Konzeption eines Modells zur Bestimmung des optimalen Investitionsbeitrags in IT-Sicherheits- bzw. IT-Notfallmaßnahmen unter Berücksichtigung Compliance-bedingter Anforderungen

Stefan Alexander Kronschnabl

ibi research an der Universität Regensburg GmbH

1 Ausgangslage, Problemstellung und Zielsetzung

Da die IT immense Bedeutung für nahezu sämtliche Geschäftsprozesse hat, muss diese durch geeignete Sicherheits- und Notfallmaßnahmen abgesichert werden (Kronschnabl 2008, S. 3). Hierbei gilt es eine Vielzahl relevanter rechtlicher und aufsichtsrechtlicher Rahmenbedingungen zu berücksichtigen. Beispielhaft aufgeführt seien hier aus nationaler Sicht das Kreditwesengesetz §25a, das Aktiengesetz §92 oder die Mindestanforderungen an das Risikomanagement (MaRisk) des Bundesamtes für Finanzdienstleistungsaufsicht (BaFin). International ist beispielsweise der Payment Card Industry Data Security Standard (PCI DSS) oder der Sarbanes Oxley Act (SOX) zu berücksichtigen. Neben allgemeinen, prinzipienbasierten Forderungen an ein angemessenes und der wirtschaftlichen Situation des Unternehmens angepasstes IT-Sicherheits-, IT-Risiko- und IT-Notfallmanagement werden hierdurch auch konkrete Anforderungen definiert. So fordern beispielsweise die MaRisk die Ausgestaltung der IT nach gängigen Best Practice Standards, wie z. B. ISO 27001/2 oder IT-Grundschutz (BaFin 2009, AT 7.2), sowie ein Notfallmanagement welches sicherstellt, dass die im Notfallkonzept festgelegten Maßnahmen erwiesener Maßen dazu geeignet sein müssen, das Ausmaß möglicher Schäden zu reduzieren. (BaFin 2009, AT 7.3).

Genau in dieser Bestimmung der Angemessenheit liegt jedoch die Problematik. Aufgrund eines in der Regel begrenzten Budgets gilt es je nach Bedeutung und monetärem Wert des Geschäftsprozesses und erwarteten Ausfallwahrscheinlichkeiten geeignete Absicherungs- und Notfallmaßnahmen zu treffen. Hinzu kommt, dass aufgrund der Wirtschaftskrise die IT-Investitionen aktuell rückläufig sind (Deloitte 2009).

Das IT-Risikomanagement kann hierzu einen wichtigen Beitrag leisten. Ziel ist es IT-Risiken nicht nur zu identifizieren, sondern auch zu überprüfen, ob eine Investition aufgrund eines Risikos überhaupt monetär sinnvoll ist. Zudem muss

eine Priorisierung von Maßnahmen erfolgen, die mit dem gegebenen Budget die Risiken am besten abdecken. Relevante Parameter hierbei sind die Effizienz der Maßnahme, die Angriffshäufigkeit sowie die Schadenshöhe (Gordon/Loeb 2002; Sonnenreich et al. 2006; Soo Hoo 2000). Ziel ist es diesbezüglich ein Modell zu konzipieren, welches eine aussagefähige Net Present Value (NPV) Verteilung möglicher Maßnahmen liefert. Hierdurch soll ein Beitrag geschaffen werden, den eingangs zitierten Anforderungen aus den MaRisk und der resultierenden Problemstellung gerecht zu werden.

2 Forschungsgrundlage

2.1 Kurzanalyse exemplarisch ausgewählter Modelle

Zur Konzeption eines Modells zur Bestimmung des optimalen Investitionsbeitrags in IT-Sicherheit- bzw. IT-Notfallmaßnahmen wurden relevante Modelle in Wissenschaft und Praxis ausgewählt und analysiert. Aufgrund des beschränkten Seitenumfangs dieses Beitrags wird auf eine detaillierte Vorstellung der Modelle verzichtet und auf die entsprechende Originalliteratur verwiesen. Um dennoch einen Überblick zu geben werden exemplarisch kurz die grundsätzlichen Inhalte der Modelle nach Gordon/Loeb (2002), Soo Hoo (2000), Cavusoglu et al. (2004), Schechter (2004) und Sonnenreich et al. (2006) skizziert sowie in einem kurzen Fazit bewertet Anschließend wird detailliert auf das Modell von Faisst et al. (2007) eingegangen, da dieses in Verbindung mit dem Verfahren von Conrad (2005) die Grundlage für das konzipierte Modell zur Bestimmung des optimalen Investitionsbeitrags bildet

Das Modell von Gordon/Loeb versucht den optimalen Investitionsbeitrag in Sicherheitsmaßnahmen anhand von Verteilungsfunktionen zu bestimmen. Es ist vor allem theoretischer Natur. Dennoch lassen sich wichtige Erkenntnisse daraus ziehen: Zum einen zeigen Gordon/Loeb auf, dass es sinnvoll sein kann, bei geringer Verwundbarkeit keine Investitionen zu tätigen. Zum anderen zeigen sie, dass die optimale Investitionssumme den prozentualen Anteil von 36,79% an der zu erwartenden Schadenssumme nicht überschreiten sollte. (Gordon/Loeb 2002)

Soo Hoo stellt ein entscheidungsbasiertes Modell vor und bedient sich Modellierungsmethoden, mit denen Einflussdiagramme erstellt werden. Es ist dabei möglich, Sicherheitsmaßnahmen zu Policies zu bündeln. Im Zentrum des Modells stehen die Bewertung und der Vergleich dieser Policies anhand ihres Nettonutzens. Das wichtigste Element zur Berechnung des Nettonutzens ist die jährliche Schadenerwartung (Annual Loss Expectancy, ALE). (Soo Hoo 2000)

Einen sehr konkreten Ansatz aus der Spieltheorie liefern Cavusoglu et al. (2004). Sie gehen von einer IT-Sicherheitsinfrastruktur aus, die sich aus einer präventiven, detektiven und reaktiven Ebene zusammensetzt. Zusätzlich werden mit dem Verhalten des Angreifers strategische Aspekte von IT-Risiken in das Modell

integriert. Ein sogenannter Game Tree stellt die Strategien der beiden „Spieler" dar. Einfluss auf diesen haben zudem Qualitätsparameter sowie auch angreifer- und firmenspezifische Parameter. Die Bestimmung des optimalen Verhältnisses aus Kosten und Nutzen geschieht letztendlich auf der reaktiven Ebene. (Cavusoglu et al. 2004)

Wie Cavusoglu et al. (2004) bezieht auch Schechter (2004) den Angreifer in sein Modell mit ein. Er geht von einem rationellen Angreifer aus, der nur so lange angreift, wie sein erwarteter Nutzen höher ist als seine Aufwendungen. Vor allem die Abschreckungswirkung von Maßnahmen soll gemessen werden. Hierzu versucht er den Return on Investment (ROI) des Angreifers herzuleiten. Ziel ist es, möglichst unattraktiv für den Angreifer zu sein, also dessen ROI zu minimieren. (Schechter 2004)

Sonnenreich wählt einen sehr praxisorientierten Ansatz. Ziel ist es sowohl Entscheidungsträger als auch Techniker bei der strategischen Planung von effektiven IT-Sicherheitsstrategien zu unterstützen. Hierzu ist es notwendig eine monetäre Bewertung der Investitionen vorzunehmen, weshalb er den Return on Security Investment (ROSI) vorschlägt (Sonnenreich 2006, S. 46):

$$ROSI = \frac{(Schadenspotential \cdot Prozentuale\ \ Schadensreduzierung) - Maßnahmenkosten}{Maßnahmenkosten}$$

Problematisch an der Formel sind die Faktoren, bzw. deren zuverlässige Bestimmung. Sonnenreich greift hier auf die ALE zurück, geht aber auf Abstand zu einer allzu genauen Messung der Faktorenwerte. Vielmehr sollte sich auf die Kostenfaktoren konzentriert werden. Bei der Vorhersage des potentiellen Schadens schlägt er vor, geeignete Werkzeuge wie die Monte-Carlo-Simulation zu nutzen und seltene Vorfälle außer Betracht zu lassen, da eine Vorhersage von häufigen Ereignissen erheblich besser möglich ist. (Sonnenreich 2006)

Die analysierten und im Rahmen dieses Beitrags kurz skizzierten Modelle nähern sich dem Problem der Bestimmung des optimalen Investitionsbeitrags in IT-Sicherheit- bzw. IT-Notfallmaßnahmen aus unterschiedlichen Blickwinkeln an. Als Bestandteil einer Kosten-Nutzen-Analyse können im Rahmen von IT-Risikoanalysen angemessene Investitionen in Maßnahmen zur IT-Sicherheit bestimmt und ökonomisch gerechtfertigt werden. Die analysierten Modelle liefern hierbei akzeptable Ergebnisse, sofern die entsprechenden Parameter – insbesondere für Eintrittswahrscheinlichkeit und Schadenshöhe – korrekt geschätzt werden. Speziell in dieser Bestimmung liegt jedoch eine entscheidende Herausforderung (Berinato 2005). Zudem fehlt es meist an einer mehrperiodigen Betrachtung, was jedoch für die Bestimmung des gewünschten NPV unerlässlich ist.

Aus diesem Grund wurde das Modell von Faisst et al. (2007) ausgewählt, da es in der erweiterten Form eine mehrperiodische Betrachtung grundsätzlich berücksichtigt, jedoch in einem wesentlichen Punkt erweitert. Für die Quantifizierung der Prognoseunsicherheit von Eintrittswahrscheinlichkeit und Schadenshöhe wird dieses zudem mit der Monte-Carlo-Simulation kombiniert. In der Monte-Carlo-

Simulation findet eine Dreiecksverteilung Verwendung. Diese wird mit den Parametern „Best Case", „Most Likely Case" und „Worst Case" bestimmt. Die Dreiecksverteilung erlaubt hohe „Worst Case" Werte, die weit von den am wahrscheinlichsten „Most Likely Case" Werten entfernt sind. Damit nähert sich die Dreiecksverteilung gut der Realität von Schadensfällen an und ist hinsichtlich der Praktikabilität vorteilhaft, da sie Expertenschätzungen in Bandbreiten ermöglicht und dennoch recht zuverlässige Werte liefert.

2.2 Verfahren zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen

Das Modell von Faisst et al. (2007) konzentriert sich auf die Beurteilung von IT-Sicherheitsprojekten, die über mehrere Perioden Ein- und Auszahlungen nach sich ziehen. Die ökonomische Vorteilhaftigkeit von Investitionen in IT-Sicherheitsmaßnahmen wird dabei auf Basis einer angepassten Kapitalwertmethode berechnet Der grundlegende Gedanke des Modells besteht darin, die beiden Optimierungskalküle Risikovermeidung und Kostenminimierung in einem Ansatz zu vereinen. Zu diesem Zweck wird die Risikoverminderung als Einzahlung, die durch IT-Sicherheitsmaßnahmen generiert wird, den Anschaffungs- und laufenden Kosten für eine Maßnahme gegenüber gestellt (Faisst et al. 2007, S. 512-513). Essenzielle Anforderungen sind dabei die „Abbildung von mehrperiodischen Laufzeiten der Maßnahme", die „Berücksichtigung der Zeitpräferenz" von Zahlungen und die „Berücksichtigung der ökonomischen Eigenkapitalunterlegung für unerwartete Schäden" (Faisst et al. 2007, S. 518). Die Kapitalwertmethode kommt diesen Kriterien am nächsten und wird von Faisst et al. modifiziert. Des Weiteren beziehen die Autoren in den Ansatz Opportunitätskosten mit ein, die aus einer nötigen Eigenkapitalunterlegung für unerwartete Schäden resultieren. Dies ist sinnvoll, da jenes Eigenkapital nicht gleichzeitig investiert werden kann, und entsprechende Opportunitätskosten zu berücksichtigen sind (Prokein 2008, S. 89-91). Die Bestimmung der unerwarteten Schäden erfolgt in Anlehnung an den „Internen Bemessungsansatz" nach Basel II. Dabei wird auf Basis der erwarteten Häufigkeit von Schadereignissen mithilfe einer Poissonverteilung der unerwartete Schaden und die dafür nötige Eigenkapitalunterlegung abgeschätzt (Faisst et al. 2007, S. 524).

Basisvariante des Verfahrens von Faisst et al.

Der Kapitalwert einer IT-Sicherheitsmaßnahme nach Faisst et al. (2007) berechnet sich durch:

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

I_0	Anfangsinvestition für die Implementierung der IT-Sicherheitsmaßnahme
C_t	Betriebs- und Wartungskosten der Maßnahme zum Zeitpunkt t, wobei angenommen wird, dass diese über den Betrachtungszeitraum konstant sind.
T	Betrachtungszeitraum
i_{calc}	Risikoloser Zinssatz i (als konstant angenommen)

Die Reduzierung der Schadenshöhe $\Delta E(L_t)$ berechnet sich dabei durch:

$$\Delta E(L_t) = E(N_0) \cdot \Delta SL_t \cdot (1 - IL_t) \cdot AV_t$$

$E(N_0)$	Erwartete Anzahl der Angriffsversuche N_0 zum Betrachtungszeitpunkt
ΔSL_t	SL_t gibt die Wahrscheinlichkeit an, dass in Periode t ein Angriffsversuch erfolgreich abgewehrt wird. ΔSL_t steht für die Zunahme des Sicherheitsniveaus durch Implementierung der IT-Sicherheitsmaßnahme. $\Delta SL_t = SL_t - SL_0$ wobei $SL \in (0;1)$
IL_t	Übertragbarkeitsquote; gibt den Anteil am Schaden an, der beispielsweise auf eine Versicherung abgewälzt werden kann (als konstant angenommen)
AV_t	Vermögenswert, der zum Zeitpunkt t durch einen erfolgreichen Angriff zu versinken droht (als konstant angenommen)

Die Reduktion der Opportunitätskosten ΔOCC_t berechnen sich durch:

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

i_{opp}	Zinssatz zur Berechnung der Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden
γ_0	Gamma-Faktor zum Zeitpunkt vor einer Investition in eine IT-Sicherheitsmaßnahme. Dieser Faktor hängt von der Anzahl erwarteter erfolgreicher Angriffe ab. Zur Berechnung des Gammafaktors sei auf Faisst et al. (2007) verwiesen
γ_t	Gamma-Faktor nach Realisierung der IT-Sicherheitsmaßnahme
$E(L_0)$	Erwarteter Schaden ohne Implementierung der IT-Sicherheitsmaßnahme
$E(L_t)$	Erwarteter Schaden nach Implementierung der IT-Sicherheitsmaßnahme

Ergibt sich ein positiver Kapitalwert, so lautet die Empfehlung die Investition durchzuführen, andernfalls sollte von der Umsetzung der Maßnahme abgesehen werden.

Erweiterung des Verfahrens von Faisst et al.

In einer ersten Erweiterung des Modells wird untersucht, wie sich verschiedene Investitionszeitpunkte auf die Vorteilhaftigkeit von IT-Sicherheitsinvestitionen

auswirken. Es besteht nun die Möglichkeit, „nicht nur zum Zeitpunkt t=0, sondern jeweils zum Zeitpunkt zwischen t=0 und t=T (…) einmalig zu investieren“ (Faisst et al. 2007, S. 527). Dies soll der Beobachtung der Autoren Rechnung tragen, dass die Investitionskosten einer IT-Sicherheitsmaßnahme im Zeitablauf sinken, während gleichzeitig eine steigende Zahl von Angriffen zu verzeichnen ist. Um diesen Sachverhalt im Modell abzubilden, wird ein Progressionsfaktor g für die erwartete Angriffshäufigkeit eingeführt, welcher die Werte pro Periode erniedrigt bzw. erhöht. Aufgrund der über den Zeitablauf steigenden Angriffshäufigkeit $E(N_t)$ müssen die Berechnungen für die erwartete Risikoreduktion und die Opportunitätskosten einer Eigenkapitalunterlegung jeweils um den Faktor $(1+g)^t$ erweitert werden (Faisst et al. 2007, S. 529):

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

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

2.3 Bewertung von IT-Sicherheits- und IT-Notfallinvestitionen mit Hilfe von Monte-Carlo Simulationen

IT-Sicherheitsexperten sehen sich oft mit der Schwierigkeit konfrontiert, für IT-Risikoprognosen mehrere Parameter, wie sie beispielsweise bei der ALE-Berechnung nötig sind, möglichst exakt anzugeben. Im Rahmen eines Modells zur Bewertung von IT-Sicherheits- bzw. IT-Notfallinvestitionen gibt es weitere Unsicherheit bei der Bestimmung der Effizienz einer Maßnahme bzw. bei der Angabe, mit welcher Wahrscheinlichkeit ein Angriff verhindert werden kann. Eine Möglichkeit, dieser Unsicherheit Ausdruck zu verleihen, ist sie mithilfe einer auf Zufallszahlen basierenden Verteilungsfunktion zu beschreiben. Die Bestimmung einer Verteilungsfunktion ist Basis für die Durchführung einer Monte-Carlo Simulation.

Die Stärke von Monte-Carlo Simulationen ist, dass sie keine eindeutigen Eingabewerte benötigt, sondern für die Durchführung der Simulation eine Abschätzung mittels Verteilungen bereits ausreichend sein kann. Es ist dennoch zu beachten, dass die Güte dieser Abschätzungen wesentlichen Einfluss auf die Qualität der Ergebnisse ausübt. Mithilfe einer Monte-Carlo Simulation ist es einem Unternehmen folglich dennoch möglich, Aussagen über beispielsweise das IT-Risiko zu treffen, auch wenn keine oder kaum historische Daten für eine Prognose zur Verfügung stehen. (Prokein 2008, S. 49-53; Everling 2008, S. 541)

Ein Modell zur Bewertung von Investitionen in IT-Sicherheitsmaßnahmen kann im Rahmen einer Monte-Carlo Simulation als Funktion gesehen werden, welcher eine Menge an Parametern übergeben wird und die daraufhin ein Ergebnis liefert (Conrad 2005, S. 2). Die übergebenen Parameter sind dabei nicht nur ein durch einen Experten geschätzter Wert, sondern Zufallszahlen, welche aus den zuvor festgelegten Verteilungen generiert werden. Diese werden für jede Iteration neu generiert. Der oder die Rückgabewerte der Funktion stellen dabei das Ergebnis

infolge der Modellberechnungen dar und werden für eine Auswertung gespeichert. Im Rahmen einer Simulation wird eine Anzahl an Iterationen vorgegeben. Nach Abschluss aller Iterationen gilt es, die erfassten Werte aufzubereiten und statistisch zu analysieren.

3 Forschungsergebnisse

3.1 Ansatz zu einer verbesserten Berechnungsformel der reduzierten Opportunitätskosten

Faisst et al. erkennen zurecht, „dass nach Implementierung einer IT-Sicherheitsmaßnahme $\Delta E(L_t)$ und ΔOCC_t mit t höher werden“ (Faisst et al. 2007, S. 530) müssen, wenn $g > 0$. Dies steht jedoch im Widerspruch zu der von den Autoren gegebenen Formel. Die Risikoreduktion sollte im Falle einer über den Betrachtungszeitraum steigenden Angriffshäufigkeit nicht wie angegeben berechnet werden. In der gegebenen Formel steht der erste Teil (Minuend) für die Opportunitätskosten einer Eigenkapitalunterlegung vor der Implementierung einer IT-Sicherheitsmaßnahme und bleibt für alle Berechnungszeitpunkte fix. Dass dies der Fall ist, ist am Index „0“ des Gamma-Faktors γ_0 und der erwarteten Schadenshöhe $E(L_0)$ abzulesen. Der zweite Teil (Subtrahend) der Gleichung steigt jedoch im Zeitablauf, da die Angriffshäufigkeit um den Faktor g und somit auch der erwartete Schaden $E(L_t)$ wächst. So wird die Opportunitätskostenreduktion mit jeder Periode kleiner und bei genügend großem g oder einem langen Betrachtungszeitpunkt auch negativ. Dies würde bedeuten, dass die IT-Sicherheitsmaßnahme eine Erhöhung der Opportunitätskosten bewirkt, obwohl genau das Gegenteil zu erwarten wäre. Somit würde die Berechnung ebenfalls der Modellannahme widersprechen, die besagt, dass „durch eine Verbesserung des Sicherheitslevels $S(L_t)$ (…) auch eine Reduktion der Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden ΔOCC_t “ (Faisst et al. 2007, S. 524) folgt. Zur Veranschaulichung ein Beispiel mit folgenden Parametern[1].

Erwartete Häufigkeit erfolgreicher Angriffe in t=0 ohne Sicherheitsmaßnahme	$E_{ohne}(Q_0) = 2$
Erwartete Häufigkeit erfolgreicher Angriffe in t=0 mit Sicherheitsmaßnahme	$E_{mit}(Q_0) = 1$
Erwarteter jährlicher Schaden ohne Sicherheitsmaßnahme	$E(L_{t,ohne}) = 2.000$
Erwarteter jährlicher Schaden mit Sicherheitsmaßnahme	$E(L_{t,mit}) = 1.000$

[1] *Hinweis:* Parameter, die den Zustand mit IT-Sicherheitsmaßnahme beschreiben, werden im Folgenden durch den Index „mit“, der Zustand ohne Absicherung mit dem Index „ohne“ gekennzeichnet.

Progressionsfaktor für Schadenshäufigkeit pro Periode	$g = 100\%$
Opportunitätskostensatz für Eigenkapitalunterlegung	$i_{opp} = 8\%$

Wird die Opportunitätskostenreduktion auf Basis der Formel von Faisst et al. (2007) berechnet, ergeben sich für die einzelnen Perioden folgende Werte:

T	0	1	2	3
Opportunitätskosten OCC_{ohne}	408,96	408,96	408,96	408,96
Opportunitätskosten OCC_{mit}		408,96	556,48	770,56
Opportunitätskostenreduktion ΔOCC_t		0	-147,52	-361,6

Die berechneten Werte verdeutlichen den zuvor beschriebenen Widerspruch. Der Kapitalwert einer IT-Sicherheitsmaßnahme würde auf Basis der Berechnung der Opportunitätskostenreduktion nach Faisst et al. (2007) für den Fall einer steigenden Angriffshäufigkeit negativ ausfallen. Folglich sollte die Opportunitätskostenreduktion mit folgender Formel berechnet werden:

$$\Delta OCC_t = \left(i_{opp} \cdot \gamma_{t,ohne} \cdot E\left(L_{t,ohne}\right)\right) - \left(i_{opp} \cdot \gamma_{t,mit} \cdot E\left(L_{t,mit}\right)\right)$$
$$\text{mit } (1 \leq t \leq T)$$

Diese Formel betrachtet immer die Opportunitätskosten der gleichen Periode. Der Minuend des Terms entspricht den Opportunitätskosten einer Eigenkapitalunterlegung für unerwartete Schäden in der Periode t unter der Annahme, dass keine IT-Sicherheitsmaßnahmen getroffen werden. Der Subtrahend hingegen entspricht den Opportunitätskosten des Zeitpunkts t bei unterstellter Absicherung der Risiken. Für das obige Beispiel ergeben sich nach der vorgeschlagenen Formel folgende Werte:

T	0	1	2	3
Opportunitätskosten OCC_{ohne}	408,96	556,48	770,56	1058,56
Opportunitätskosten OCC_{mit}		408,96	556,48	770,56
Opportunitätskostenreduktion ΔOCC_t		147,52	214,08	288,00

3.2 Kombination einer Monte-Carlo Simulation mit der dynamischen Investitionsrechnung und deren Interpretation

Jedes Modell zur Bewertung von IT-Sicherheitsinvestitionen kann grundsätzlich ohne große Anpassungen für eine Monte-Carlo Simulation verwendet werden. Dazu muss das bestehende Bewertungsmodell lediglich mit einem geeigneten Monte-Carlo Tool verlinkt werden, sodass die erzeugten Zufallszahlen in die Bewertung einfließen und die Ergebnisse im Anschluss abgegriffen werden können

(Conrad 2005, S. 2). Dies wurde mithilfe einer eigens entwickelten Softwarelösung realisiert. Relevante Parameter dabei sind die geschätzten Werte für die Effizienz einer IT-Sicherheits- bzw. Notfallmaßnahme, die Angriffs- bzw. Ausfallhäufigkeit sowie die Schadenshöhe pro Angriff bzw. Ausfall. Durch die Erhebung des jeweils zu erwartenden besten, wahrscheinlichsten und schlechtesten Falls, lassen sich die gewünschten Dreiecksverteilungen bestimmen (vgl. Abbildung 1).

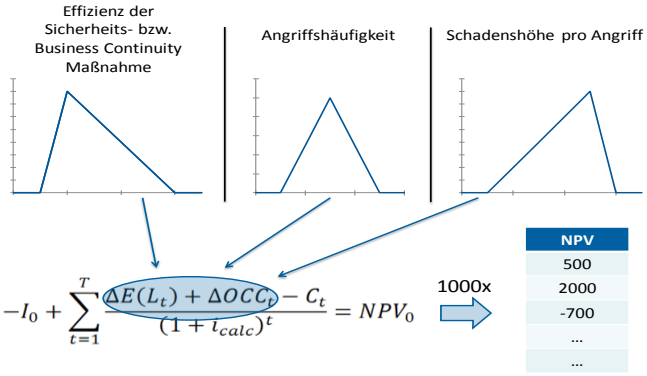

Abbildung 1: Eingabeparameter des Modells

Für die Interpretation der Monte-Carlo Simulation werden mit Histogramm und Verteilungsfunktion die üblichen zwei Diagramme herangezogen, da diese die Simulationsergebnisse sehr anschaulich zusammenfassen (vgl. Abbildung 2 und 3). In Folge der Implementierung der betrachteten IT-Sicherheitsmaßnahme kann deren Kapitalwert zwischen den Extremwerten von ca. - 25.000 und + 75.000 Euro variieren. Das Histogramm gibt Aufschluss darüber, wie stark mögliche Kapitalwerte streuen oder ob sie sich eher um einen Wert konzentrieren. Da beispielsweise die bestbesetzte Klasse des Histogramms gerade noch für einen negativen Kapitalwert steht, kann man aus dem Histogramm nicht ohne Weiteres ablesen, ob eher ein positiver oder negativer Kapitalwert zu erwarten ist.

Dieses Problem löst die Verteilungsfunktion (vgl. Abbildung 3). Anhand dieser kann ermittelt werden, dass in mehr als der Hälfte aller Fälle bereits ein positiver Kapitalwert zu erwarten ist. Bei einem Kapitalwert von Null kann man in etwa eine Unterschreitungswahrscheinlichkeit von 42% ablesen. Es kann gefolgert werden, dass zu rund 42% ein negativer und folglich zu rund 58% ein positiver Kapitalwert zu erwarten ist.

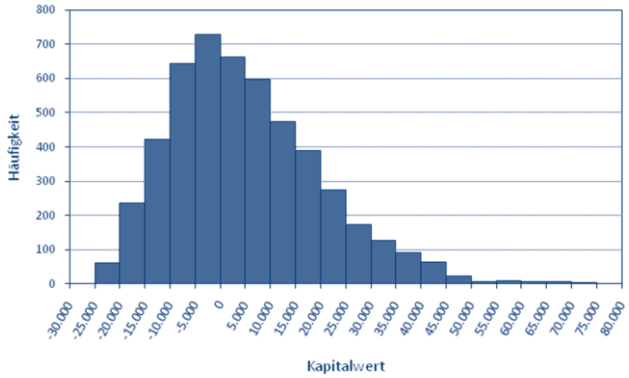

Abbildung 2: Errechnetes Histogramm

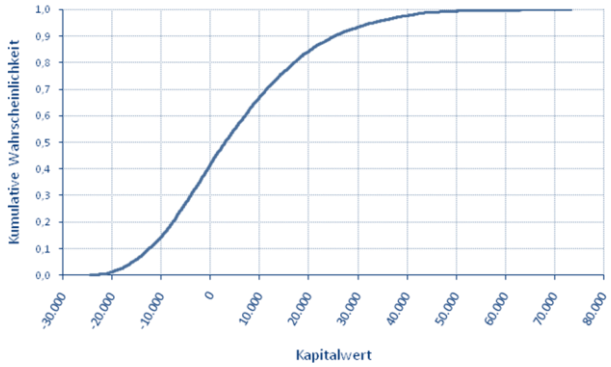

Abbildung 3: Errechnete Verteilungsfunktion

3.3 Beispiel

Zur Verifizierung der Eignung des konzipierten Modells für die Bestimmung des optimalen Investitionsbeitrags in IT-Sicherheits- bzw. IT-Notfallmaßnahmen wurden unterschiedliche Szenarien getestet Als Beispiel behandelt das folgende Szenario unterschiedliche Investitionsentscheidungen für den Prozess „Kreditvergabe". Als IT-Notfallmaßnahmen in Bezug auf die Absicherung des „Rechenzentrumsbetriebs" kommen drei unterschiedliche Szenarien S1, S2 und S3 in Betracht (vgl. Abbildung 4). Die Eingabeparameter sind die Anfangsinvestitionen, die laufenden Kosten der Maßnahme, die erwartete Verbesserung der Verfügbarkeit sowie der durchschnittliche Schaden bis zum Wiederanlauf der Systeme bei Durchführung der Maßnahme. Weiterhin werden das Verfügbarkeitslevel sowie die erwarteten Ausfälle pro Jahr vor der Investition berücksichtigt.

Die teuersten Anfangsinvestitionen sowie laufenden Kosten entstehen mit der Lösung S1, bei der ein Stand-By-Rechenzentrum mit vollständiger, redundanter

Infrastruktur zum Einsatz kommt. Jedoch kann mit dieser Lösung das Verfügbarkeitsniveau um 17% verbessert werden. Der durchschnittliche Schaden bis zum Wiederanlauf ist zudem am geringsten. Die beiden anderen Lösungen sind zwar günstiger, können dafür aber das Verfügbarkeitsniveau nicht so stark erhöhen. Auf Grundlage der gelieferten Auswertung kann so die Vorteilhaftigkeit von Maßnahmen beurteilt und eine Priorisierung vorgenommen werden

Prozess „Rechenzentrums-betrieb“ MTA = 10 Tage	S1: „Hot“-Lösung Stand-By-Rechenzentrum mit kompletter, redundanter Infrastruktur	S2: „Warm“-Lösung eigenes Rechenzentrum; vollständige IT vorhanden; Einspielen von Sicherungen im Notfall notwendig	S3: „Cold“-Lösung Beschaffung von Hardware, Installation der Software und Anwendungen und Einspielen von Sicherungskopien
Anfangsinvestition	5 Mio. €	3 Mio. €	1.2 Mio. €
Laufende Kosten	30.000 €	20.000 €	20.000 €
Verfügbarkeitslevel vor Notfallmaßnahme	82%	82%	82%
Verbesserung des Verfügbarkeitslevels	17%	12 %	2,3 %
Erwartete Ausfälle pro Jahr	~ 5	~ 5	~ 5
Durchschnittlicher Schaden bis zum Wiederanlauf	~ 630.000 €	~ 1.060.000 €	~ 1.850.000 €

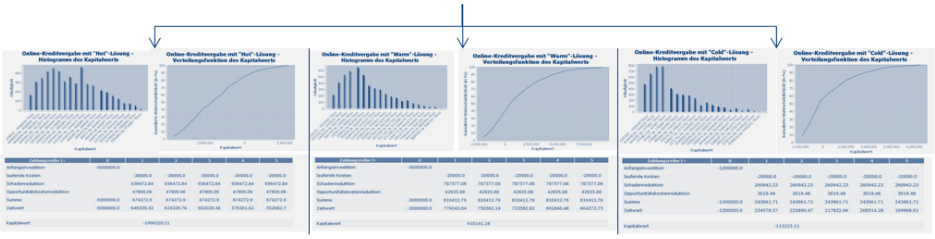

Abbildung 4: Bestimmung des optimalen Investitionsbeitrags

4 Fazit

Das beschriebene Modell erzielt einen großen Erkenntnisgewinn. Die angepasste Formel zur Opportunitätskostenreduktion liefert die notwendige Grundlage für eine mehrperiodische Betrachtung.

Parameter, die sich auf die Zukunft beziehen, enthalten zwangsläufig eine gewisse Unsicherheit. Diese Unsicherheit und ihre Auswirkung kann mithilfe der betrachteten Simulationsmethode anschaulich dargestellt werden. Die aus einer Monte-Carlo Simulation resultierenden Diagramme stellen sowohl für IT-Risikomanager als auch für Budget-Entscheider eine gute und nachvollziehbare Entscheidungsgrundlage für Investitionen dar. Budget-Entscheider haben hierbei die Möglichkeit bestehende Modelle, wie beispielsweise einen NPV-Ansatz, weiterhin zu verwenden, IT-Sicherheitsexperten sind nicht mehr gezwungen, sich im

Rahmen der Abschätzung sehr unsicherer Werte, wie der Angriffshäufigkeit, auf eine einzige Zahl festzulegen. Die Monte-Carlo Simulation stellt somit eine sehr gute Möglichkeit dar, das mit Entscheidungen über IT-Sicherheitsinvestitionen verbundene Risiko quantitativ zu untersuchen.

Literatur

Berinato S (2005) A few good metrics. http://www.csoonline.com/read/070105/metrics.html. Abruf am 2009-11-25.

Bundesanstalt für Finanzdienstleistungsaufsicht (2009) Konsultation – Neufassung der Mindestanforderungen an das Risikomanagement (MaRisk).

Cavusoglu H, Mishra B, Ragunathan S (2004) A model for evaluating IT security investments. Communications of the ACM 47 (7): 87-92.

Conrad J (2005) Analyzing the risks of information security investments with Monte-Carlo Simulations. http://infosecon.net/workshop/pdf/13.pdf. Abruf am 2009-04-15.

Deloitte (2009) Loosing Ground 2009 TMT Global Security Survey. http://www.deloitte.com/assets/Dcom-Germany/Local%20Assets/Documents/dtt_TMT-Security-Survey09-full(1).pdf. Abruf am 2009-11-25.

Everling O (2008) Bankrisikomanagement. Mindestanforderungen, Instrumente und Strategien für Banken. Gabler. Wiesbaden.

Faisst U, Prokein O, Wegmann N (2007) Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. ZfB 77 (5): 511-538.

Gordon L, Loeb M (2002) The economics of information security investment. ACM Transactions on Information and System Security 5 (4): 438-457.

Kronschnabl S (2008) IT-Security Governance. Bankinnovationen Band 23. Universitätsverlag Regensburg.

Prokein O (2008) IT-Risikomanagement. Identifikation, Quantifizierung und wirtschaftliche Steuerung. Gabler. Wiesbaden.

Schechter S (2004) Computer security strength & risk – a quantitative approach. Dissertatiton Cambridge. Massachusetts.

Sonnenreich W, Albanese J, Stout B (2006) Return on security investment (ROSI) – A practical quantitative model. JRPIT 38 (1): 45-55.

Soo Hoo K (2000) How Much Is Enough? A Risk-Management Approach to Computer Security. http://iis-db.stanford.edu/pubs/11900/soohoo.pdf, 2000. Abruf am 2009-01-06.