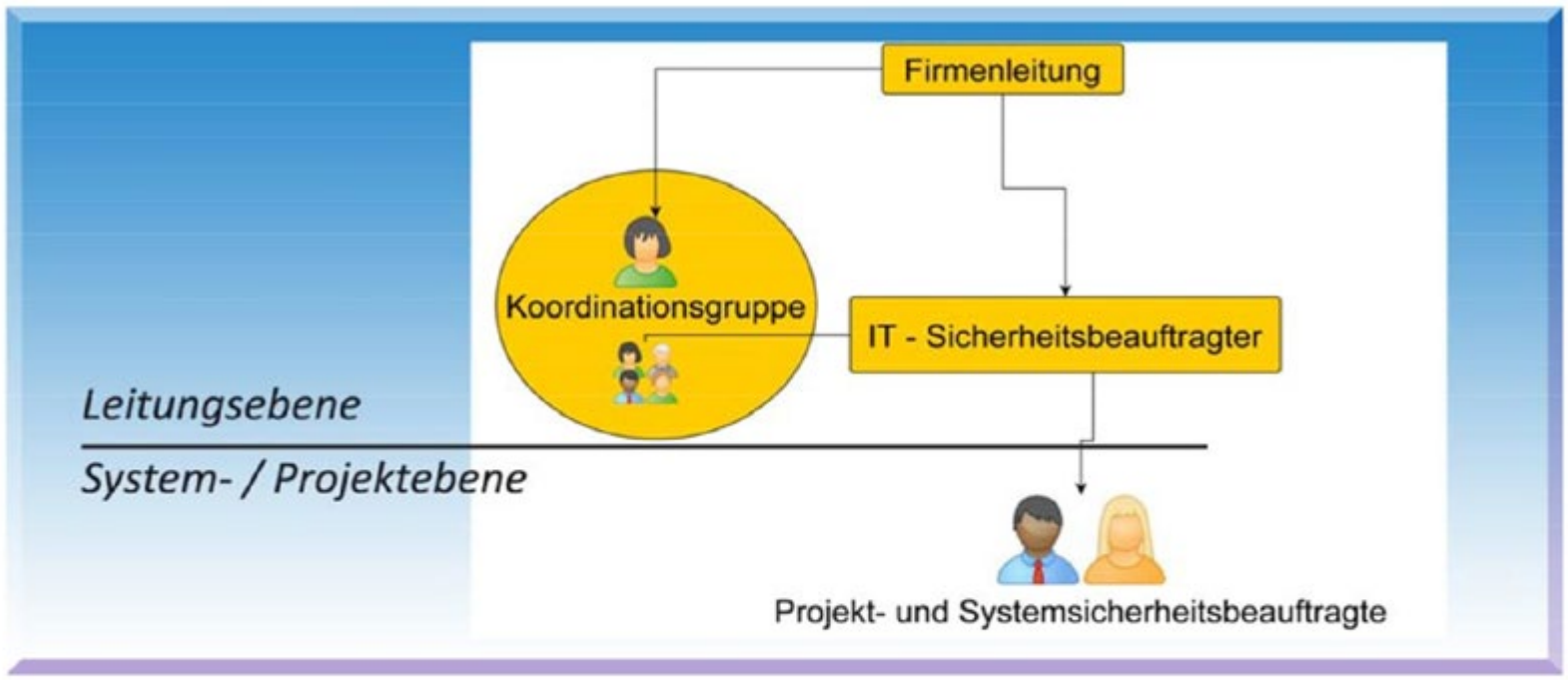

Abb. 6: Grafik „Organisationsstruktur für IT-Sicherheit: Mittlere Organisationen“ nach Prof. Dr.-Ing. Hannes Federrath, Vorlesungsskript „Wie viel darf IT-Sicherheit kosten?“, S. 10.

Während kleinen Unternehmen in aller Regel eine flache Struktur zugrunde liegt, findet bei mittelständigen Unternehmen eine Einteilung in Leitungsebene und System-/Projektebene statt. Innerhalb der Leitungsebene wird in aller Regel neben dem IT-Sicherheitsbeauftragten eine Koordinationsgruppe installiert, der in besten Fall der Firmenleitung vorsitzt. Über den IT-Sicherheitsbeauftragten werden die Aufgaben und Projekte dann an die Projekt- und Systemsicherheitsbeauftragten verteilt.

3.3. Große Organisationen

Nach den oben zitierten Zuordnungen von Professor Dr. Adelsberger spricht man ab einer Größe von 500 Mitarbeitern von einem großen Unternehmen.

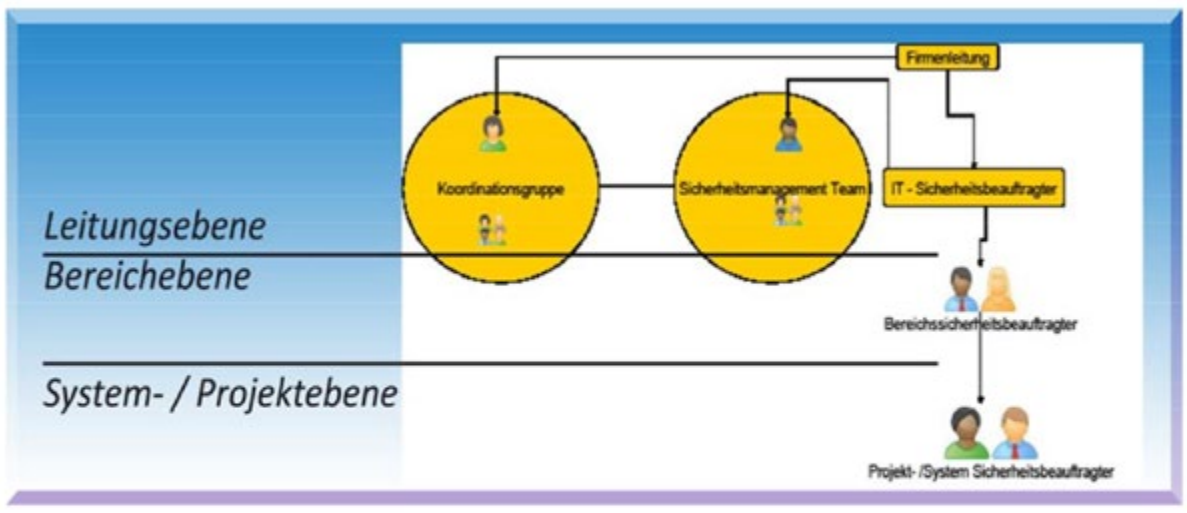

Abb. 7: Grafik „Organisationsstruktur für IT-Sicherheit: Große Organisationen“ nach Prof. Dr.-Ing. Hannes Federrath, Vorlesungsskript „Wie viel darf IT-Sicherheit kosten?“, S. 11.

In Bezug auf die Organisation der IT-Sicherheit ergibt sich hier folgender Unterschied zu mittleren Unternehmen: Auf der Leitungsebene wird zwischen der Koordinationsgruppe und dem IT-Sicherheitsbeauftragten ein Sicherheitsmanagement-Team eingesetzt. Außerdem wird unter der Leitungsebene zunächst auf Bereichsebene ein Bereichssicherheitsbeauftragter eingesetzt, d.h. erst anschließend folgt der Verantwortungsbereich der Projekt/-System-Sicherheitsbeauftragten.

3.4. Ein erstes Fazit unter wirtschaftlichen Aspekten

Was zu erwarten war ist, dass mit der Größe des Unternehmens auch die Höhe der Kosten für die IT-Sicherheit steigt. Dabei sollten wir beachten, dass es sehr darauf ankommt, wie das Geld ausgegeben wird. Nicht jede Maßnahme, die gemacht werden könnte, ist sinnvoll. Beispielsweise macht die Einführung eines Sicherheitsmanagement, wie wir es bei großen Unternehmen und Organisationen dargestellt haben, bei kleinen und mittelständigen Unternehmen allein schon aus Kostengründen keinen Sinn.

Dieser Logik folgend kommen wir zu einer möglichen allgemeinen Antwort, nämlich der Betrachtung der Grenzkosten:

Natürlich müssen wir diese theoretische Betrachtungsweise kritisch hinterfragen. Was ist eigentlich der Nutzen einer konkreten Maßnahme innerhalb eines IT-Sicherheitskonzeptes? Kann man den Nutzen bewerten und wenn ja wie? Daraus folgt zwangsläufig die Frage nach den Kosten und deren Zusammensetzung. Wir kommen hier zwangsläufig zum Risikomanagement-Ansatz auf der operativen Ebene.

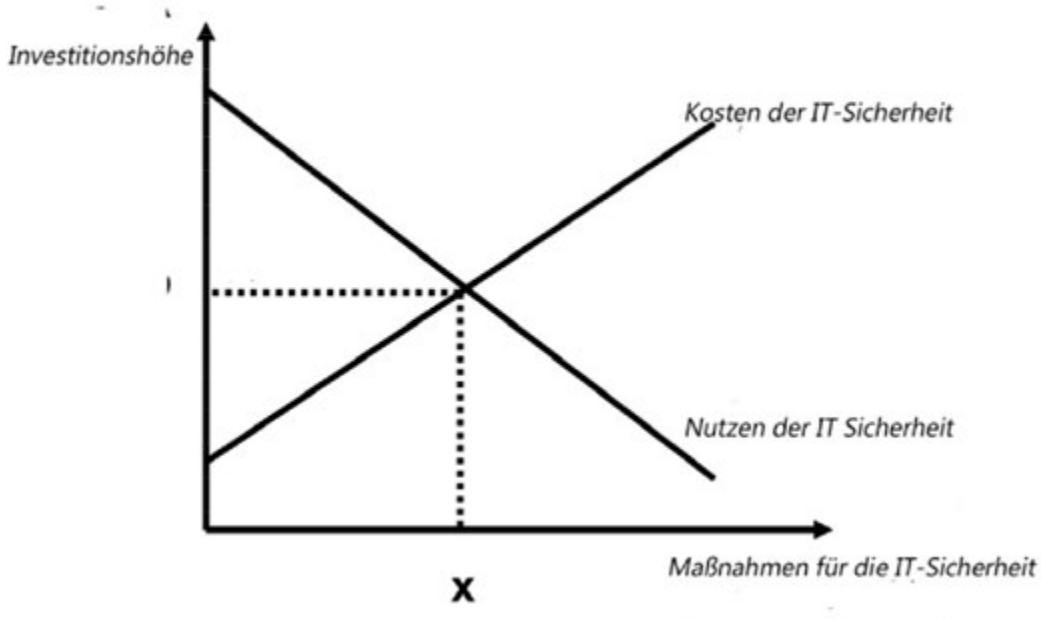

Abb. 8: Betrachtung der Kosten-Nutzenfunktion im Hinblick auf die Grenzkosten

4. BETRACHTUNG DES RISIKOMANAGEMENT-KREISLAUFES

Auf der operativen Ebene gilt es, Strategien festzulegen. Als ein Beispiel wird die Frage nach vorgefertigten oder individuellen Lösungen aufgezeigt und erörtert:

Am Anfang der Überlegung sollte die Frage nach den Human-Ressourcen im IT-Bereich stehen. Mitarbeiter, die ein Sicherheitskonzept erarbeiten, die das Konzept an die sich laufend veränderten Situationen am Markt anpassen, die aber auch die Befindlichkeiten innerhalb des Unternehmens kennen, sind in aller Regel flexibler und besser, aber eben auch teurer als vorgefertigte Lösungen. Da Sicherheit von Anfang an integraler Bestandteil der Prozesse und Arbeitsabläufe sein sollte, baut sich das Unternehmen auf lange Sicht mit einem solchen Stamm wertvolles Knowhow auf. In aller Regel ist es teurer, nachträglich Sicherheitsprozesse in laufende Unternehmensprozesse „hinein zu basteln" als diese von Anfang an zu integrieren und mitwachsen zu lassen. Wie wichtig IT-Sicherheits-Knowhow ist, möchte ich mit folgendem Zitat aus „Die Lage der IT-Sicherheit in Deutschland 2011" noch einmal deutlich machen: „Die Methoden werden immer raffinierter, und die Abwehr von Angriffen erfordert einen immer höheren Aufwand. So griff etwa das Trojanische Pferd „Stuxnet" gezielt Prozesssteuerungssysteme an. Die Art und Weise, mit der seine Programmierung erfolgte, erfordert einen sehr hohen Aufwand und hochspezialisiertes Wissen auf Seiten der Angreifer." [1]

Die Frage, wonach überhaupt gesucht werden soll und wie das Gefundene bewertet werden soll, führt uns zu dem Risikomanagement-Kreislauf:

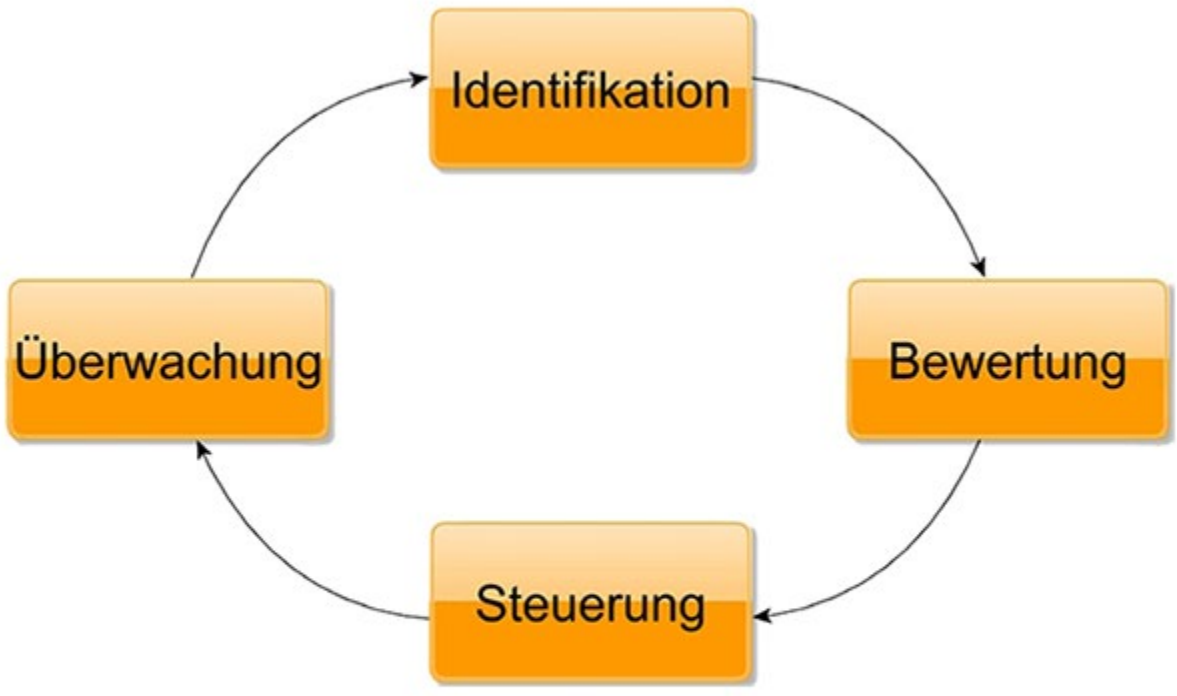

Abb. 9: Risikomanagement-Kreislauf in Anlehnung an Prof. Dr.-Ing. Hannes Federrath, Vorlesungsskript „Wie viel darf IT-Sicherheit kosten?", S. 18.

1 Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland 2011", S. 4.

4.1. Identifikation

An dieser Stelle seien zwei Begriffe aufgenommen, die der Abgrenzung dieses Unterpunktes dienen. Bedrohungen, die von innen kommen, fasst man unter dem Begriff der White Box zusammen, Bedrohungen von außen werden unter dem Begriff der Black Box gesammelt. Ich werde mich im Folgenden nur mit den Bedrohungen von außen, also der Black Box, beschäftigen.

- Sicherheitslücken

  Manchmal kommen Unternehmen wie Microsoft oder Adobe in die Nachrichten und sind für diese „Werbung" nicht dankbar. Nämlich immer dann, wenn mal wieder eine Sicherheitslücke im Programm entdeckt wurde. In aller Regel bieten die Unternehmen dann schnell Updates an, um diese Lücken zu schließen. Was viele User nicht wissen: „Für rund die Hälfte der neu gemeldeten Schwachstellen wurde von den Herstellern der Produkte kein Update zur Behebung des Sicherheitsproblems bereitgestellt." [2]

- Schadprogramme

  Zu den Schadprogrammen zählen Viren, Würmer, Trojanischer Pferde und Bots (Es gibt gutartige und bösartige Bots oder Roboter-Programme. Bösartige Bots sammeln E-Mailadressen zum Aussenden von Werbemails oder spionieren systematisch Sicherheitslücken in Servern aus).

- DoS – Angriffe

  Denial-of-Service-Angriff. Es handelt sich hierbei um den Versuch, die Verfügbarkeit von IT-System nachhaltig zu stören. Viele verteilte (disributed) Clientsysteme erzeugen eine Lastsituation, bei der IT-Systeme effektiv blockiert werden.

- Unerwünschte E – Mails

  Das Spam Aufkommen ist laut den Zahlen des Bundesamtes für Sicherheit in den letzten Jahren erheblich gestiegen. Man versucht mit Hilfe von Anti-Spam-Methoden, die Flut der Spam-Mails eizudämmen.

- Bot-Netze

  Bei Bot-Netzen handelt es sich um ein Netz von PCs, die über Sicherheitslücken mit bösartigen Bots infiziert wurden. Sie dienen beispielsweise als Ablagestelle für illegale Software aber auch zum massenhaften Versand von E-Mails mit bösartigen Anhängen.

- Identitätsdiebstahl

  Hier wird versucht, von einer Person persönliche Daten zu stehlen und diese missbräuchlich zu nutzen. Die klassischen Phishing Mails locken Nutzer auf gefälschte Webseiten von Banken, um so an Passwörter, PINS und TANS zu kommen.

- Betrügerische Webangebote

  Hier werden Dialer (oder deutsch: Einwahlprogramme) installiert, die dann über teure Rufnummern Internetverbindungen herstellen.

- Kompromittierende Abstrahlung

  IT- Geräte strahlen elektromagnetische Störstrahlungen aus. Hierbei können auch die gerade verarbeiteten Informationen des Gerätes transportiert werden. Durch Empfangen und Auswerten dieser Daten aus einiger Entfernung können diese Informationen mitgelesen werden. Die Vertraulichkeit der Daten ist somit nicht mehr gewährleistet.

Die hier aufgezählten Bedrohungen sind nur oberflächlich beschrieben. Die Gefahren im Netz nehmen zu und werden zukünftig Unternehmen und Organisationen vor immer größere Herausforderungen stellen. Ein Beispiel, die Verbreitung von durch Bots verschickten E-Mails zu verhindern,

2 Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland 2009", S. 19.

nennt Rainer Hattenhauer in seinem Buch „Digital Survival Guide 2010“: „Die Registrierungsprozeduren der meisten Forenbetreiber setzen das Erkennen sogenannter Captchas voraus. Das sind kleine stilisierte Grafiken, die aus verzerrten Ziffern und Buchstaben bestehen, um Roboterprogramme (kurz: Bots), die Spam-Mails verschicken, den Zutritt zu den Foren zu versperren.“ [3]

4.2. Die Bewertung von Risiken

Die Kernfrage bei der Bewertung von Risiken nach Prof. Dr.-Ing. H. Federrath ist die, wie groß die Eintrittswahrscheinlichkeit eines potentiellen Schadensereignisses ist. In Abbildung 10 sehen wir die Einteilung von hoch bis niedrig für die Schadenshöhe und die Schadenswahrscheinlichkeit.

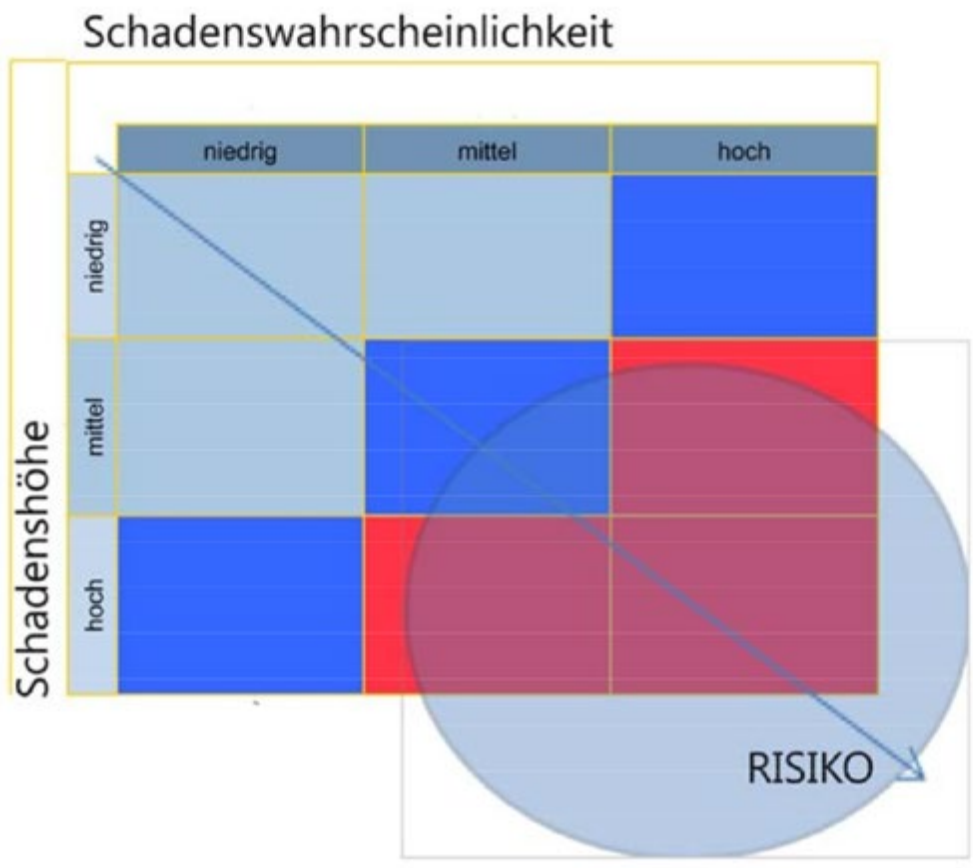

Abb. 10: Grafik zur Bewertung von Risiken in Anlehnung an Prof. Dr.-Ing. Hannes Federrath, Vorlesungsskript „Wie viel darf IT-Sicherheit kosten?“, S. 20.

3 R. Hattenhauer, Digital Survival Guide 2010, Seite 29.

Die Methoden und Werkzeuge zum Abarbeiten der Risiken sind vielfältig. In der Vorlesung von Dr. Otto Schmitt „Betriebliches Umweltmanagement" im Fachbereich Wirtschaftsingenieurwesen an der HTW des Saarlandes im WS 2011/12 wurde beispielsweise auf die ISO 9001 eingegangen. Es ging dabei um die systematische Behandlung von Risiken, die in folgenden Schritten ablaufen sollte:

- Risikoanalyse,
- Risikobewertung,
- Risikominimierung,
- Risikokontrolle,
- Risikoverfolgung.

Weitere Methoden und Werkzeuge zur Bewertung von Risiken sind: [4]

- Qualitative Bewertung
- Quantitative Bewertung
- Spieltheorie
- Maximalwirkungsanalyse

Als Entscheidungshilfen bei der Bewertung werden Antworten auf folgende Fragen gesucht:

- Welche Vermögenswerte und Gegenstände sollen eigentlich geschützt werden?
- Wer ist der strategische Angreifer?
- Welche Beziehungen bestehen zwischen den einzelnen Bedrohungen?
- Wie ist das alles zu bewerten?

Die Bewertung von Risiken sowie deren Steuerung und Überwachung soll an folgendem Beispiel aus der Praxis gezeigt werden:

Die Basso & Kuster GmbH, eine Ton- und Musikproduktion aus Saarbrücken, hatte sich als Dienstleister für die werbetreibende Wirtschaft über Jahre innerhalb Deutschlands einen Namen gemacht. In der Hauptsache produzierte das Unternehmen Musik. Im Gegensatz zu Zeiten von Wagner wurden diese Stücke nicht mehr notiert, also als Noten zu Papier gebracht, sondern waren als Bits und Bytes auf dem firmeneigenen Server abgelegt. Hier gab es nun auch viele unveröffentlichte Stücke. Der Wert dieser Stücke war im Grunde deswegen nicht zu beziffern, als das der Wert eines Musikstückes erst nach der Veröffentlichung durch den Erfolg quantifizierbar wird. So hatte beispielsweise das Stück, dass das Unternehmen für die Zapf Creation AG für das Produkt Baby Born geschrieben hatte und das weltweit zum Einsatz kam, in einem Jahr allein in den USA einen großen, sechsstelligen Gema-Betrag eingespielt. Die Bewertung eines Angriffes von außen, also die Schadenswahrscheinlichkeit, wurde vom IT-Sicherheitsbeauftragen als mittel eingestuft, die dann eintretende Schadenshöhe als hoch. Natürlich war der Server des Unternehmens durch Angriffe von außen geschützt. Allerdings ging es im konkreten Fall der nicht veröffentlichten Musikstücke nicht allein darum, dass die Stücke nicht gestohlen werden sollten sondern vielmehr auch darum, was im Falle einer nicht durch das Unternehmen autorisierten Veröffentlichung geschehen sollte. Es ging präzise um die Frage, wie in einem solchen Fall rechtlich der eindeutige Nachweis der Urheberschaft geführt werden kann. Hier ist man dazu übergegangen, Datensicherungen in

4 Prof. Dr.-Ing.H.. Federrath, Skript „Wie viel darf IT-Sicherheit kosten?", S. 20.

regelmäßigen Abständen einem Notar zu übergeben, die dieser beglaubigte, versiegelte und in seinen Tresor ablegte. Der Zeitpunkt der „internen" Veröffentlichung wurde sozusagen vorverlegt; bis zur der internen Veröffentlichung wurden die Daten nicht auf dem Server abgelegt.

4.3. Die Steuerung von Risiken

Wie aus eben aufgezeigten Beispiel ersichtlich ist, geht es bei der Steuerung von Risiken zunächst einmal darum, die möglichen Risiken zu bewerten. Erst wenn diese Bewertung abgeschlossen ist, kann mit der Steuerung der Risiken begonnen werden. Dabei steht die Frage im Vordergrund, welche Risiken wie behandelt werden können. Ein Risiko, dessen Schadenshöhe und Eintrittswahrscheinlichkeit niedrig ist, wird in der Steuerung anders behandelt als eine Bewertung hoch/hoch. Das im letzten Punkt genannte Unternehmen sammelte beispielsweise Daten, um diese für die Akquisition von Kunden zu nutzen. Die Schadenshöhe und die Schadenswahrscheinlichkeit wurden hier als niedrig bewertete. Innerhalb der Steuerung reichten also die normalen Schutzmechanismen des Servers aus, um diese Daten zu schützen.

Als Hilfsmittel zur Steuerung haben sich nach Prof. Dr.-Ing. Hannes Federrath Methoden aus der Investitionsrechnung und der Entscheidungstheorie durchgesetzt. Hier sind folgende Methoden zu nennen:

- Investitionsrechnung
  Die Kapitalwertmethode (NPV [(englisch für Net Present Value))
  Die Methode des internen Zinsfußes (IRR (englisch für Internal Rate of Return))
- Entscheidungstheorie
  AHP (englisch für Analytic Hierarchy Process). Hier werden Kriterien und Alternativen dargestellt. Die Ergebnisse werden bewertet und verglichen, um die optimale Lösung zu finden.

Im Folgenden möchte ich kurz auf die Methoden der Investitionsrechnung eingehen. Hierbei nutze ich das Skript von Prof. Dr. rer. oec. Andy Junker, der im Wintersemester 2011/12 die Vorlesung „Investition" im Fachbereich Wirtschaftsingenieurwesen an der HTW des Saarlandes hält.

Bei der Investition geht es vorrangig darum, dass man zwischen mindestens zwei Möglichkeiten einer Investition entscheiden kann. Grundlagen dafür sind verschiedenen Verfahren. Man unterscheidet statische und dynamische Verfahren. Die hier zu betrachtende Kapitalwertmethode und die Methode des internen Zinsfußes zählen zu den dynamischen Verfahren. Prof. Dr. Junker betonte in seiner Vorlesung immer wieder den exakteren und genaueren Wert der dynamischen Verfahren.

Mit der Kapitalwertmethode beurteilen wir die Sinnhaftigkeit einer Erweiterungsinvestition. Die Formel lautet [5]

$$C_0 = -A_0 + \sum_{t=1}^{n} EZ\ddot{U} * (1+i)^{-t} + Ln * (1+i)^{-n}$$

mit

- C0: Kapitalwert
- A: Investition
- n: Betrachtungsdauer (in Perioden)
- EZÜ: Rückfluss in Periode t
- Ln: Liquidationserlös/Resterlös
- i: Kalkulationszinssatz

C0 =0 bedeutet, die EZÜ der Investition reichen aus, die Anschaffungsauszahlung zu tilgen und die Verzinsung zum Kalkulationszins zu gewährleisten.

C0 = 0 bedeutet damit, dass die Investition vorteilhaft ist.

Mit der internen Zinsfußmethode können wir berechnen, ob eine Investition oder Kapitalanlage bei unregelmäßigen Erträgen eine mittlere Rendite erbringt.

5 Prof. Dr. A. Junker, Vorlesungsskript „Investition“, S. 72.

Allen Methoden ist gemein, dass wir aus mehreren Möglichkeiten der Investition versuchen, die Beste zu ermitteln.

Grundsätzlich sollte man festhalten, dass innerhalb unseres Risikomanagement Kreislaufes die Daten für die Steuerung aus dem vorangegangenen Schritt der Bewertungen kommen.

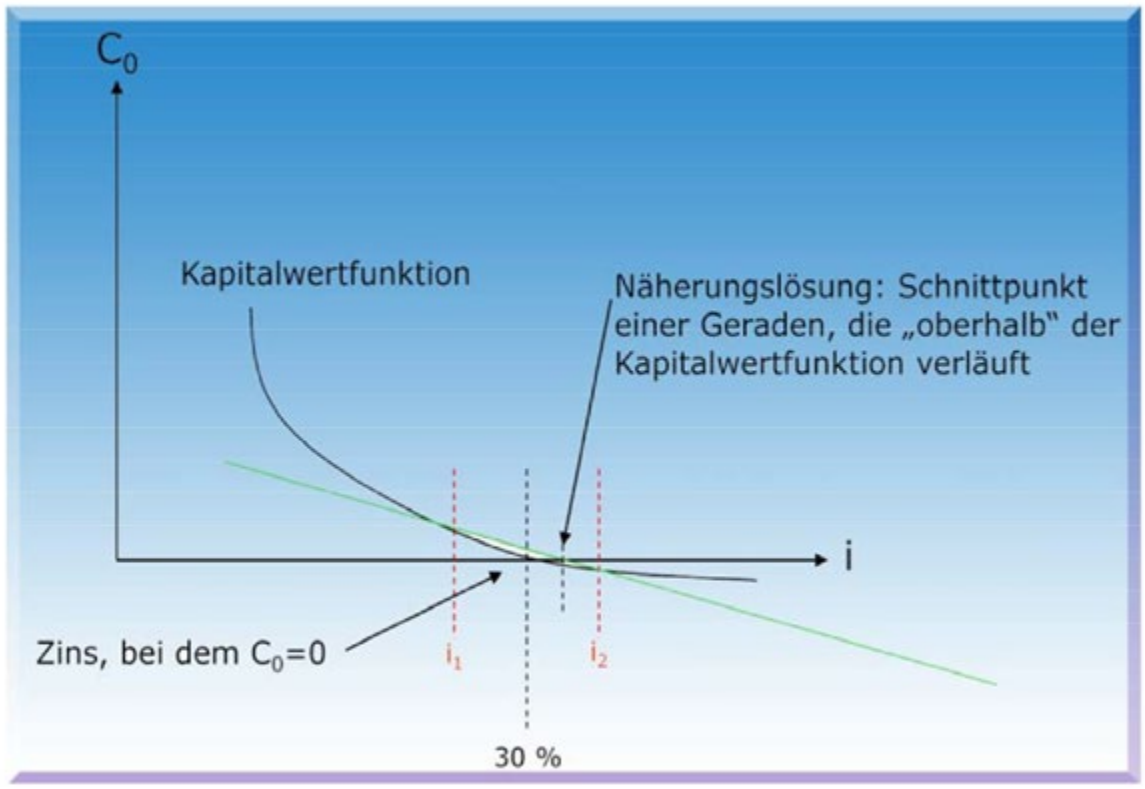

Abb. 11: Grafik „Interne Zinsfußmethode" nach Prof. Dr. Andy Junker, Vorlesungsskript „Investition" , S. 90.

Im letzten Schritt geht es nun darum, die Risiken und Maßnahmen zu überwachen:

4.4. Überwachung der Risiken und Maßnahmen

Nachdem die Risiken identifiziert und bewertet sind, die Steuerung abgeschlossen ist, geht es im letzten Schritt unseres Risikomanagement-Kreislaufs um die Überwachung. Diese Überwachung wird hier konkret unter dem Aspekt der IT-Sicherheit durchgeführt. Waren die Maßnahmen effektiv? Wie sicher ist die Organisation?

Diese und ähnliche Fragen werden in Unternehmen oft gestellt. Meist geht es dabei um die Schaffung von Wettbewerbsvorteilen. „Die Schaffung von Wettbewerbsvorteilen wird dabei als Zusammenspiel von kurz- und langfristigen Unternehmenszielen gesehen." [6] Prof. Dr. Stefan Georg geht in seiner Vorlesung „Controlling" an der HTW Saarbrücken im WS 2011/12 auf diese Punkte ein. Die Methoden zur Überwachung von Risiken können beispielsweise Kennzahlensysteme sein. „Kennzahlensysteme sind verdichtete Informationen und beziehen sich auf quantifizierbare betriebliche Tatbestände. Sie berücksichtigen dabei alle Arten von Aktivitäten und Funktionsbereiche des Unternehmens." [7] Kennzahlen erfüllen grundsätzlich Abbildungsaufgaben, Informationsaufgaben, Planungsaufgaben und Kontrollaufgaben.

6 Prof. Dr. S. Georg „Anwendungsorientiertes Controlling", 2. Auflage", Seite 120.
7 Ebd., Seite 99.

Damit sind Kennzahlensysteme genauso wie die Security Scorecard oder die Balanced Scorecard als Instrument für die Überwachungen der Risiken und Maßnahmen in der IT-Sicherheit bestens geeignet. Ein Beispiel für eine Balanced Scorecard finden wir im Buch „Anwendungsorientierte Controlling“ von Prof. Dr. Stefan Georg auf Seite 129:

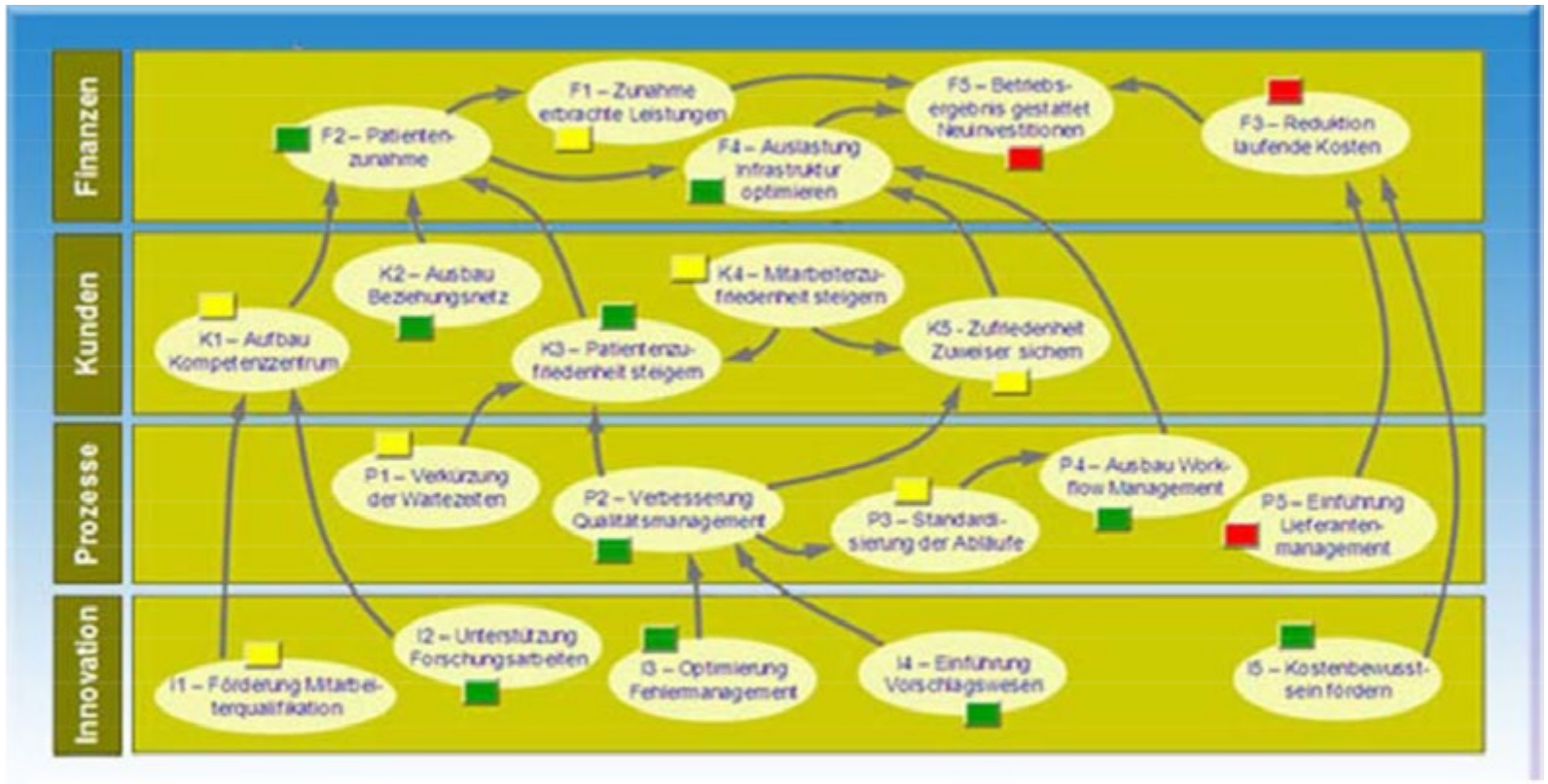

Abb. 12: Beispiel für eine Balanced Scorecard nach Prof. Dr. Stefan Georg, „Anwendungsorientiertes Controlling – 2. Auflage“, S. 129.

Mit Hilfe der Balanced Scorecard können Strategien dargestellt, operationalisiert und kommuniziert werden. Die Strategie lässt sich in operatives Handeln herunterbrechen. Lead- (vorlaufend/ Ursachen) und Lag-Indikatoren (nachlaufend/ Wirkung) sollen eine ausgewogenes (balanced) Bild vermitteln und eine vorrausschauende Planung ermöglichen. Durch das Einbeziehen von strukturellen Frühindikatoren (siehe Initiierung) kann es der Überwachung der Risiken und Maßnahmen innerhalb des hier besprochenen Risikomanagement Kreislaufes sehr gut dienen.

5. WIRTSCHAFTLICHE ASPEKTE DER IT-SICHERHEIT – EIN FAZIT

Die wirtschaftlichen Aspekte der IT-Sicherheit beginnen damit, dass man zunächst entsprechende Anlaufstellen schafft. Wie in der Arbeit gezeigt, folgen diese Aspekte zunächst der Größe des Unternehmens. Je größer ein Unternehmen ist, desto vielfältiger sind die Aufgaben an die IT-Sicherheit, desto höher sind die Kosten. Hier ist zweifellos ein kausaler Zusammenhang dargestellt.

Weniger ist manchmal mehr. Am Beispiel der Basso & Kuster GmbH sieht man, dass es nicht unbedingt notwendig ist, aus dem Server ein Fort Knox zu machen. Sinnvolle Strategien, wie im Beispiel gezeigt, müssen nicht viel Geld kosten. Sicherheit ist immer mehr als nur Technik.

IT-Sicherheit ist heute ein Thema, mit dem viel Geld zu verdienen ist. Die Frage, ob ein Unternehmen ein solches Thema outsourcen oder ob es eine eigene Abteilung aufbauen soll, ist immer eine strategische Entscheidung der Unternehmensspitze. Dabei sollten allerdings auch die Aspekte des Aufbaus von eigenem Knowhow innerhalb der IT-Sicherheit gesehen werden. An dieser Stelle möchte ich auch auf die Vorlesung „Beschaffungsmanagement" im WS 2011/12 im Fach Wirtschaftsingenieurwesen an der HTW de Saarlandes verweisen. Dipl.-Wirt.-Ing. Torsten Maus, der die Vorlesung hält, erzählte, dass die Firma ZF so weit geht, dass sie theoretisch große Maschinen, die sie bestellen, selbst nachbauen „könnte". Das Ziel ist es, so viele Informationen zu gewinnen, dass ZF Angebote auf „versteckte" Gewinne hin prüfen kann. Wenn man diese Argumentation auf den Bereich der IT-Sicherheit anwendet, dann ist grundsätzlich kein Outsourcing im Ganzen sinnvoll.

Ein Informationsaustausch zwischen Unternehmen sollte heute angesichts der bestehenden Gefahren bei jedem Unternehmen ein MUSS sein. Das Sammeln von Informationen und Erfahrungsberichten ist eine Quelle für die IT-Sicherheit, die nicht unbedingt viel Geld kosten muss. Ein Nebeneffekt dabei könnte der sein, dass man so durchaus auch das Vertrauen zukünftiger Neukunden gewinnen kann.

Zu den wirtschaftlichen Aspekten möchte ich aber auch die Folgen eines Angriffes erwähnen. Wenn man erfolgreich auf dem Server von Sony einbrechen kann oder Kundendaten der X-Box Nutzer stehlen kann, wirft das letztlich kein gutes Bild auf die Unternehmen selbst. Der Schaden, der dadurch entsteht, dass zukünftige Kunden das Produkt meiden, weil sie kein Vertrauen mehr in das Unternehmen haben, kann immens sein. Somit ist der wirtschaftliche Aspekt der IT-Sicherheit nicht nur unter dem Aspekt der Kosten für ein IT- Sicherheitssystem selbst, sondern auch unter dem Aspekt der nicht gemachten Gewinne zu sehen.

LITERATURVERZEICHNIS

Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2009, Bonn, 2009.

Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2011, Bonn, 2011.

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch 2008 (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html).

Federrath, Prof. Dr.-Ing. H.: IT-Sicherheitsmanagement nach ISO 17799 und nach BSI-Grundschutzhandbuch – Eine vergleichende Betrachtung, Universität Regensburg, http://www-sec.uni-regensburg.de.

Federrath, Prof. Dr.-Ing. H.: Vorlesungsskript „Wie viel darf IT-Sicherheit kosten?", Lehrstuhl Management der Informationssicherheit, Universität Regensburg, 2007.

Georg, Prof. Dr. rer. oec. S.: Anwendungsorientiertes Controlling 2. Auflage, Saarbrücken, 2011.

Hattenhauer, Dr. R.: Digital Survival Guide 2010, München, 2009.

Junker, Prof. Dr. rer. oec. A.: Vorlesungsskript Investition, Wirtschaftsingenieurwesen, HTW des Saarlandes, WS 11/12.

wikipedia.de

Witt, B.C.: IT-Sicherheit kompakt und verständlich, Wiesbaden, 2006.