Universität Augsburg
Prof. Dr. Hans Ulrich Buhl
Kernkompetenzzentrum
Finanz- & Informationsmanagement
Lehrstuhl für BWL, Wirtschaftsinformatik,
Informations- & Finanzmanagement

Diskussionspapier WI-176

Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen

von

Ulrich Faisst, Oliver Prokein[1], Nico Wegmann

Juli 2006

in: Zeitschrift für Betriebswirtschaft, 77, 5, 2007

[1] Institut für Informatik und Gesellschaft, Universität Freiburg

Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen

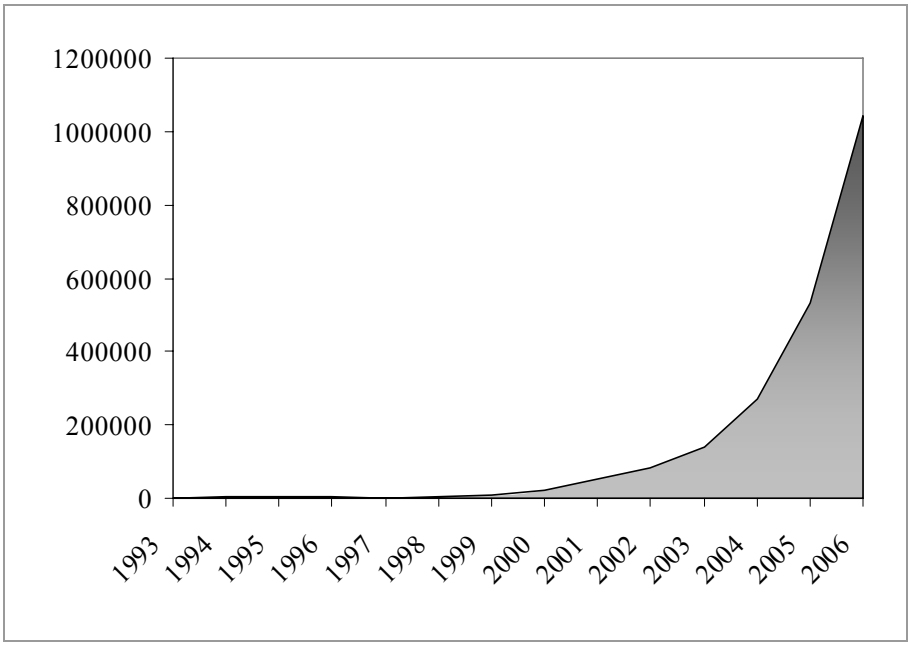
Überblick

- Die Bedeutung von IT-Sicherheitsrisiken hat in den vergangenen Jahren stark zugenommen. Unternehmungen können durch IT-Sicherheitsmaßnahmen die aufgrund von IT-Sicherheitsrisiken zu erwartenden Schäden reduzieren, müssen jedoch für deren Durchführung Auszahlungen in Kauf nehmen. Benötigt wird ein Modell, das Unternehmungen bei Entscheidungen über IT-Sicherheitsinvestitionen unterstützt.
- Dieser Beitrag präsentiert - auf Basis der Kapitalwertmethode - ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. Das Modell ermöglicht - bei bekannten Eingangsgrößen - die Bewertung der Vorteilhaftigkeit von IT-Sicherheitsinvestitionen. Zusätzlich wird in einer Erweiterung des Modells unter Zugrundelegung von im Zeitablauf fallenden Anfangsinvestitionen und steigenden IT-Sicherheitsrisiken die Vorteilhaftigkeit von Maßnahmen zu unterschiedlichen Zeitpunkten untersucht sowie der optimale Investitionszeitpunkt ermittelt. Schließlich werden die Auswirkungen von Risiko- bzw. Budgetlimiten betrachtet.
- Der Beitrag richtet sich zugleich an Wissenschaft und Praxis. Das vorgestellte, neu entwickelte Modell wird von einem führenden, internationalen Finanzdienstleister zur Entscheidungsunterstützung über IT-Sicherheitsinvestitionen bereits eingesetzt.

A. Problemstellung

Die zunehmende Virtualisierung von Geschäftsprozessen und wachsende externe Risiken (z.B. Hackerangriffe, Viren) stellen neue Herausforderungen an das Management von IT-Sicherheitsrisiken. So zeigen bspw. die Statistiken des CERT, dass die Anzahl der gemeldeten Zwischenfälle einen exponentiellen Verlauf annimmt (vgl. Abbildung 1). Legt man zugrunde, dass mit einem Anstieg der Anzahl der gemeldeten Zwischenfällen auch die Anzahl der Schadensereignisse gestiegen ist - sowie deren jeweilige durchschnittliche Schwere ebenfalls zugenommen hat oder zumindest nicht gesunken ist - so folgt daraus, dass auch die Gesamtschäden durch eingetretene IT-Sicherheitsrisiken gestiegen sind.

Abb. 1: Anzahl gemeldeter Zwischenfälle[1]



Unternehmungen können mit der Implementierung von IT-Sicherheitsmaßnahmen ihre erwarteten und unerwarteten Schäden reduzieren. In der Praxis hängt die Investitionsbereitschaft in IT-Sicherheitsmaßnahmen jedoch oftmals von den bestehenden Verantwortlichkeiten für die IT-Sicherheitsrisiken ab:

- Bestehen explizite Verantwortlichkeiten, werden Investitionen zur Verminderung bzw. Vermeidung von Risiken durchgeführt, welche z. T. betriebswirtschaftlich nicht vorteilhaft sind (Optimierungskalkül: Risiken minimieren).[2]
- Bestehen keine expliziten Verantwortlichkeiten, werden die IT-Sicherheitsrisiken häufig unterschätzt und betriebswirtschaftlich sinnvolle Investitionen nicht getätigt (Optimierungskalkül: Für das operative Geschäft nicht zwingend erforderliche Auszahlungen minimieren).

Zur Entscheidungsunterstützung wird ein Modell zur Investitionsrechnung von IT-Sicherheitsmaßnahmen benötigt. Häufig dürften die erforderlichen Anfangsinvestitionen für IT-Sicherheitsmaßnahmen im Zeitablauf sinken, jedoch die zu erwartenden Schäden tendenziell steigen. Somit stellt sich dem Entscheider zusätzlich zu der Frage, ob investiert werden soll, auch die Frage, zu welchem Zeitpunkt investiert werden soll. Ziel des Beitrags ist es, ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen zu entwickeln. Untersucht werden hierzu folgende Forschungsfragen:

- Welche Methode ist geeignet, um IT-Sicherheitsmaßnahmen betriebswirtschaftlich zu bewerten?

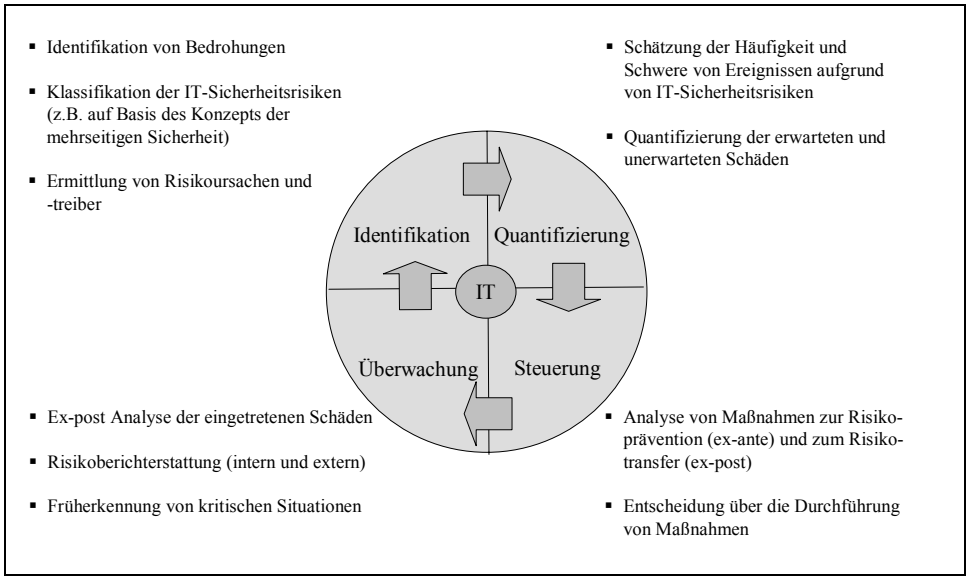
- Wie kann eine Bewertung der Vorteilhaftigkeit einer IT-Sicherheitsmaßnahme - trotz in der Praxis bestehender Probleme bei der Abschätzung der Eingangsgrößen - erfolgen?
- Wie kann unter der zusätzlichen Annahme im Zeitablauf fallender Anfangsinvestitionen und steigender IT-Sicherheitsrisiken die Vorteilhaftigkeit von IT-Sicherheitsmaßnahmen zu unterschiedlichen Zeitpunkten bewertet und ein optimaler Investitionszeitpunkt ermittelt werden?
- Wie beeinflussen Risiko- bzw. Budgetlimite die Vorteilhaftigkeit von IT-Sicherheitsmaßnahmen und den optimalen Investitionszeitpunkt?

Um die Grundlagen zur Beantwortung dieser Forschungsfragen zu legen, soll zunächst der wissenschaftliche State-of-the-art vorgestellt werden.

B. Kreislauf des IT-Sicherheitsmanagements

Der betriebswirtschaftliche Stand der Forschung lässt sich entlang des Kreislaufs des IT-Sicherheitsmanagements in vier Phasen beschreiben: Identifikation, Quantifizierung, Steuerung und Überwachung (vgl. Abbildung 2).[3]

Abb. 2: Kreislauf des IT-Sicherheitsmanagements



I. Identifikationsphase

Die *Identifikationsphase* dient der Definition und Klassifizierung von bestehenden IT-Sicherheitsrisiken, der Bestandsaufnahme von Bedrohungsszenarien sowie der Ermittlung von Risikoursachen und -treibern. Zur Definition und Klassifizierung erscheint das Konzept der Mehrseitigen Sicherheit geeignet.[4] Insbesondere bei offenen Kommunikationssystemen kann nicht davon ausgegangen werden, dass sich alle Parteien – wie etwa eigene Mitarbeiter der Unternehmung oder externe Mitarbeiter von IT-Dienstleistern, Diensteanbieter, Netzbetreiber oder Kunden – gegenseitig kennen oder gar vollständig vertrauen. Entsprechend müssen bei der Analyse der Sicherheit neben externen Angreifern auch alle anderen beteiligten Parteien als potentielle Angreifer betrachtet werden. Die IT-Sicherheitsrisiken ergeben sich aus der Bedrohung der vier Schutzziele:

- Vertraulichkeit (Risiko des unbefugten Informationsgewinns),
- Integrität (Risiko der unbefugten Modifikation von Informationen und Daten),
- Zurechenbarkeit (Risiko der unzulässigen Unverbindlichkeit) und
- Verfügbarkeit (Risiko der unbefugten Beeinträchtigung der Funktionalität).[5]

Die Ermittlung möglicher Bedrohungsszenarien kann bspw. anhand der im IT-Grundschutzhandbuch des BSI aufgeführten Gefährdungskataloge für höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen erfolgen.[6] Zusätzlich zu derartigen extern entwickelten Katalogen der Bedrohungsszenarien und möglichen IT-Sicherheitsrisiken finden insbesondere folgende Methoden zur Risikoidentifikation bei Unternehmungen oftmals Anwendung:

- Mitarbeiter- und Experteninterviews mit Hilfe von Fragebogen bzw. Checklisten und
- Analyse historischer unternehmensinterner und branchenweiter Schadensfälle.

II. Quantifizierungsphase

Auf die Identifikationsphase folgt in einem nächsten Schritt die Bewertung der IT-Sicherheitsrisiken im Rahmen der *Quantifizierungsphase*. Die Bewertung kann insbesondere durch die Beschreibung der Verteilung der Häufigkeit und der Schwere von Schadensereignissen geschehen, um daraus die zukünftig erwarteten und unerwarteten Schäden abzuschätzen.[7]

Die existierenden Quantifizierungsmethoden können in vier Gruppen zugeordnet werden:[8]

- Befragungstechniken,
- Indikator-Ansätze,

- Stochastische Methoden und
- Kausal-Methoden.

Bei *Befragungstechniken* wird i.d.R. mit Hilfe von strukturierten Fragebögen versucht, IT-Sicherheitsrisiken zu identifizieren und zu quantifizieren. *Indikator-Ansätze* hingegen fokussieren auf eine bestimmte Kennzahl respektive auf ein Kennzahlensystem, anhand dessen das vorliegende IT-Sicherheitsrisiko indirekt ermittelt wird. Dabei werden einerseits auf Basis empirischer Untersuchungen und andererseits auf Basis von Expertenmeinungen Indikatoren gewählt, für die ein Zusammenhang mit der Höhe des IT-Sicherheitsrisikos vermutet wird. *Stochastische Methoden* benutzen statistische Verteilungsfunktionen zur Schätzung der Höhe der IT-Sicherheitsrisiken. Anhand von historischen Schadensdaten bzgl. der Häufigkeit und Schwere von eingetretenen Schäden werden mit Hilfe von Simulationen Prognosen für zukünftige Ereignisse getroffen.[9] Bei *Kausal-Methoden* werden speziell Zusammenhänge zwischen den identifizierten Risikoquellen bzw. -treibern und den daraus resultierenden Schäden unter Zuhilfenahme statistischer Methoden untersucht.

III. Steuerungsphase

Nach der Quantifizierung der IT-Sicherheitsrisiken soll die darauf folgende *Steuerungsphase* betriebswirtschaftliche Entscheidungen über die Durchführung von IT-Sicherheitsmaßnahmen unterstützen. Mit der Durchführung von IT-Sicherheitsmaßnahmen kann bspw. das Eintreten von Schadensereignissen vermindert und bzw. oder ein Teil des möglichen Ausmaßes der Schadensereignisse an Dritte übertragen werden. Die zur Steuerung von IT-Sicherheitsrisiken eingesetzten Instrumente lassen sich in interne und externe Steuerungsinstrumente klassifizieren (vgl. Tabelle 1).

Tab. 1: Ausgewählte interne und externe Steuerungsinstrumente[10]

Interne Steuerungsinstrumente	Externe Steuerungsinstrumente
▪ Maßnahmen zum Schutz von Daten, Soft- und Hardware sowie Vernetzungstechnologien ▪ Prozessverbesserungen ▪ Maßnahmen zur Mitarbeitermotivation	▪ Versicherungen ▪ Outsourcing ▪ Alternative Risiko-Transferinstrumente

Die internen Steuerungsinstrumente zielen auf die Ursachen von IT-Sicherheitsrisiken. Sie umfassen u. a. Maßnahmen zum Schutz von Daten, Soft- und Hardware sowie Vernetzungstechnologien, zur Prozessverbesserung sowie zur Mitarbeitermotivation. Mit Hilfe von exter-

nen Steuerungsinstrumenten werden IT-Sicherheitsrisiken auf Dritte übertragen. Zu externen Steuerungsinstrumenten zählen neben Versicherungen das Outsourcing von Prozessen und Systemen sowie Alternative Risiko-Transferinstrumente.[11]

Zur Entscheidungsunterstützung über die Durchführung von IT-Sicherheitsmaßnahmen und damit den Einsatz der vorgestellten Instrumente wurden bereits erste Ansätze entwickelt. So betrachtet bspw. *Faisst* (2004) in einem einperiodigen Modell den Trade-off zwischen Auszahlungen für IT-Sicherheitsmaßnahmen einerseits, sowie den Auszahlungen, die durch die erwarteten Schäden sowie durch die Opportunitätskosten[12] einer Eigenkapitalunterlegung für unerwartete Schäden hervorgerufen werden, andererseits.[13] Je niedriger die Auszahlungen für IT-Sicherheitsmaßnahmen sind, desto höher ist das Risiko. Mit einem höheren Risiko verbunden sind steigende Auszahlungen aufgrund von zu erwartenden Schäden und durch die Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden. Dieses Modell ist jedoch zur Bewertung von Investitionen in IT-Sicherheitsmaßnahmen nur bedingt geeignet. So dürfte aufgrund der oftmals hohen Anfangsinvestitionen eine einperiodige Betrachtung nicht ausreichend sein und sollte durch eine mehrperiodige Betrachtung erweitert werden.[14]

IV. Überwachungsphase

Der Kreislauf des IT-Sicherheitsmanagements wird durch die *Überwachungsphase* abgerundet. Während in der Identifikations-, Quantifizierungs- und Steuerungsphase eine ex-ante Betrachtung von IT-Sicherheitsrisiken vorgenommen wird, dient die Überwachungsphase der ex-post Analyse der eingetretenen Schäden und der Evaluation der in den vorangegangenen Phasen getroffenen Annahmen und Entscheidungen. So kann bspw. untersucht werden:

- ob die eingetretenen Schadensfälle bekannten Risikoarten bzw. Szenarien entsprechen und falls nicht, ob gegebenenfalls die vorgenommene Risikoklassifikation in der Identifikationsphase unvollständig war,
- ob die eingetretenen Schadensfälle in ihrer Häufigkeit und Schwere die vorgenommene Quantifizierung in Frage stellen und
- ob die in der Steuerungsphase verabschiedeten Investitionen in IT-Sicherheitsmaßnahmen aus einer ex post Sicht den gewünschten Effekt hatten.[15]

Zu den Aufgaben der Überwachungsphase gehört darüber hinaus die fortlaufende Berichterstattung an unterschiedliche Stakeholder wie Aufsichtsbehörden sowie zuständige Verantwortliche im Management der Unternehmung.

Nachdem der Kreislauf des IT-Sicherheitsmanagements in vier Phasen vorgestellt wurde, gibt die folgende Tabelle 2 einen zusammenfassenden Überblick über den Stand der Forschung anhand von untersuchten Forschungsfragen in ausgewählten Beiträgen.

Tab. 2: Überblick über ausgewählte Beiträgen zum Management operationeller Risiken im allgemeinen und zum IT-Sicherheitsmanagement im speziellen

Phase	Forschungsfrage	Beitrag	Methodik
Identifikation	▪ Wie können IT-Sicherheitsrisiken und Bedrohungsszenarien kategorisiert werden?	*Rannenberg* (1998); *Müller/Rannenberg* (1999); *BSI* (2006)	deskriptive Analyse
	▪ Mit welchen Verfahren und Methoden können potentielle Schadensereignisse identifiziert werden? ▪ Wie können Risikoquellen und -treiber analysiert werden?	*Brink* (2000) *Basel Committee on Banking Supervision* (2001); *Marshall* (2001); *Piaz* (2001); *Cruz* (2002); *Eller/Gruber/Reif* (2002); *Füser/Rödel/Kang* (2002); *Jörg* (2002); *Locarek-Junge/Hengmith* (2003)	deskriptive Analyse
		Hoffman (2002)	Fallstudie
Quantifizierung	▪ Mit welchen Methoden kann die Höhe von IT-Sicherheitsrisiken bestimmt werden? ▪ Wie können IT-Sicherheitsrisiken aggregiert werden? ▪ Wie können seltene Ereignisse großen Ausmaßes quantifiziert werden?	*Brink* (2000); *Buhr* (2000); *Marshall* (2001); *Piaz* (2001); *Cruz* (2002); *Eller/Gruber/Reif* (2002); *Füser/Rödel/Kang* (2002); *Jörg* (2002)	deskriptive Analyse
		Hoffman (2002)	Fallstudie
	▪ Welche Quantifizierungsmethoden eignen sich für bestimmte Einsatzgebiete bzw. Risikotypen?	*Faisst/Kovacs* (2003)	deskriptive Analyse / Klassifikation
	▪ Wie hoch sind die Schäden aufgrund operationeller Risiken auf Basis historischer Daten?	*Basel Committee on Banking Supervision* (2003); *Fontnouvelle et al.* (2003); *Gordon et al.* (2005); *Fontnouvelle/Rosengren* (2004); *Chavez-Demoulin/Embrechts/Neslehová* (2005);	empirische Studie
		Beeck/Kaiser (2000); *Wiedemann* (2004)	Simulationsmodell
	▪ Wie hoch ist der Beitrag einzelner Prozesse zur Gesamthöhe operationeller Risiken?	*Ebnöther/Vanini/McNeil/Antolinez-Fehr* (2001)	Simulationsmodell
Steuerung	▪ Welche Instrumente stehen zur Steuerung von operationellen Risiken im allgemeinen bzw. von IT-Sicherheitsrisiken im speziellen zur Verfügung? ▪ Wie wirkt sich die Anwendung von Steuerungsinstrumenten auf die Häufigkeit und Schwere operationeller Risiken aus?	*Brink* (2000); *Marshall* (2001); *Piaz* (2001); *Cruz* (2002); *Eller/Gruber/Reif* (2002); *Grzebiela* (2002); *Jörg* (2002); *Locarek-Junge/ Hengmith* (2003); *Müller/Eymann/ Kreutzer* (2003); *Eckert* (2004)	deskriptive Analyse
		Spahr (2001); *Hoffman* (2002); *Gordon/Loeb* (2006)	Fallstudie
		Faisst (2004); *Faisst/Prokein* (2005); *Gordon/Loeb* (2002)	formal-mathematisches Modell
Überwachung	▪ Welche Methoden und Verfahren eignen sich für die Überwachung von operationellen Risiken? ▪ Welche organisatorischen Anforderungen beinhaltet eine Überwachung von operationellen Risiken im laufenden Geschäftsbetrieb?	*Brink* (2000); *Anders* (2001); *Basel Committee on Banking Supervision* (2001); *Marshall* (2001); *Piaz* (2001); *Cruz* (2002); *Eller/Gruber/Reif* (2002); *Locarek-Junge/Hengmith* (2003); *Basel Committee on Banking Supervision* (2003).	deskriptive Analyse
		Hoffman (2002)	Fallstudie

C. Bewertung von IT-Sicherheitsmaßnahmen - Anforderungen und Methoden

In diesem Abschnitt sollen zunächst Anforderungen an eine betriebswirtschaftliche Bewertung von IT-Sicherheitsmaßnahmen formuliert werden, anschließend soll untersucht werden, inwieweit die vorhandenen Methoden diesen Anforderungen entsprechen.

I. Anforderungen

Die eingesetzte Methode zur Bewertung von IT-Sicherheitsmaßnahmen sollte folgenden Anforderungen genügen:

1. *Abbildung von mehrperiodigen Laufzeiten der Maßnahmen***:** IT-Sicherheitsmaßnahmen werden zu einem bestimmten Zeitpunkt eingerichtet und dann i.d.R. über mehrere Perioden hinweg in der Unternehmung durchgeführt. Die Bewertungsmethode sollte daher die relevanten Bewertungsgrößen auch über mehrere Perioden abbilden können.
2. *Berücksichtigung der Zeitpräferenz:* Eine Unternehmung als Investor besitzt eine Zeitpräferenz, die sich durch seine Möglichkeit zur Wiederanlage erklären lässt. So kann sie - im Vergleich zur Investition in eine IT-Sicherheitsmaßnahme - in alternative Anlagen investieren. Sie fordert daher eine Mindestverzinsung für das für die Durchführung von IT-Sicherheitsmaßnahmen gebundene Kapital.
3. *Berücksichtigung der ökonomischen Eigenkapitalunterlegung für unerwartete Schäden**:*** Wenn die Risikotragfähigkeit[16] der Unternehmung zu einem bestimmten Konfidenzniveau sichergestellt werden soll, dann sind die unerwarteten Schäden aufgrund von IT-Sicherheitsrisiken durch ökonomisches Eigenkapital zu unterlegen.[17] Durch die Eigenkapitalunterlegung entstehen der Unternehmung Opportunitätskosten, da dieses Eigenkapital nicht für alternative risikobehaftete Geschäfte eingesetzt werden kann. Die Durchführung von IT-Sicherheitsmaßnahmen dürfte zur Verringerung auch der unerwarteten Schäden und damit der Opportunitätskosten der ökonomischen Eigenkapitalunterlegung beitragen.

Vereinfachend werden im Weiteren Wechselwirkungen zwischen IT-Sicherheitsmaßnahmen vernachlässigt. Auf eine Portfoliobetrachtung wird verzichtet, zumal diese weitere Anforderungen bezüglich der Aggregationsfähigkeit der Ergebnisse bedingt hätte.

II. Vergleich der Methoden

In der Literatur ist eine Vielzahl von Methoden bekannt, die zur Entscheidungsunterstützung bei der Bewertung von IT-Sicherheitsmaßnahmen herangezogen werden können. Im Folgenden werden ausgewählte Methoden kurz formal definiert und anhand der gestellten Anforderungen bewertet:

Eine in der Praxis häufig verwendete Kennzahl zur Bewertung von Investitionsmaßnahmen stellt der *Return on Investment (ROI)* dar. Dabei wird der Gewinn der betrachteten Investition ins Verhältnis zum gebundenen Kapital gesetzt:

(1) $$\text{ROI} = \frac{\text{Gewinn vor Zinsen}}{\text{Kapitaleinsatz}}$$.[18]

Speziell für den IT-Sicherheitsbereich wurde ein modifizierter *ROI* entwickelt, der als *Return on Security Investment (ROSI)* bezeichnet wird. Die Rentabilität einer IT-Sicherheitsmaßnahme wird anhand eines Vergleichs des gesenkten IT-Sicherheitsrisikos durch die Implementierung einer IT-Sicherheitsmaßnahme mit den Kosten für die Maßnahme ermittelt:

(2) $$\text{ROSI} = \frac{(\text{Monetäre Bewertung der IT-Sicherheitsrisiken} \cdot \text{anteilige Reduktion}) - \text{Projektkosten}}{\text{Projektkosten}}$$.[19]

Zusätzlich kann die Vorteilhaftigkeit einer Investitionsmaßnahme durch die Berechnung der *Amortisationsdauer*, d.h. die Anzahl der Jahre, nach der sich die getätigte Investition selbst refinanziert hat, bewertet werden:

(3) $$\text{Amortisationsdauer} = \frac{\text{ursprünglicher Kapitaleinsatz}}{\text{durchschnittlicher Rückfluss pro Jahr}}$$.[20]

So genannte *risikoadjustierte Performance Kennzahlen (RAPM)* bewerten den Erfolg eines Geschäfts im Verhältnis zum damit eingegangenen Risiko:

(4) $$\text{RAPM} = \frac{\text{(risikoadjustierte) Ertragsgröße}}{\text{(risikoadjustierte) Kapitalgröße}}$$.[21]

Mit Hilfe des *Economic Value Added (EVA)* kann der in Geldeinheiten gemessene Betrag berechnet werden, den eine Unternehmung innerhalb einer Periode nach Abzug aller Kosten erwirtschaftet hat. Zur Berechnung des *EVA* in der Periode zwischen t-1 und t (EVA_t) wird

das gebundene Kapital in Periode t-1 ($Capital_{t-1}$) mit der Differenz aus dem *ROI* in Periode t (ROI_t) und den *Weighted Average Cost of Capital (WACC)* multipliziert:

(5) $$EVA_t = (ROI_t - WACC) \cdot Capital_{t-1}.$$ [22]

Ein dynamisches Verfahren der Bewertung von Investitionsmaßnahmen stellt die *Kapitalwertmethode* dar. Hierbei werden sämtliche mit einer Investition verbundenen Einzahlungen (laufende periodige Einzahlungen E_t sowie Liquidationserlös L_T) und Auszahlungen (laufende periodige Auszahlungen A_t und Anfangsinvestition I_0) auf den Kalkulationszeitpunkt mit dem Diskontierungszinssatz i abgezinst:

(6) $$NPV_0 = -I_0 + \sum_{t=1}^{T} \frac{E_t - A_t}{(1+i)^t} + \frac{L_T}{(1+i)^T}.$$ [23]

Der *interne Zinssatz* stellt denjenigen Zinssatz dar, bei dem der *Kapitalwert* den Wert Null annimmt:

(7) $$NPV_0 = 0 = -I_0 + \sum_{t=1}^{T} \frac{E_t - A_t}{(1+i)^t} + \frac{L_T}{(1+i)^T}.$$ [24]

Tabelle 3 stellt die ausgewählten Methoden den Anforderungen gegenüber.

Tab. 3: Vergleich der Methoden der Investitionsrechnung gemäß den Anforderungen

	ROI	ROSI	Amortisationsdauer	EVA	RAPM	Kapitalwertmethode	Interne Zinsatzmethode
Abbildung von mehrperiodigen Laufzeiten der Maßnahmen	-	-	✔	-	-	✔	✔
Berücksichtigung der Zeitpräferenz	-	-	-	-	-	✔	✔
Berücksichtigung der ökonomischen Eigenkapitalunterlegung für unerwartete Schäden	-	-	-	✔	✔	-	-

Eine Analyse der ausgewählten Methoden hinsichtlich der *Abbildung von mehrperiodigen Laufzeiten der Maßnahmen* liefert das Ergebnis, dass diese Anforderung nur von der Amortisationsdauer, der Kapitalwertmethode sowie der internen Zinssatzmethode erfüllt wird.

Im Gegensatz zur *Amortisationsdauer* wird bei der Berechnung des *Kapitalwerts* sowie des internen Zinssatzes weiter die *Zeitpräferenz* berücksichtigt. Alle weiteren Methoden genügen dieser Anforderung ebenfalls nicht. Die *ökonomische Eigenkapitalunterlegung für unerwartete Schäden* wird nur vom *Economic Value Added (EVA)* sowie den *risikoadjustierten Performance Kennzahlen (RAPM)* berücksichtigt.

Keine der vorgestellten Methoden entspricht damit allen gestellten Anforderungen. Die *Kapitalwertmethode* (und damit verbunden die *interne Zinssatzmethode*) entspricht jedoch den gestellten Anforderungen bereits in zwei von drei Kriterien. Die *Kapitalwertmethode* wird daher im folgenden Modell um die Berücksichtigung der ökonomischen Eigenkapitalunterlegung für unerwartete Schäden angepasst.

D. Modell

Vorgestellt wird ein Modell zur Entscheidungsunterstützung über Investitionen in IT-Sicherheitsmaßnahmen. Bewertet werden IT-Sicherheitsmaßnahmen zum Schutz gegen zum Zeitpunkt t=0 - aufgrund von identifizierten Angriffsszenarien[25] - bekannte IT-Sicherheitsrisiken.[26] In t=0 nicht identifizierte Angriffsszenarien und damit verbundene IT-Sicherheitsrisiken werden in diesem Beitrag nicht betrachtet. Zunächst werden in Abschnitt I Annahmen getroffen und in Abschnitt II die Vorteilhaftigkeit von IT-Sicherheitsmaßnahmen zum Zeitpunkt t=0 untersucht. In Abschnitt III wird das Modell um zusätzliche Annahmen - wie im Zeitablauf sinkende Anfangsinvestitionen und zugleich steigende IT-Sicherheitsrisiken - erweitert, und die Vorteilhaftigkeit zu allen Zeitpunkten zwischen t=0 und t=T (Betrachtungshorizont) untersucht, um daraus den optimalen Investitionszeitpunkt zu bestimmen. Schließlich werden zusätzlich Risiko- bzw. Budgetlimite in Abschnitt IV betrachtet und deren Auswirkungen untersucht.

I. Annahmen

Dem Modell liegen folgende Annahmen A1 bis A4 (in *Kursivschrift*) zugrunde:

A1 (IT-Sicherheitsmaßnahme zum Schutz von Vermögenswerten):

Betrachtet wird eine IT-Sicherheitsmaßnahme, die zum Schutz von Vermögenswerten (z. B. Fortgang des Geschäftsbetriebs, Markenwert der Unternehmung, etc.) eingesetzt wird. Wechselwirkungen zwischen verschiedenen IT-Sicherheitsmaßnahmen sowie Vermögenswerten werden vereinfachend nicht berücksichtigt.

A2 (Bewertung der Vorteilhaftigkeit):

Ausgehend von einem risikoneutralen Entscheider soll die Vorteilhaftigkeit einer IT-Sicherheitsmaßnahme anhand des Kapitalwerts NPV_0 *in t=0 bewertet werden. Der Kapitalwert* NPV_0 *setzt sich zusammen:*

- *einerseits aus der Anfangsinvestition* I_0 (mit $I_0 \geq 0$) *zum Zeitpunkt* t=0*, zzgl. den zusätzlichen laufenden Auszahlungen für Betrieb und Wartung der IT-Sicherheitsmaßnahme* C_t *(*mit $C_t \geq 0$*) zu den Zeitpunkten* t=1 *bis* t=T,[27] *sowie*
- *andererseits aus der - durch die Implementierung der IT-Sicherheitsmaßnahme bewirkten - Reduktion der erwarteten Schäden* $\Delta E(L_t)$ *zzgl. der Reduktion der Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden* ΔOCC_t *jeweils zu den Zeitpunkten* t=1 *bis* t=T.[28]

Vereinfachend sollen die jeweiligen Zahlungen[29] der Periode]t-1;t] für 1≤t≤T (mit t ∈ ℕ über eine Laufzeit von T) nachschüssig zu den Zeitpunkten t=1 bis t=T anfallen.[30] Ebenso vereinfachend werde ein konstanter risikoloser Zinssatz i_{calc} (mit $i_{calc} \geq 0$) *zugrunde gelegt.[31] Der Kapitalwert* NPV_0 *ist daher:*

$$(8) \qquad NPV_0 = -I_0 + \sum_{t=1}^{T} \frac{\Delta E(L_t) + \Delta OCC_t - C_t}{(1+i_{calc})^t}.$$

A3 (Erwartete Schäden und deren Reduktion durch die Implementierung einer IT-Sicherheitsmaßnahme):

A3.1 (Erwartete Schäden):

Die erwarteten Schäden $E(L_t)$ (mit $E(L_t) \geq 0$) *werden durch Multiplikation der erwarteten Häufigkeit von Schadensereignissen* $E(Q_t)$ (mit $E(Q_t) \geq 0$) *mit der erwarteten durchschnittlichen Schwere von Schadensereignissen* LGE_t (mit $LGE_t \geq 0$) *ermittelt. Dabei seien die Häufigkeit von Schadensereignissen* Q_t *und deren Schwere voneinander unabhängig. Es gilt für die erwarteten Schäden* $E(L_t)$ *jeweils zu den Zeitpunkten* t=1 *bis* t=T*:*

(9) $E(L_t) = E(Q_t) \cdot LGE_t$.

Die Implementierung einer IT-Sicherheitsmaßnahme führt zu einer Reduktion der erwarteten Häufigkeit von Schadensereignissen $E(Q_t)$*. Vereinfachend wird die Schwere eines Schadensereignisses* LGE_t *nach Einführung der IT-Sicherheitsmaßnahme jeweils in Höhe der erwarteten durchschnittlichen Schwere angenommen.*

A3.2 (Erwartete Häufigkeit von Schadensereignissen):

Die erwartete Häufigkeit von Schadensereignissen $E(Q_t)$ *ergibt sich durch Multiplikation der erwarteten Häufigkeit versuchter Angriffe* $E(N_t)$ *(mit* $E(N_t) \geq 0$*) mit* $(1\text{-}SL_t)$*. Die Häufigkeit versuchter Angriffe* N_t *sei exogen gegeben.* SL_t *bezeichnet den Sicherheitslevel, d.h. den Anteil der versuchten Angriffe, der durch die eingesetzte IT-Sicherheitsmaßnahme abgewehrt werden kann (mit* $0 \leq SL_t \leq 1$*).*[32] *Es gilt für die erwartete Häufigkeit von Schadensereignissen* $E(Q_t)$ *jeweils zu den Zeitpunkten* t=1 *bis* t=T*:*

(10) $E(Q_t) = E(N_t) \cdot (1 - SL_t)$.

A3.3 (Erwartete durchschnittliche Schwere eines Schadensereignisses):

Die erwartete durchschnittliche Schwere eines Schadensereignisses LGE_t *ergibt sich durch die Multiplikation des im Falle eines Schadensereignisses durchschnittlich betroffenen Vermögenswerts* AV_t *(*mit $AV_t \geq 0$*) mit dem Faktor (*$1\text{-}IL_t$*). Die Übertragbarkeitsquote* IL_t *(*mit $0 \leq IL_t \leq 1$*) zu den Zeitpunkten t=1 bis t=T beschreibt die Übertragung von eingetretenen Schäden auf Dritte (z.B. aufgrund bestehender Versicherungspolicen, Outsourcing-Verträge, etc.). Es gilt für die erwartete durchschnittliche Schwere eines Schadensereignisses* LGE_t *jeweils zu den Zeitpunkten t=1 bis t=T:*

(11) $LGE_t = AV_t \cdot (1 - IL_t)$.

Anmerkung: Bei der Abschätzung des betroffenen Vermögenswerts AV_t sind insbesondere der Schaden aufgrund von Geschäftsausfall (durch Betriebsunterbrechung), die Wiederherstellungskosten sowie der buchhalterische Wert des betroffenen IT-Systems zu berücksichtigen. Darüber hinaus könnte man aber auch durchaus auch „weiche“ Größen, wie Imageverlust im Falle eines Schadensereignisses in die Betrachtung mit einschließen.

Durch die Implementierung der IT-Sicherheitsmaßnahme verbessert sich der Sicherheitslevel, sofern $\Delta SL_t = (SL_t - SL_0) \geq 0$ gilt (mit SL_0 als Sicherheitslevel zum Zeitpunkt t=0 vor Implementierung der IT-Sicherheitsmaßnahme und SL_t als Sicherheitslevel zu den Zeitpunkten t=1 bis t=T nach Implementierung der IT-Sicherheitsmaßnahme).

Ist $\Delta SL_t \geq 0$ und sind zugleich die erwarteten versuchten Angriffe $E(N_t)$, die durchschnittlich betroffenen Vermögenswerte AV_t sowie die Übertragbarkeitsquote IL_t konstant, so gilt für die Reduktion der erwarteten Schäden $\Delta E(L_t)$ durch die Implementierung der IT-Sicherheitsmaßnahme:

(12) $\Delta E(L_t) \geq 0$ mit $\Delta E(L_t) = \Delta SL_t \cdot E(N_t) \cdot (1 - IL_t) \cdot AV_t$.

A4 (Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden): Die Häufigkeit von Schadensereignissen Q_t unterliege der Poisson-Verteilung.

Da nach Annahme A4 eine poissonverteilte Häufigkeit von Schadensereignissen Q_t und zugleich nach Annahme A3 die Schwere eines Schadensereignisses LGE_t in durchschnittlicher Höhe betrachtet wird, ist es möglich, aus den erwarteten Schäden $E(L_t)$ mit Hilfe eines von $E(Q_t)$ abhängigen Gamma-Faktors die zu einem bestimmten Konfidenzniveau bestehenden unerwarteten Schäden zu ermitteln und daraus die notwendige Eigenkapitalunterlegung CC_t zu bestimmen:[33]

(13) $CC_t = \gamma_t \cdot E(L_t)$

mit

γ_t = Gamma-Faktor in Abhängigkeit von $E(Q_t)$ zu den Zeitpunkten t=1 bis t=T.

Eine tabellarische Übersicht über die entsprechenden Werte für γ befindet sich im Anhang 1.[34]

Die Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden betragen:

(14) $OCC_t = CC_t \cdot i_{opp}$

mit

i_{opp} = Opportunitätskostenzinssatz des Eigenkapitals.

Eine Eigenkapitalunterlegung für unerwartete Schäden ist ökonomisch sinnvoll, da durch Allokation von Eigenkapital die Risikotragfähigkeit für unerwartete Schäden zu einem bestimmten Konfidenzniveau sichergestellt wird. Für das gebundene Eigenkapital entstehen der Unternehmung Opportunitätskosten, da dieses nicht mehr für andere risikobehaftete Geschäftsaktivitäten verwendet werden kann. Pro Einheit gebundenem Eigenkapital entstehen Opportunitätskosten, die mit dem Opportunitätskostenzinssatz i_{opp} ausgedrückt werden. Dabei gilt i. d. R. $i_{opp} > i_{calc}$.

Durch eine Verbesserung des Sicherheitslevels SL_t folgt auch eine Reduktion der Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden ΔOCC_t. Die Reduktion der

Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden durch die Implementierung einer IT-Sicherheitsmaßnahme ΔOCC_t beträgt:

(15) $\Delta OCC_t = (i_{opp} \cdot \gamma_0 \cdot E(L_0)) - (i_{opp} \cdot \gamma_t \cdot E(L_t)) = i_{opp} \cdot (\gamma_0 \cdot E(L_0) - \gamma_t \cdot E(L_t))$

mit

γ_0 = Gamma-Faktor zum Zeitpunkt t=0,

γ_t = Gamma-Faktor zu den Zeitpunkten t=1 bis t=T.

Der erste Term der Gleichung (15) entspricht den Opportunitätskosten für unerwartete Schäden *vor* Implementierung der IT-Sicherheitsmaßnahme OCC_0, der zweite Term stellt die Opportunitätskosten für unerwartete Schäden OCC_t *nach* Implementierung der IT-Sicherheitsmaßnahme zu den Zeitpunkten t=1 bis t=T dar.

II. Bewertung der Vorteilhaftigkeit einer Investition zum Zeitpunkt t=0

Im Folgenden wird die Vorteilhaftigkeit der Durchführung einer (zusätzlichen) IT-Sicherheitsmaßnahme zum Zeitpunkt t=0 bewertet.

Ergebnis 1: Anhand des Kapitalwerts NPV_0 kann die Vorteilhaftigkeit einer IT-Sicherheitsmaßnahme beurteilt werden. Bei Vorliegen nur einer Alternative gilt folgende Empfehlung:

(16) für $NPV_0 > 0$: die IT-Sicherheitsmaßnahme durchzuführen bzw.

für $NPV_0 \leq 0$: die IT-Sicherheitsmaßnahme nicht durchführen.

Bei Vorliegen mehrerer, sich ausschließender Alternativen soll die Alternative mit dem größten Kapitalwert NPV_0 durchgeführt werden, sofern dieser größer null ist.

Ergebnis 1 setzt voraus, dass die in den Annahmen vorgestellten Eingangsgrößen zur Bestimmung des Kapitalwerts bekannt und über den Zeitablauf konstant sind. Die Eingangsgrößen dürften unterschiedlich leicht bestimmbar sein, wie sich in der praktischen Umsetzung des Modells zeigte. Während die Anfangsinvestition I_0 und die zusätzlichen laufenden Auszahlungen für Betrieb und Wartung der IT-Sicherheitsmaßnahme C_t anhand der Projektkalkulation meist einfach zu bestimmen sein dürften, sind die zukünftige Reduktion der erwarteten Schäden $\Delta E(L_t)$ und die Reduktion der Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden ΔOCC_t auf Basis von, häufig für Simulationen unzureichenden, historischen Daten und Expertenmeinungen zu schätzen. Gerade die Häufigkeit und die Schwere von Schadensereignissen dürften i. d. R. schwierig bestimmbar sein. Mit der Analyse unterschiedlicher Szenarien können dennoch Aussagen über die Vorteilhaftigkeit der IT-Sicherheitsmaßnahme bei Vorliegen bspw. unterschiedlicher erwarteter Häufigkeiten von

versuchten Angriffen pro Jahr $E(N_t)$, unterschiedlicher Sicherheitslevel SL_t (und somit auch unterschiedlichen erwarteten Häufigkeiten erfolgreicher Angriffe pro Jahr $E(Q_t)$) sowie unterschiedlichen durchschnittlich erwarteten Schweren eines Schadensereignisses LGE_t jeweils getroffen werden (vgl. Beispiel 1).[35]

Beispiel 1: Analyse unterschiedlicher Szenarien bei ungenau vorliegenden Eingangsgrößen

Das Beispiel 1 illustriert, dass auch bei einer ungenau vorliegenden reduzierten Häufigkeit von Schadensereignissen $\Delta E(Q_t)$ sowie einer ungenau vorliegenden durchschnittlichen Schwere eines Schadensereignisses LGE_t Aussagen über die Vorteilhaftigkeit einer IT-Sicherheitsmaßnahme getroffen werden können. Betrachtet werde dazu die Entscheidung über die Einführung von Portsecurity in zugangsgesicherten Räumen. Folgende Eingangsgrößen und Parameter sind tendenziell in der Praxis leichter abzuschätzen und werden daher als bekannt angenommen: Laufzeit T=5 Jahre, Übertragbarkeitsquote IL_t=0%, Anfangsinvestition I_0 = 800.000 €, Auszahlungen für laufenden Betrieb und Wartung C_t =125.000 €, Opportunitätskostenzinssatz der Eigenkapitalunterlegung i_{opp}=8% sowie Kalkulationszinssatz i_{calc}=5%.
Für die nachfolgende Analyse unterschiedlicher Szenarien werde vereinfachend der Sicherheitslevel vor Einführung der Sicherheitsmaßnahme auf SL_0=90% gesetzt und der Sicherheitslevel nach Einführung der Sicherheitsmaßnahme auf SL_t = 99%, wobei auch der Sicherheitslevel prinzipiell variiert werden könnte. Abbildung 3 zeigt, dass die Entscheidungsempfehlung auf Basis des Kapitalwerts für die betrachteten Eingangsgrößen unterschiedlich ausfällt.

Abb. 3: Beispielhafte Analyse unterschiedlicher Szenarien

Erwartete Häufigkeit erfolgreicher Angriffe pro Jahr	Erwartete Häufigkeit versuchter Angriffe pro Jahr	Empfehlung: IT-Sicherheitsmaßnahme durchführen / Empfehlung: IT-Sicherheitsmaßnahme nicht durchführen		
0,10	10,00	NPV_0= -1.150.030 €	NPV_0= 570.366 €	NPV_0= 17.774.321 €
0,01	1,00	NPV_0= -1.319.690 €	NPV_0= -1.126.236 €	NPV_0= 808.300 €
0,001	0,1	NPV_0= -1.328.479 €	NPV_0= -1.214.125 €	NPV_0= -70.592 €
		40.000 €	400.000 €	4.000.000 €
		Durchschnittliche Schwere eines Schadensereignisses		

Die in Beispiel 1 aufgeführten Szenarien können als Ausgangspunkt für weitergehende Analysen dienen. So können einzelne Szenarien zusätzlich mit bekannten Wahrscheinlichkeiten belegt werden, um darauf eine Gesamtentscheidung zu stützen. Wir können Ergebnis 2 festhalten:

Ergebnis 2: Auch wenn die zugrunde liegenden Eingangsgrößen nur ungenau vorliegen, so können mit der Analyse unterschiedlicher Szenarien dennoch Aussagen über die Vorteilhaftigkeit von IT-Sicherheitsmaßnahmen getroffen werden.

Zugleich ist in der Praxis oftmals zu beobachten, dass Entscheider zwar unterschiedliche Szenarien analysieren, jedoch dann ihre Entscheidung auf Basis des Ergebnisses eines Szenarios treffen.

Die zur Berechnung des Kapitalwerts NPV_0 notwendigen Eingangsgrößen können zusätzlich auch für weitere Kennzahlen als alternative Entscheidungsgrundlage verwendet werden. So ist es möglich mit Hilfe der Eingangsgrößen auch statische Kennzahlen, wie bspw. den Return on Investment (ROI) oder die Amortisationsdauer sowie den Internen Zinssatz (IRR) - als weitere dynamische Bewertungsmethode neben der Kapitalwertmethode - zu berechnen. Letztere besitzt eine große Verbreitung in der Praxis, insbesondere in der IT-Projektbewertung.[36]

Im vorgestellten Modell wurde die Anfangsinvestition bislang nur zum Zeitpunkt t=0 betrachtet. In der Realität ist aber beobachtbar, dass Anfangsinvestition für IT-Sicherheitsmaßnahmen im Zeitablauf sinken können, zugleich aber die bereits zum Zeitpunkt t=0 bekannten erwarteten und unerwarteten Schäden steigen. Im folgenden Abschnitt III werden daher entsprechende zusätzliche Annahmen getroffen, um die Vorteilhaftigkeit einer IT-Sicherheitsmaßnahme zu unterschiedlichen Zeitpunkten zu untersuchen und so den optimalen Investitionszeitpunkt zu ermitteln.

III. Bewertung der Vorteilhaftigkeit einer Investition zu unterschiedlichen Zeitpunkten und Ermittlung des optimalen Investitionszeitpunkts

Im Folgenden soll der Entscheidungsraum erweitert werden und die Möglichkeit bestehen, nicht nur zum Zeitpunkt t=0, sondern jeweils zu jedem Zeitpunkt zwischen t=0 und t=T (d.h. für alle $t \in N_0$ und $0 \leq t < T$) einmalig zu investieren (bzw. nicht zu investieren). Die Investitionsentscheidung wird dabei weiterhin bezogen auf den Zeitpunkt t=0 betrachtet.
Mit dieser Erweiterung des Entscheidungsraums soll folgenden in der Realwelt zu beobachtenden Entwicklungen Rechnung getragen werden:

- IT-Sicherheitsmaßnahmen unterliegen oftmals einem kontinuierlichen Preisrückgang. Die im Folgenden formulierte Annahme A5 beruht auf dem Vorliegen von Skaleneffekten. Es wird davon ausgegangen, dass die Höhe der Anfangsinvestition für eine IT-Sicherheitsmaßnahme bei Implementierung zu einem späteren Zeitpunkt sinkt. Des Weiteren wird angenommen, dass auch zu späteren Zeitpunkten die zum Zeitpunkt t=0 verfügbare IT-Sicherheitsmaßnahme ebenso verfügbar ist, jedoch auf Grund des technologischen Fortschritts nur innerhalb des Zeithorizonts T (bis zur Ablösung durch eine neue Technologie) eingesetzt werden kann.
- Zugleich steigt, wie oben dargestellt, die Anzahl der Angriffe auf die IT von Unternehmungen. Daher wird eine periodig wachsende Häufigkeit erwarteter versuchter Angriffe $E(N_t)$ im Folgenden abgebildet.

Das Modell wird dazu um die Annahmen A5 und A6 erweitert, die eine dynamische Betrachtung von einer im Zeitablauf sinkenden Anfangsinvestition I_t und - aufgrund der Steigerung der erwarteten versuchten Angriffe $E(N_t)$ - zugleich steigenden Auszahlungen durch erwartete Schäden $E(L_t)$ sowie durch Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden OCC_t ermöglichen. Die Unternehmung sieht sich einem Trade-off gegenüber, welcher durch die Wahl des optimalen Investitionszeitpunkts y* zwischen den Zeitpunkten t=0 bis t=T-1 gelöst werden soll.

Im Einzelnen wird zur dynamischen Betrachtung einer im Zeitablauf sinkenden Anfangsinvestition Annahme A2 durch Annahme A5 erweitert.

A5 (Degressionsfaktor der Anfangsinvestition): Die Anfangsinvestition I_0 *kann nun zu jedem Zeitpunkt t innerhalb eines Gesamtbetrachtungshorizonts zwischen t=0 und t=T-1 geleistet werden. Die Anfangsinvestition wird fortan mit* I_t *beschrieben. Im Zeitablauf wird von einer Degression der Höhe der Anfangsinvestition* I_t *zum Zeitpunkt t mit einem bekannten Faktor* $(1-d)^t$ *(mit* $0 \leq d < 1$*) ausgegangen und es gilt:* $I_t = I_0 \cdot (1-d)^t$.[37]

Zur dynamischen Betrachtung im Zeitablauf steigender Auszahlungen durch erwartete Schäden $E(L_t)$ und durch Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden OCC_t werden die Annahmen A3 und A4 durch Annahme A6 erweitert.

A6 (Wachstumsfaktor der erwarteten Häufigkeit versuchter Angriffe): Die erwartete Häufigkeit versuchter Angriffe $E(N_0)$ *zum Zeitpunkt t=0 wird zum Zeitpunkt t mit dem bekannten Faktor* $(1+g)^t$ *(mit* $g \geq 0$*) multipliziert und es gilt:* $E(N_t) = (1 + g)^t \cdot E(N_0)$[38].

Aufgrund von Annahme (A6) betragen die erwarteten Schäden $E(L_t)$ für den Zeitpunkt t:

(17) $$E(L_t) = (1 - SL_t) \cdot E(N_t) \cdot (1 - IL_t) \cdot AV_t = (1 - SL_t) \cdot E(N_0) \cdot (1 + g)^t \cdot (1 - IL_t) \cdot AV_t.$$

Nach Implementierung zum Zeitpunkt y ermittelt sich die Reduktion der in den kommenden Zeitpunkten t>y nachschüssig anfallenden Auszahlungen durch erwartete Schäden $\Delta E(L_t)$ (mit t>y) wie folgt:

(18) $$\Delta E(L_t) = \Delta SL_t \cdot (1 + g)^t \cdot E(N_0) \cdot (1 - IL_t) \cdot AV_t \qquad (\text{mit } y<t<T).$$

Die Reduktion der Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden ΔOCC_t beträgt nach der Implementierung für t>y:[39]

(19) $$\Delta OCC_t = (i_{opp} \cdot \gamma_0 \cdot E(L_0)) - (i_{opp} \cdot \gamma_t \cdot E(L_t)) \text{ (mit } y<t\leq T).$$

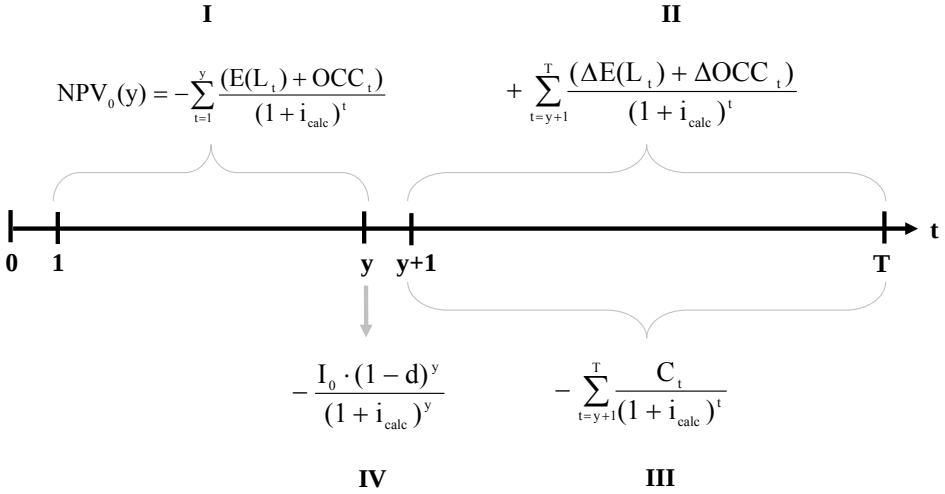
Als Zielfunktion ZF dient der Kapitalwert $NPV_0(y)$, der nach dem Investitionszeitpunkt y (mit $y \in N_0$ und $0 \leq y < T$) zu maximieren ist:

(20) $$ZF := \max_y NPV_0(y).$$

Für den Kapitalwert der IT-Sicherheitsmaßnahme $NPV_0(y)$ in Abhängigkeit zum Investitionszeitpunkt y gilt (21), wie in Abbildung 4 dargestellt:

Abb. 4: Berechnung des Kapitalwerts NPV_0 in Abhängigkeit zum Investitionszeitpunkt y

(21)



Wie aus Abbildung 4 ersichtlich wird, sinkt die Anfangsinvestition ceteris paribus je später der Investitionszeitpunkt y ist, zugleich steigen jedoch die erwarteten und unerwarteten Schäden (und somit die Opportunitätskosten einer Eigenkapitalunterlegung unerwarteter Schäden). Dies bedeutet auch, dass nach Implementierung der IT-Sicherheitsmaßnahme $\Delta E(L_t)$ und ΔOCC_t mit t höher werden, allerdings aufgrund der Begrenzung des Betrachtungshorizonts T der Kapitalwert aller $\Delta E(L_t)$ und ΔOCC_t geringer ausfällt.

Ergebnis 3: Anhand des in (21) angegebenen Kapitalwerts einer IT-Sicherheitsmaßnahme $NPV_0(y)$ kann die Vorteilhaftigkeit einer IT-Sicherheitsmaßnahme zu unterschiedlichen Investitionszeitpunkten y (mit $y \in N_0$ und $0 \leq y < T$) analysiert werden. Die Zielfunktion (21) beschreibt diskrete Investitionszeitpunkte y.[40] $NPV_0(y^*)$ bezeichne den höchsten Kapitalwert bei Betrachtung aller y. Es gilt folgende Empfehlung:

(22) Für $NPV_0(y^*) > 0$: Investition zum Zeitpunkt y^*,
Für $NPV_0(y^*) \leq 0$: Keine Investition.

Die Vorteilhaftigkeit einer IT-Sicherheitsmaßnahme kann sich im Zeitablauf ändern. So können Investitionen, die in t=0 nicht vorteilhaft sind, ggf. zu einem späteren Zeitpunkt vorteilhaft sein. Bereits zum Zeitpunkt t=0 vorteilhafte Maßnahmen können ggf. zu einem späteren Zeitpunkt mit einem noch höheren NPV_0 durchgeführt werden.

Anhang 2[41] illustriert diese Ergebnisse an einem Beispiel und zeigt insbesondere die Auswirkungen unterschiedlicher Annahmen bezüglich des Wachstumsfaktors g.

Im anschließenden Abschnitt IV werden zusätzlich Risiko- bzw. Budgetlimite berücksichtigt.

IV. Zusätzliche Berücksichtigung von Risiko- bzw. Budgetlimiten

Sollen zusätzlich Risiko- bzw. Budgetlimite auf den optimalen Investitionszeitpunkt betrachtet werden, so muss die Zielfunktion (21) unter Berücksichtigung der folgenden Nebenbedingungen maximiert werden:

- Risikolimit: Begrenztes Eigenkapital CC_{Limit} zur Deckung unerwarteter Schäden als Nebenbedingung NB1:

(23) NB1: $CC_{Limit} - CC_t \geq 0$

mit

CC_{Limit} = vorgegebenes Limit einer Eigenkapitalunterlegung für unerwartete Schäden.

Das Risikolimit CC_{Limit} drückt die Knappheit des Eigenkapitals aus, das nur begrenzt für eine Unterlegung von unerwarteten Schäden zur Verfügung steht.

- Budgetlimit: Begrenztes Budget I_{Limit} für Anfangsinvestition als Nebenbedingung NB2:

(24) NB2: $I_{Limit} - \left[I_0 \cdot (1-d)^y\right] \geq 0$

mit

I_{Limit} = vorgegebenes Budgetlimit für die Anfangsinvestition.

Die beiden Nebenbedingungen NB1 und NB2 wirken entgegengesetzt, d. h. während die Anfangsinvestition im Zeitablauf sinkt und somit der Erfüllung der Nebenbedingung näher rückt, steigen die erwarteten und unerwarteten Schäden an und nähern sich dem Risikolimit an. Sind die Nebenbedingungen NB1 und NB2 gleichzeitig verletzt, liegt ein Dilemma vor. Es kann auf Grund des Budgetlimits nach NB2 nicht investiert werden, obwohl das Risikolimit nach NB1 bereits überschritten wurde. Als Ausweg bleibt in dieser Situation, eines der beiden Limite zu erweitern. Ansonsten müsste das betroffene System deaktiviert werden, um das Risikolimit einzuhalten, dies hätte ggf. jedoch auch einen zusätzlichen Geschäftsverlust für die Unternehmung zur Folge, der bei einer solchen Entscheidung zusätzlich noch zu berücksichtigen wäre.

Muss aufgrund des Risikolimits zu einem Zeitpunkt y'< y* investiert werden, so entgeht dem Entscheider folgender Kapitalwert:[42]

(25)
$$NPV_0 = -\sum_{t=y'+1}^{y^*} \frac{(E(L_t) + OCC_t)}{(1+i_{calc})^t} + \sum_{t=y'+1}^{y^*} \frac{C_t}{(1+i_{calc})^t}$$
$$- \sum_{t=y'+1}^{y^*} \frac{(\Delta E(L_t) + \Delta OCC_t)}{(1+i_{calc})^t} + \frac{I_0 \cdot \left[(1-d)^{y'} - (1-d)^{y^*}\right]}{(1+i_{calc})^{y^*}}.$$

Dem Nachteil einer nicht weiter sinkenden Anfangsinvestition steht bei Investition zum Zeitpunkt y'<y* der Vorteil gegenüber, die erwarteten und unerwarteten Schäden ab einem früheren Zeitpunkt zu reduzieren.

Ergebnis 4: Bei Vorliegen von Risiko- bzw. Budgetlimiten als Nebenbedingungen NB1 bzw. NB2 kann der optimale Investitionszeitpunkt nur realisiert werden, wenn durch diesen keine der beiden Nebenbedingungen verletzt wird. So muss bei Erreichen des Risikolimits nach NB1 die Investition in die IT-Sicherheitsmaßnahme zu einem suboptimalen früheren Zeitpunkt erfolgen, während ein Budgetlimit nach NB2 zu einem suboptimalen späteren Zeit-

punkt führen kann. Ein Risikolimit als Nebenbedingung kann dazu führen, dass auch nicht vorteilhafte Investitionen mit einem Kapitalwert $NPV_0(y')<0$ durchgeführt werden müssen.[43]

Im Anhang 3[44] werden die Ausführungen zu Risikolimiten an einem Beispiel verdeutlicht.

Vor dem Hintergrund des Ergebnisses 4 erscheint es nahe liegend, bei geringfügigem Abweichen der vom Management vorgegebenen Risiko- und Budgetlimiten diese aus Perspektive der Gesamtunternehmung kritisch zu hinterfragen und ggf. anzupassen.

Die Ergebnisse dieses Beitrags werden im Folgenden zusammengefasst und Limitationen sowie weiterführende Forschungsfragen des Modells diskutiert.

E. Fazit und Ausblick

Das vorgestellte Modell wird von einem führenden, internationalen Finanzdienstleister zur Entscheidungsunterstützung über die Durchführung von IT-Sicherheitsmaßnahmen eingesetzt und wurde im Rahmen eines gemeinsamen Projekts mit dem Lehrstuhl WI-IF und dem Kernkompetenzzentrum IT&Finanzdienstleistungen an der Universität Augsburg sowie dem IIG - Abteilung Telematik an der Universität Freiburg von den Autoren entwickelt. Mit dem Modell kann die Vorteilhaftigkeit von IT-Sicherheitsmaßnahmen zu unterschiedlichen Zeitpunkten bewertet werden. Die Vorteilhaftigkeit wird dazu auf Basis der Kapitalwertmethode unter Berücksichtigung der Reduktion der erwarteten Schäden $\Delta E(L_t)$ und der Reduktion der Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden ΔOCC_t einerseits sowie der Anfangsinvestition I_0 und den laufenden Auszahlungen für Betrieb und Wartung C_t andererseits ermittelt. Im Modell wird eine Reihe von Parametern als bekannt vorausgesetzt bzw. ist bei dessen Anwendung anhand historischer Daten oder Experteninterviews abzuschätzen. Erfahrungen des Finanzdienstleisters beim praktischen Einsatz belegen, dass insbesondere die Häufigkeit und Schwere von - durch IT-Sicherheitsmaßnahmen zukünftig verhinderten - Schadensereignissen i. d. R. nur sehr ungenau angegeben werden können. Mit der Analyse unterschiedlicher Szenarien können trotz ungenauer Eingabewerte für die reduzierte Häufigkeit und Schwere von Schadensereignissen dennoch Aussagen über die Vorteilhaftigkeit von IT-Sicherheitsmaßnahmen getroffen und damit Entscheidungen über deren Durchführung unterstützt werden.

Zudem sind oftmals wachsende erwartete und unerwartete Schäden sowie sinkende Anfangsinvestitionen für IT-Sicherheitsmaßnahmen zu beobachten. Daher ist die Vorteilhaftigkeit von

IT-Sicherheitsmaßnahmen im Zeitablauf zu bewerten und der optimale Investitionszeitpunkt zu bestimmen. Dabei kann es je nach Eingangsgrößen vorteilhaft sein, eine Investition zu verschieben, sofern der Kapitalwert NPV_0 einer Investition in eine IT-Sicherheitsmaßnahme in der Zukunft höher ist als zum Zeitpunkt t=0. Zusätzlich wurden im Modell Risiko- bzw. Budgetlimite als Nebenbedingungen berücksichtigt und deren Auswirkungen analysiert. Die Berücksichtigung von Risikolimiten dürfte bei einer im Zeitablauf steigenden Anzahl von Angriffen zu einem früheren Investitionszeitpunkt führen, während Budgetlimite als Nebenbedingung die Realisierung von Maßnahmen verzögern und ggf. verhindern können.
Das Modell besitzt folgende Limitationen, die zugleich weiterführende Forschungsfragen aufwerfen:

- Die Überführung der erwarteten Schäden in unerwartete Schäden anhand des Gamma-Faktors für die poissonverteilte Häufigkeit von Schadensereignissen ist lediglich eine Approximation. Die Höhe der unerwarteten Schäden und damit der Eigenkapitalunterlegung wird auf Grund der Annahme durchschnittlicher Schwere von Schadensereignissen unterschätzt. Die gleichzeitige Modellierung der Verteilung von Häufigkeit und Schwere würde die Anwendung von Simulationsverfahren erforderlich machen. Eine Anwendung von Simulationsverfahren dürfte jedoch in der Regel aufgrund einer - für Simulationsverfahren - nicht ausreichenden Anzahl von historischen Daten zur Einzelprojektbewertung nicht umsetzbar sein. Durch die gewählte Vorgehensweise wird die Reduktion der Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden unterschätzt und somit auch die Vorteilhaftigkeit des Projekts.
- Die Abbildung wechselseitiger Beziehungen zwischen unterschiedlichen IT-Sicherheitsmaßnahmen bzw. unterschiedlichen Vermögenswerten wirft weitere Forschungsfragen auf. Die Modellierung komplexer stochastischer Abhängigkeiten von Vermögenswerten und Maßnahmenbündeln kann bspw. mit Hilfe von Copula-Funktionen erreicht werden.
- Budgetlimite für Betrieb und Wartung wurden im Modell vernachlässigt. Eine Betrachtung derartiger Limite kann weitere Auswirkungen auf den Lösungsraum und somit die mögliche Implementierbarkeit von IT-Sicherheitsmaßnahmen besitzen.

Für die Steuerung von IT-Sicherheitsrisiken ist eine integrierte Betrachtung der Einzahlungen durch Reduktion der erwarteten Schäden zzgl. der Reduktion der Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden einerseits und der Auszahlungen für Anfangsinvestition und laufenden Betrieb und Wartung aufgrund der IT-Sicherheitsmaßnahme andererseits notwendig. Weiterhin wird durch eine dynamische Betrachtung des optimalen

Investitionszeitpunkts auf Basis von wachsenden erwarteten und unerwarteten Schäden einerseits und einer sinkenden Anfangsinvestition andererseits den aktuellen Entwicklungen in der Praxis Rechnung getragen. Auf Grundlage des Modells kann eine Entscheidungsunterstützung über die Vorteilhaftigkeit von IT-Sicherheitsmaßnahmen zu unterschiedlichen Zeitpunkten erfolgen und der optimale Investitionszeitpunkt bestimmt werden. Schließlich besteht weiterer Forschungsbedarf in der empirischen Untersuchung und Überprüfung der Modellergebnisse. Weiterhin kann das vorgestellte Modell auch in anderen Bereichen des Operational Risk Managements Anwendung finden, so bspw. bei der Bewertung von Maßnahmen zur Sicherstellung des Geschäftsbetriebs (Business Continuity Management).[45]

Literatur

Alexander, C. (2003): Statistical models of operational loss, in: Alexander, C. (Hrsg.): Operational Risk – Regulation, Analysis and Management, Prentice Hall, London.

Anders, U. (2001): Qualitative Anforderungen an das Management operativer Risiken, in: Die Bank, Nr. 5.

Basel Committee on Banking Supervision (2003): The 2002 Loss Data Collection Exercise for Operational Risk: Summary of the Data collected, http://www.bis.org/bcbs/qis/ldce2002.pdf. Abruf am: 2005-03-04.

Basel Committee on Banking Supervision (2001): Working Paper on the Regulatory Treatment of Operational Risk, http://www.bis.org/publ/bcbs_wp8.pdf. Abruf am: 2005-03-05.

Beeck, H./Kaiser, T. (2000): Quantifizierung von Operational Risk, in: *Johannig, L./ Rudolph, B.* (Hrsg.): Handbuch Risikomanagement Band 2. Uhlenbruch Verlag, Bad Soden/Ts., S. 633-654.

Brauers, J./Weber, M. (1986): Szenarioanalyse als Hilfsmittel der strategischen Planung: Methodenvergleich und Darstellung einer neuen Methode, in: Zeitschrift für Betriebswirtschaft, 56. Jg, H. 7, S. 631-652.

Brink, J. van den (2000): Operational Risk: Wie Banken das Betriebsrisiko beherrschen. Dissertation, St. Gallen.

Buhr, R. (2000): Messung von Betriebsrisiken – ein methodischer Ansatz, in: Die Bank, Nr. 3, S. 202-206.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2006): IT-Grundschutzhandbuch, http://www.bsi.de/gshb/deutsch/index.htm, Abruf am 2006-03-03.

CERT (2005): CERT/CC Statistics 1988-2005, http://www.cert.org/stats/#vulnerabilities, Abruf am 2005-11-30.

Chavez-Demoulin, V./Embrechts, P./Neslehová, J. (2005): Quantitative Models for Operational Risk: Extremes, Dependence and Aggregation, http://www.math.ethz.ch/%7Ebaltes/ftp/manuscript_cen.pdf. Abruf am: 2005-03-03.

Cruz, M.G. (2002): Modeling, Measuring and Hedging Operational Risk. John Wiley & Sons.

Ebnöther, S./Vanini, P./ McNeil, A./Antolinez-Fehr, P. (2001): Modelling Operational Risk, http://www.math.ethz.ch/~mcneil/ftp/operational.pdf. Abruf am: 2005-03-03.

Eckert, C. (2004): IT-Sicherheit: Konzepte, Verfahren, Kontrolle. Oldenbourg Verlag, München.

Eller, R./Gruber, W./Reif, M. (2002): Handbuch Operationelle Risiken. Schäffer-Poeschel Verlag, Stuttgart.

Faisst, U. (2004): Ein Modell zur Steuerung operationeller Risiken in IT-unterstützten Bankprozessen, in: Banking and Information Technologie (BIT) – Sonderheft zur Multikonferenz Wirtschaftsinformatik 2004 in Essen, 1, S. 35-50.

Faisst, U./Kovacs, M. (2003): Quantifizierung operationeller Risiken – ein Methodenvergleich, in: Die Bank, Nr. 5, S. 342-349.

Faisst, U./Prokein, O. (2005): An Optimization Model for the Management of Security Risks in Banking Companies, in: *Müller, G., Lin, K.-J.* (Hrsg.): Proceedings of the 7th IEEE International Conference on E-Commmerce Technology (CEC) 2005, München, Juli 2005, IEEE Computer Society Press, Los Alamitos, CA, 2005, S.266-273.

Fontnouvelle, P. de/DeJesus-Rueff, V./Jordan, J./Rosengren, E. de (2003): Using Loss Data to Quantify Operational Risk, http://www.bis.org/bcbs/events/wkshop0303/p04deforose.pdf. Abruf am: 2006-03-03.

Fontnouvelle, P./Rosengren, E. de (2004): Implications of Alternative Operational Risk Modeling Techniques, http://www.nber.org/books/risk/deFontnouvelle-jordan3-22-5.pdf. Abruf am: 2005 -03-03.

Franke, G./Hax, H. (2003): Finanzwirtschaft des Unternehmens und Kapitalmarkt, 5. Auflage, Springer Verlag, Berlin et al.

Füser, K./Rödel, K./Kang, D. (2002): Identifizierung und Quantifizierung von „Operational Risk“, in: FinanzBetrieb, Nr. 9, S. 495-502.

Gordon, L./Loeb, M. (2006): Budgeting Process for Information Security Expenditures, in: Communications of the ACM, Vol. 49, No. 1, S. 121-125.

Gordon, L./Loeb, M. (2002): The Economics of Information Security Investment, in: ACM Transactions on Information Systems and Security, Vol. 5, No. 4, S. 438-457.

Gordon, L./Loeb, M./Lucyshyn, W./Richardson, R. (2005): 2005 CSI/FBI Computer Crime and Security Survey, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf, Abruf am 2005-10-24.

Grzebiela, T. (2002): Internet-Risiken: Versicherbarkeit und Alternativer Risikotransfer. Deutscher Universitätsverlag, Wiesbaden.

Hölscher, R. (2002): Von der Versicherung zur integrativen Risikobewältigung: Die Konzeption eines modernen Risikomanagements, in: *Hölscher, R./Elfgen, R.*: Herausforderung Risikomanagement, Gabler-Verlag, Wiesbaden, S. 3-31.

Hoffman, D.G. (2002): Managing Operational Risk. John Wiley & Sons.

Hostettler, S. (1997): Das Konzept des Economic Value Added (EVA), Paul Haupt Verlag, Bern.

Jörg, M. (2002): Operational Risk – Herausforderung bei der Implementierung von Basel II. Diskussionsbeiträge zur Bankbetriebslehre, Hochschule für Bankwirtschaft, Frankfurt.

Kappler, E./Rehkugler, H. (1991): Kapitalwirtschaft, in: *Heine, E.* (Hrsg.): Industriebetriebslehre. 9. Auflage, Gabler-Verlag, Wiesbaden, S. 897-1068.

Locarek-Junge, H./Hengmith, L. (2003): Management des operationellen Risikos der Informationswirtschaft in Banken, in: *Geyer-Schulz, A./Taudes, A.* (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft – Symposium. GI-Edition Lecture Notes in Informatics, Wien, September 2003. Band, Köllen Druck + Verlag, Bonn.

Marshall, C.L. (2001): Measuring and Managing Operational Risk in Financial Institutions. John Wiley & Sons.

Müller, G./Rannenberg, K. (1999): Multilateral Security in Communications, Vol. 3: Technology, Infrastructure, Economy, Addison-Wesley-Longman, New York.

Müller, G./Eymann, T./Kreutzer, M. (2003): Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft. Oldenbourg Verlag, München.

Perridon, L./Steiner, M. (2002): Finanzwirtschaft der Unternehmung, 11. Auflage, Verlag Vahlen, München.

Peter, A./Vogt, H.-J./Kraß, V. (2000): Management operationeller Risiken bei Finanz dienstleister, in: *Johannig, L./Rudolph, B.* (Hrsg.): Handbuch Risikomanagement Band 2. Uhlenbruch Verlag, Bad Soden/Ts., S. 655-677.

Piaz, J.-M. (2001): Operational Risk Management bei Banken, Versus Verlag, Zürich.

Rannenberg, K. (1998): Zertifizierung Mehrseitiger Sicherheit: Kriterien und organisatorische Rahmenbedingungen, Vieweg-Verlag, Braunschweig, Wiesbaden.

Schierenbeck, H. (2001): Ertragsorientiertes Bankmanagement – Band 2: Risiko-Controlling und integrierte Rendite-/Risikosteuerung. 7. Aufl., Gabler-Verlag, Wiesbaden.

Schneier, B. (2001): Secrets & lies. IT-Sicherheit in der vernetzten Welt. dpunkt-Verlag GmbH, Heidelberg.

Sonnenreich, W. (2005): Return On Security Investment (ROSI): A Practical Quantitative Model, http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf, Abruf am 2005-10-24.

Spahr, R. (2001): Steuerung operationeller Risiken im Electronic und Investment Banking, in: Die Bank, Nr. 9.

Tödtmann, C. (2005): Wo Vorstand draufsteht, ist Haftung drin, in: Handelsblatt vom 18.12.2005, Rubrik Karriere&Management, S. 6.

Wiedemann, A. (2004): Risikotriade Zins-, Kredit- und operationelle Risiken. Bankakademie Verlag, Frankfurt.

Willinsky, C. (2001): Wert- und risikoorientierte Steuerung dezentraler Einheiten von Banken, Botermann & Botermann Verlag, Köln.

Zusammenfassung

Das vorgestellte Modell dient zur Entscheidungsunterstützung über die Durchführung von IT-Sicherheitsmaßnahmen und wird von einem führenden, internationalen Finanzdienstleister bereits eingesetzt. IT-Sicherheitsmaßnahmen werden dazu auf Basis der Kapitalwertmethode unter Berücksichtigung der Reduktion der erwarteten Schäden und der Reduktion der Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden in Form von Einzahlungen, sowie anhand der Anfangsinvestition und den zusätzlichen laufenden Kosten für Betrieb und Wartung in Form von Auszahlungen bewertet. Darüber hinaus wird - unter der Annahme von periodig steigenden erwarteten und unerwarteten Schäden sowie einer periodig sinkenden Anfangsinvestition - die Vorteilhaftigkeit von IT-Sicherheitsmaßnahmen zu unterschiedlichen Zeitpunkten untersucht und daraus der optimale Investitionszeitpunkt ermittelt. Schließlich werden Auswirkungen von Risiko- bzw. Budgetlimiten untersucht.

Summary

The model presented serves to support decisions on the implementation of IT security measures and is already deployed at a leading international financial services company. IT security investments are analysed using the net present value method taking account of the reduction in expected losses and the reduction in opportunity costs of capital charge for unexpected losses in the form of cash inflows. The analysis is also performed on the basis of the initial investment amount and the additional recurring maintenance and running costs in the form of cash outflows. Assuming that expected as well as unexpected losses periodically increase and the investment amount periodically decreases, the effectiveness of IT security investments at various investment dates is examined and the optimal investment date determined. Finally, the impacts of risk limits and budget limits are evaluated.

JEL: D81, G31

Danksagung

Die Autoren danken Herrn Prof. Dr. Armin Heinzl sowie drei anonymen Gutachtern für ihre konstruktiven Anmerkungen und die Unterstützung im Begutachtungsverfahren sowie Herrn Prof. Dr. Günter Bamberg, Prof. Dr. Hans Ulrich Buhl und Prof. Dr. Günter Müller für zahlreiche Anregungen im Entstehungsprozess dieses Beitrags.

Anmerkungen

[1] Vgl. *CERT* (2005). Das CERT hat eine Statistik bzgl. der gemeldeten Zwischenfälle bis zum Jahr 2003 im Internet veröffentlicht (URL: http://www.cert.org/stats/cert_stats.html). Für die Jahre 2004 bis 2006 wurde eine Extrapolation auf Basis des Durchschnitts der Wachstumsfaktoren von 1999 bis 2003 vorgenommen.

[2] Insbesondere vor dem Hintergrund, dass Vorstände und Geschäftsführer für IT-Sicherheitsrisiken haftbar sind, werden oftmals zu hohe Investitionen in IT-Sicherheitsmaßnahmen getätigt. Für eine Übersicht der Rechtslage vgl. bspw. *Tödtmann* (2005).

[3] Vgl. *Piaz* (2001).

[4] Vgl. *Müller/Rannenberg* (1999).

[5] Vgl. *Müller/Rannenberg* (1999) und *Rannenberg* (1998).

[6] Vgl. *Bundesamt für Sicherheit in der Informationstechnik (BSI)* (2006).

[7] Vgl. *Faisst/Kovacs* (2003).

[8] Vgl. *Faisst/Kovacs* (2003).

[9] Vgl. *Peter/Vogt/Kraß* (2000).

[10] Eigene Darstellung in Anlehnung an *Faisst* (2004). Alternativ könnte man die Steuerungsinstrumente auch nach folgenden Kategorien aufteilen: Risikovermeidung, Risikoverminderung, Risikodiversifikation, Risikotransfer und Risikovorsorge (vgl. *Hölscher, R.* (2002) und *Schierenbeck, H.* (2001)).

[11] Vgl. *Piaz* (2001).

[12] Auszahlungen im Sinne entgangener Einzahlungen, da das zu unterlegende Eigenkapital nicht mehr für andere risikobehaftete Geschäfte zur Verfügung steht.

[13] Der Trade-off zwischen der Höhe der Auszahlungen für IT-Sicherheitsmaßnahmen einerseits und der Auszahlungen für erwartete Schäden andererseits wurde bspw. auch von *Gordon/Loeb* (2002) in einem einperiodigen Modell dargestellt. Allerdings berücksichtigt

dieses Modell im Gegensatz zu *Faisst* (2004) keine Auszahlungen für die Opportunitätskosten der Eigenkapitalunterlegung für unerwartete Schäden.

[14] Vgl. Abschnitt C.I. zu den Anforderungen an eine Methode zur Bewertung von IT-Sicherheitsmaßnahmen.

[15] Vgl. *Hölscher* (2002). Bei der ex-post Analyse muss jedoch berücksichtigt werden, dass die Reduktion der Häufigkeit von Schadensereignissen i.d.R. eine stochastische Größe ist. Es kann jedoch untersucht werden, inwieweit die ex-ante angenommenen Erwartungswerte von (mehreren) ex-post Realisationen abweichen und diese daher in Frage zu stellen sind.

[16] Vgl. *Schierenbeck* (2001).

[17] Werden die erwarteten Schäden nicht bei der Mindestmargenkalkulation berücksichtigt, so muss auch für die erwarteten Schäden Eigenkapital unterlegt werden.

[18] Vgl. *Perridon/Steiner* (2002).

[19] Vgl. *Sonnenreich* (2005).

[20] Vgl. *Perridon/Steiner* (2002).

[21] Vgl. *Willinsky* (2001).

[22] Vgl. *Hostettler* (1997).

[23] Vgl. *Kappler/Rehkugler* (1991).

[24] Vgl. *Kappler/Rehkugler* (1991).

[25] Die Schutzziele des Konzepts der Mehrseitigen Sicherheit beschreiben den angestrebten Sicherheitszustand einer Unternehmung bzw. eines Vermögensgegenstandes und können durch Bedrohungen verletzt werden. Um eine solche Bedrohung umzusetzen, muss ein Angreifer einen konkreten Angriff durchführen. Dabei wird meist eine Schwachstelle des IT-Systems ausgenutzt.

[26] Für zum Entscheidungszeitpunkt t=0 unbekannte Angriffszenarien existieren i.d.R. keine IT-Sicherheitsmaßnahmen (vgl. *Schneier* (2001)), die bewertet werden könnten.

[27] Diese fallen zusätzlich zu Auszahlungen bereits bestehender IT-Sicherheitsmaßnahmen an.

[28] Bewertet werden die - durch die zu bewertende zusätzliche IT-Sicherheitsmaßnahme bewirkte - Reduktion der erwarteten Schäden sowie die Reduktion der Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden, sofern diese der betrachteten IT-Sicherheitsmaßnahme direkt zugeordnet werden können. Die verminderten Auszahlungen in Form von $\Delta E(L_t)$ und ΔOCC_t werden als Einzahlungen aufgefasst.

[29] Als Basis des Modells dienen Zahlungsströme, da diese im Vergleich zu buchhalterischen Größen bewertungsunabhängig und somit als objektive Entscheidungsgrundlage geeignet sind. Vgl. hierzu *Franke/Hax* (2003).

[30] Die von t abhängigen Eingangsgrößen können für jeden Zeitpunkt t unterschiedliche Werte annehmen.

[31] Bei Annahme einer nicht-flachen Zinsstrukturkurve können die Zahlungsüberschüsse der Laufzeit T zu den Zeitpunkten t=0 bis t=T auf den Zeitpunkt t=0 mit dem risikolosen Zinssatz $i_{calc,p}$ (jeweils für die Perioden p □ N mit 1≤p≤T zwischen den Zeitpunkten t=p-1 und t=p) diskontiert werden. Der Kapitalwert berechnet sich dann wie folgt: $NPV_0 = -I_0 + \sum_{t=1}^{T} \frac{\Delta E(L_t) + \Delta OCC_t - C_t}{\prod_{p=1}^{t} \left(1 + i_{calc,p}\right)}$. Von dieser Erweiterung wird zur Vereinfachung im Folgenden abgesehen. Da bereits ein Risikoabschlag im Zähler (in Form der Opportunitätskosten der Eigenkapitalunterlegung für unerwartete Verluste) vorgenommen wird, würde ein weiterer Risikozuschlag (bspw. durch den WACC) im Nenner eine unzulässige Vermischung von Risikoabschlags- und Risikozuschlagsmethode bedeuten. Daher wird ein risikoloser Zinssatz angewendet.

[32] Der Sicherheitslevel beschreibt somit die Leistungsfähigkeit einer IT-Sicherheitsmaßnahme. Denkbar wäre, dass Angreifer über den Zeitablauf Möglichkeiten finden, eine bestehende IT-Sicherheitsmaßnahme zu überlisten. Der Sicherheitslevel sinkt ab diesem Zeitpunkt auf ein niedriges Niveau; im Extremfall kann die IT-Sicherheitsmaßnahme dem Angriff nicht mehr entgegenwirken. In diesem Fall würde der Sicherheitslevel den Wert Null annehmen.

[33] Bei der Ermittlung der Eigenkapitalunterlegung wird davon ausgegangen, dass erwartete Schäden bereits in der betrachteten Periode budgetiert wurden. Ist dies nicht der Fall, müssen diese ebenfalls mit Eigenkapital unterlegt werden.

[34] Der Anhang 1 steht im Internet unter http://www.wi-if.de/publikationen zur Verfügung.

[35] Die in Beispiel 1 aufgeführte Analyse unterschiedlicher Szenarien kann durch die Anwendung verschiedener Verfahren erweitert werden, indem den einzelnen Szenarien gemäß ihrer Bedeutung Wahrscheinlichkeiten zugeordnet werden (*Brauers/Weber* (1986)).

[36] Vgl. *Gordon/Loeb/Lucyshyn/Richardson* (2005).

[37] Vereinfachend wird d als konstant angenommen. Weiterhin wäre ein d_t denkbar, das zu jedem Zeitpunkt t angepasst werden kann.

[38] Ebenso vereinfachend wird g als konstant angenommen. Weiterhin wäre ein g_t denkbar, das zu jedem Zeitpunkt t angepasst werden kann.

[39] Bei der Ermittlung der Opportunitätskosten einer Eigenkapitalunterlegung unerwarteter Schäden erweitert sich die Formel zur Berechnung des Gamma-Faktors (siehe Anhang 3) wie folgt: $E(Q_t)=E(N_0) \cdot (1 + g)^t \cdot (1-SL_t)$.

[40] Eine stetige Darstellung der Zielfunktion nach y kann nicht erfolgen, da der tabellierte Gamma-Faktor zur Bestimmung der unerwarteten Schäden zwangsläufig zu Sprungstellen in (21) führt. Die Zielfunktion (21) ist daher nicht stetig differenzierbar. Das Optimum der Zielfunktion nach dem Investitionszeitpunkt y kann jedoch durch Enumeration bestimmt werden. Ein solches enumeratives Vorgehen scheint aufgrund der i. d. R. geringen Anzahl von betrachteten möglichen Investitionszeitpunkten durchaus praktikabel.

[41] Der Anhang 2 steht im Internet unter http://www.wi-if.de/publikationen zur Verfügung.

[42] Bei Investition zu einem Zeitpunkt y'>y* aufgrund eines Budgetlimits kann der Kapitalwert analog ermittelt werden.

[43] Anders als bei Risikolimiten werden bei Vorliegen von Budgetlimiten jedoch keine nicht vorteilhaften Investitionen mit einem Kapitalwert $NPV_0(y')<0$ empfohlen.

[44] Der Anhang 3 steht im Internet unter http://www.wi-if.de/publikationen zur Verfügung.

[45] So z. B. allgemeine Notfallpläne, Gebäudesicherungen etc.

Anhang 1: Bestimmung des Gamma-Faktors

Der in diesem Modell angewandte vereinfachte Ansatz zur Ermittlung der unerwarteten Schäden geht von einer poissonverteilten Häufigkeit Q mit E(Q)= E(N)·(1-SL) der Schadensereignisse aus (vgl. Annahme A3.2).

Es gilt nach *Alexander* (2003):

(a) $CC = \gamma \cdot E(Q) \cdot (1\text{-}IL) \cdot AV$ sowie

(b) $CC = L^{0,999} - E(L)$

mit

CC = Ökonomische Eigenkapitalunterlegung

$L^{0,999}$ = 99,9%-Quantil

E(L) = Erwartungswert der Schadensverteilung L.

Setzt man (a) und (b) gleich und löst nach γ auf, erhält man

(c) $$\gamma = \frac{L^{0,999} - E(L)}{E(Q) \cdot LGE} = \frac{L^{0,999} - E(L)}{E(L)} = \frac{Q^{0,999} - E(Q)}{E(Q)}$$

Es gilt folgende Tabelle 4 nach *Alexander* (2003):

Tab. 4: Übersicht γ/δ-Werte in Abhängigkeit von der erwarteten Häufigkeit E(Q)

E(Q)	100	50	40	30	20	10
$Q^{0,999}$	131.805	72.751	60.452	47.812	34.714	20.662
δ	3.180	3.218	3.234	3.252	3.290	3.372
γ	0.318	0.455	0.511	0.594	0.736	1.066
E(Q)	8	6	5	4	3	2
$Q^{0,999}$	17.630	14.449	12.771	10.956	9.127	7.113
δ	3.405	3.449	3.475	3.478	3.537	3.615
γ	1.204	1.408	1.554	1.739	2.042	2.556
E(Q)	1	0.9	0.8	0.7	0.6	0.5
$Q^{0,999}$	4.868	4.551	4.234	3.914	3.584	3.255
δ	3.868	3.848	3.839	3.841	3.853	3.896
γ	3.868	4.056	4.292	4.591	4.974	5.510
E(Q)	0.4	0.3	0.2	0.1	0.05	0.01
$Q^{0,999}$	2.908	2.490	2.072	1.421	1.065	0.904
δ	3.965	3.998	4.187	4.176	4.541	8.940
γ	6.269	7.300	9.362	13.205	20.306	89.401

Anmerkung: $Q^{0,999}$ ist das 99,9 % Quantil der Verteilung Q.

Anhang 2: Vorteilhaftigkeit einer Investition zu unterschiedlichen Zeitpunkten und Ermittlung des optimalen Investitionszeitpunkts

Beispiel 2 (Fortsetzung Beispiel 1):

Wie in Beispiel 1, wird die Entscheidung zum Zeitpunkt t=0 über die Einführung von Portsecurity in zugangsgesicherten Räumen zu den Zeitpunkten t (mit $0 \leq t < T$ innerhalb eines Betrachtungszeitraums von T=5 Jahren) betrachtet. Der Wachstumsfaktor g beträgt g=75%, der Degressionsfaktor d hat den Wert d=25%. Alle weiteren Inputparameter entsprechen denen des Beispiels 1. Berechnet man die jeweiligen Kapitalwerte einer Investition zu den Zeitpunkten y=0 bis y=4, so erhält man folgendes Ergebnis (Tabelle 5):

Tab. 5: Kapitalwerte bei unterschiedlichen Investitionszeitpunkten y

y	0	1	2	3	4
NPV_0	-317.249 €	-76.541 €	50.665 €	**53.575 €**	-103.695 €

Der optimale Investitionszeitpunkt ist y*=3, da der Kapitalwert bei dieser Alternative am höchsten ist. Anhand der Analyse unterschiedlicher Wachstumsfaktoren g kann aufgezeigt werden, dass bei anderen Eingangswerten es ggf. zu einer anderen Entscheidungsempfehlung kommen kann. Die Auswirkungen unterschiedlich hoch angenommener Wachstumsraten auf die Vorteilhaftigkeit von IT-Sicherheitsmaßnahmen und den optimalen Investitionszeitpunkt stellt Tabelle 6 dar:

Tab. 6: Kapitalwerte bei unterschiedlichen Wachstumsfaktoren g

Y	0	1	2	3	4
NPV_0 mit g=75%	-317.249 €	-76.541 €	50.665 €	**53.575 €**	-103.695 €
NPV_0 mit g=156%	3.711.778 €	3.921.629 €	**3.922.173 €**	3.530.557 €	2.268.537 €
NPV_0 mit g=168%	4.820.955 €	**5.026.235 €**	5.003.966 €	4.526.947 €	2.980.693 €

Bei höheren Wachstumsraten wird der optimale Investitionszeitpunkt y* tendenziell früher erreicht. Die Wachstumsraten verdeutlichen, dass auch bei geringen erwarteten versuchten Angriffen zum Zeitpunkt t=0 $E(N_0)$ durch den in der Praxis beobachtbaren exponentiellen Anstieg eine Investition in eine IT-Sicherheitsmaßnahme zu einem späteren Zeitpunkt vorteilhaft sein kann.

Anhang 3: Zusätzliche Berücksichtigung eines Risikolimits

Beispiel 3 (Forts. Beispiel 2):

Betrachtet wird die Entscheidung zum Zeitpunkt t=0 über die Einführung von Portsecurity in zugangsgesicherten Räumen zum Zeitpunkt $t \geq 0$. Der Wachstumsfaktor beträgt g=200%, das Risikolimit CC_{Limit} = 600.000 €. Alle anderen Inputparameter entsprechen denen der Ausgangssituation in Beispiel 2.

Tab. 7: Eigenkapitalunterlegung für unerwartete Schäden CC_t bei Investition in y

y	0	1	2	3	4
CC_t	528.200 €	658.392 €	731.016 €	1.011.096 €	1.390.608 €

Wie Tabelle 7 illustriert, muss in t=0 investiert werden, da nach Ablauf von einem Jahr $CC_1 > CC_{Limit}$ wäre. Somit kann die optimale Lösung y*=1 nicht realisiert werden und es wird zum suboptimalen früheren Zeitpunkt y'=0 investiert. Dem Entscheider entgeht somit ein Kapitalwert NPV0=193.090 €.