

# Verfahren zur Wirtschaftlichkeitsanalyse von IT-Sicherheitsinvestitionen

Rainer Rumpel<sup>a</sup>, Richard Glanze<sup>b</sup>

<sup>a</sup> Facheinheit Wirtschaftsinformatik, Fachbereich Berufsakademie, Fachhochschule für Wirtschaft Berlin, Deutschland, [Rainer.Rumpel@fhw-berlin.de](mailto:Rainer.Rumpel@fhw-berlin.de)

<sup>b</sup> neu-itec GmbH, Neubrandenburg, Deutschland, [richard.glanze@neu-sw.de](mailto:richard.glanze@neu-sw.de)

**Keywords:** Return on Security Investment, Annual Loss Expectancy, Net Benefit, Stochastic Dominance

## Abstract

*The private sector always has to consider seriously the cost-efficiency of projects. This applies also to projects treating security management or risk management. Until now there are not too much publications regarding the cost-efficiency of security investments. Based on well-known methods like Total Cost of Ownership (TCO), Total Benefit of Ownership (TBO) and Return on Investment (ROI), in 2002 there was introduced the Return on Security Investment (ROSI) idea, presented by S. Berinato [Berinato2002]. Today, there exist some approaches for computing ROSI. One is based on risk management statistical decision theory [SooHoo2000], another uses calculus [GordonLoeb2002]. And Cavusoglu et alii [Cavusoglu2004] developed a game-theoretic model using the rule of Bayes. One of the typical problems of evaluating the benefit of security investments is the lack of statistical data regarding security incidents. Can this lack be compensated by a suitable choice of model respectively of theory? To answer this question, two real business cases will be studied to check the applicability of the ideas. The results presented are based on case studies done in German companies.*

*Im Jahr 2002 wurde von Scott Berinato [Berinato2002] die Idee des Return on Security Investment (ROSI) präsentiert, die auf wohl bekannten Methoden wie Total Cost of Ownership (TCO), Total Benefit of Ownership (TBO) und Return on Investment (ROI) beruhen. Ein Problem des ursprünglichen Return-on-Security-Investment-Ansatzes ist, dass präzise Berechnungen auf Basis grober Schätzungen durchgeführt werden. Eines der typischen Probleme der Nutzenermittlung von Sicherheitsinvestitionen ist der Mangel an genauen Daten zu Sicherheitsvorfällen. Heutzutage gibt es verschiedene Verfeinerungen des Ansatzes zur ROSI-Ermittlung, die Statistik, Analysis und Spieltheorie verwenden. Kann der Mangel an Genauigkeit der Inputdaten durch eine geeignete Verfahrenswahl kompensiert werden? Um diese Frage zu beantworten, wird der Ansatz von Kevin J. Soo Hoo [SooHoo2000] hinsichtlich seiner praktischen Anwendbarkeit an zwei Sicherheitsinvestmentszenarien deutscher Unternehmen geprüft. Es sind Ergebnisse erzielbar, die für den Einsatz in der Praxis geeignet sind.*

## Inhaltsübersicht

|     |   |    |
|-----|---|----|
| 1   | Situation und Motivation .....                      | 2  |
| 2   | Nutzenermittlung .....                              | 2  |
| 3   | Stochastischer Ansatz zur Ermittlung des ROSI ..... | 3  |
| 4   | Anwendbarkeit der ROSI-Ansätze .....                | 5  |
| 4.1 | Fallbeispiel Notfallrechenzentrum .....             | 5  |
| 4.2 | Fallbeispiel Grundschutzprojekt .....               | 9  |
| 5   | Fazit und Ausblick .....                            | 11 |
| 6   | Literatur .....                                     | 12 |

# 1 Situation und Motivation

Das Risikomanagement-Framework für IT-Sicherheit hat sieben grundlegende Elemente [SooHoo2000, S. 5]:

- Requirements (Nebenbedingungen, Anforderungen)
- Assets (Werte)
- Security Concerns (Sicherheitsaspekte)
- Threats (Bedrohungen, Gefährdungen)
- Safeguards (Sicherheitsmaßnahmen)
- Vulnerabilities (Verletzungsanfälligkeit)
- Outcomes (Ergebnisse)

Mit diesen Elementen des Risikomanagements ist der IT-Sicherheitsmanager fast täglich befasst. Er hat die Werte des Unternehmens zu schützen, indem er geeignete organisatorische oder technische Sicherheitsmaßnahmen ergreift. Er hat dabei verhältnismäßig zu agieren, indem er die Gefährdungslage angemessen einschätzt, die Sicherheitslücken analysiert und mit der Unternehmensführung den Schutzbedarf und die Sicherheitsziele der diversen Assets priorisiert. In vielen Fällen bleibt aber die Frage offen, welche der zur Diskussion stehenden Sicherheitsmaßnahmen in einem günstigen Nutzen-Kosten-Verhältnis stehen. Übliche Methoden zur Berechnung des Nutzens versagen, weil durch IT-Sicherheitsmaßnahmen meistens weder ein direkter Nutzen noch eine unmittelbare Aufwandsersparnis erzielt wird. Gibt es also Methoden zur Quantifizierung des Nutzens von IT-Sicherheitsmaßnahmen, die in der Praxis anwendbar sind?

## 2 Nutzenermittlung

Die Nutzwertanalyse [Zangemeister1976] ist ein Verfahren zur quantitativen Bewertung von Maßnahmen. Hier werden aber keine monetären Ergebnisse erzielt, sondern für jede Handlungsvariante ein Punktwert berechnet, der dann mit den Punkten der Alternativen verglichen. Das Verfahren hat insbesondere dann seine Stärken, wenn die Nutzwerte nicht oder nur schwer monetarisierbar sind. Ist aber die Monetarisierung des Nutzens gefordert, dann ist die Nutzwertanalyse nicht die geeignete Wahl.

Der Return on Investment (kurz ROI) soll die Rendite des eingesetzten Kapitals messen. Der ROI ist die Spitzenkennzahl des 1919 im Unternehmen Du Pont de Nemours eingeführten Rentabilitätsschemas. Der ROI ist der Quotient aus Periodengewinn und Kapitaleinsatz. Die Gewinnermittlung ist bei klassischen Investitionsentscheidungen wie dem Kauf einer Produktionsanlage relativ leicht. Bei IT-Investitionen entsteht üblicherweise kein direkter, monetärer Nutzen, so dass ersatzweise Ersparnisse als Gewinn betrachtet werden. Bei IT-Sicherheitsinvestitionen gibt es normalerweise auch keine unmittelbaren Ersparnisse. So hat nach wie vor in Managementkreisen die Meinung Bestand, dass IT-Sicherheit eigentlich nur Kosten verursacht.

Zieht man sich aber nun bei der Nutzenbetrachtung von IT-Sicherheitsmaßnahmen lediglich auf qualitative Aspekte zurück, so besteht die Gefahr, dass sich der IT-Sicherheitsmanager auf die FUD<sup>1</sup>-Methode zurückzieht, die in erster Linie ein Versuch ist, die Unternehmensleitung einzuschüchtern, indem man ihr die heutigen IT-Gefahren bedrohlich vor Augen hält. Dieses Vorgehen ist aber unbefriedigend, wenn es nicht von belastbaren Hintergrundinformationen getragen ist und die Entscheider die Verhältnismäßigkeit der Kosten nicht einschätzen können. Aufgrund dessen gibt es heutzutage auch bei IT-Sicherheitsprojekten immer mehr Ansprüche an den Nachweis der Wirtschaftlichkeit.

---

<sup>1</sup> FUD: Fear, Uncertainty and Doubt („Furcht, Ungewissheit und Zweifel“)

### 3 Stochastischer Ansatz zur Ermittlung des ROSI

Seitdem der Begriff Return on Security Investment (ROSI) eingeführt wurde [Berinato2002], hat sich das Interesse an der Betrachtung der Wirtschaftlichkeit von Investitionen in IT-Sicherheit verstärkt. In der Diskussion des ROSI spielt die jährliche Verlusterwartung (Annual Loss Expectancy, im Folgenden kurz ALE) des klassischen Risikomanagements eine wichtige Rolle. Sie wurde 1979 vom amerikanischen National Bureau of Standards (NBS) eingeführt [SooHoo2000, S.4]:

$$ALE = \sum_{i=1}^n I(O_i) \cdot P_i$$

wobei die  $O_i$  Sicherheitsvorfälle, die  $I(O_i)$  die diesbezüglichen Schadensauswirkungen in Euro und die  $P_i$  die jeweiligen Schadenseintrittswahrscheinlichkeiten darstellen. Da die ALE-Berechnung eine notwendige Voraussetzung für die Ermittlung des ROSI (den man auch Netto-Nutzen nennen kann) ist, haben sich schnell kritische Stimmen gemehrt, die diesen Ansatz in Frage gestellt haben, da in vielen Fällen weder Schadensauswirkungen noch Schadenseintrittswahrscheinlichkeiten befriedigend genau quantifiziert werden können. Die Folge sind präzise Berechnungen, die auf unpräzisen Eingabedaten beruhen.

Dieser Kritik ist Soo Hoo mit einem statistischen Verfahren begegnet. Er bedient sich analytischer und statistischer Verfahren verbunden mit einer Modellierungstechnik, die auf sogenannten Einflussdiagrammen basiert. Mit dem Ansatz von Soo Hoo lassen sich verschiedene Bündel von Sicherheitsmaßnahmen auf ihren Netto-Nutzen hin vergleichen. Gehen wir davon aus, dass wir  $l$  Bündel miteinander vergleichen, so lässt sich für jedes Bündel  $B_k$  ( $k \in \{1, \dots, l\}$ ) der Nutzen der darin enthaltenen Sicherheitsmaßnahmen bestimmen:

$$\text{Nutzen}_k = ALE_0 - ALE_k$$

$ALE_0$  ist die jährliche Verlusterwartung für das leere Bündel  $B_0$ , also für den Fall, dass keine Sicherheitsmaßnahmen gegenüber dem Status Quo ergriffen werden. Man kann davon ausgehen, dass durch Anwendung eines Sicherheitsbündels die Schadenseintrittswahrscheinlichkeiten bzw. die Schadenshöhen sinken, somit also auch  $ALE_k$  kleiner als  $ALE_0$  ist. Somit führt das Anwenden von Sicherheitsmaßnahmen zu einem positiven Nutzen:  $\text{Nutzen}_k > 0$ . Kaum ein Unternehmensvorstand wird jedoch lediglich auf Basis eines berechneten Brutto-Nutzens eines Bündels von Sicherheitsmaßnahmen eine Investitionsentscheidung treffen. Der IT-Sicherheitsbeauftragte muss zusätzlich plausibel machen können, dass diese Sicherheitsmaßnahmen auch einen Netto-Nutzen (Net Benefit) haben. Man hat Rechenschaft abzulegen über die Kosten, die den Nutzen hervorbringen. Bei genauerer Analyse ist weiterhin ein sogenannter Zusatznutzen (ZNutzen) zu berücksichtigen, der durch IT-Sicherheit entsteht (z.B. Business-Enabler-Funktion der IT-Sicherheit). Folglich ergibt sich der Netto-Nutzen eines Sicherheitsbündels als

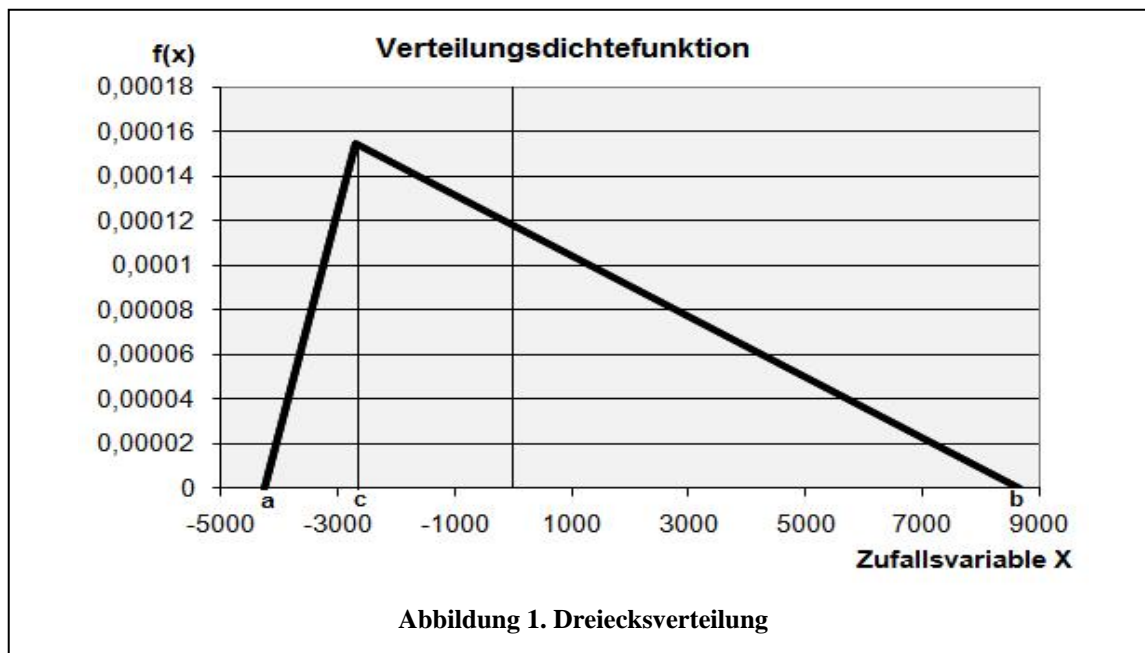
$$\text{NNutzen}_k = \text{Nutzen}_k - \text{Kosten}_k + \text{ZNutzen}_k$$

Kommen wir zurück zum Kritikpunkt, dass beim ALE präzise Berechnungen auf Basis grober Schätzungen durchgeführt werden. Begegnen kann man diesem Argument mit der Zulassung einer Werteverteilung entsprechend den Schätzungen von Experten oder den Ergebnissen von geeigneten empirischen Studien. In diesen Fällen bietet sich oft die sogenannte Dreiecksverteilung an, welche in Abbildung 1 dargestellt ist.

Bei einer Dreiecksverteilung ist die Verteilungsdichtefunktion  $f$  eine stückweise lineare Funktion. Wenn bei  $x=a$  der linke Schenkel beginnt und bei  $x=b$  der rechte Schenkel endet, so ist die zugehörige Dichtefunktion

$$f(x) = \begin{cases} \frac{2(x-a)}{(b-a)(c-a)} & a \leq x \leq c \\ \frac{2(b-x)}{(b-a)(b-c)} & c < x \leq b \end{cases} \quad \text{für } ,$$

wobei  $a$  der niedrigste,  $b$  der höchste und  $c$  der wahrscheinlichste Wert (Modus) ist.



Die kumulative Verteilungsfunktion F ergibt sich durch Integration der Verteilungsdichtefunktion f:

$$F(x) = \begin{cases} \frac{(x-a)^2}{(b-a)(c-a)} & a \leq x \leq c \\ 1 - \frac{(b-x)^2}{(b-a)(b-c)} & c < x \leq b \end{cases} \quad \text{für } .$$

F(x) gibt die Fläche unter dem Dreieck bis zur Stelle x wieder. Die Fläche des Dreiecks muss aus stochastischen Gründen gleich 1 sein.

Der Erwartungswert der Zufallsvariable X bezüglich der Verteilungsdichtefunktion f lässt sich mit der Formel

$$E(X) = \int_{-\infty}^{\infty} xf(x)dx$$

berechnen. Er entspricht dem Flächenschwerpunkt der Verteilungsdichtefunktion. Bei der Dreiecksverteilung beträgt der Erwartungswert

$$E(X) = \frac{x_{\min} + x_w + x_{\max}}{3}$$

Um Entscheidungen hinsichtlich einer IT-Sicherheitsinvestition unterstützen zu können, kann man auch die Frage nach der stochastischen Dominanz benutzen. Die Wahrscheinlichkeit, dass eine Zufallsvariable X höchstens x beträgt, ist

$$F(x) = P(X \leq x) = \int_{-\infty}^x f(t)dt .$$

Das gilt nicht nur für die Dreiecksverteilung. Die kumulative Verteilungsfunktion F dominiert die kumulative Verteilungsfunktion G genau dann, wenn für alle x gilt:

$$F(x) \geq G(x) , \text{ d.h. } \int_{-\infty}^x f(t)dt \geq \int_{-\infty}^x g(t)dt$$

## 4 Anwendbarkeit der ROSI-Ansätze

### 4.1 Fallbeispiel Notfallrechenzentrum

Bei der hier betrachteten Organisation handelt es sich um ein gemäß KMU-Definition der EU großes Unternehmen der Immobilienbranche mit Sitz in Berlin. Es soll die Wirtschaftlichkeit der Bereitstellung eines Notfallrechenzentrums vor den notwendigen Investitionen bzw. der Inanspruchnahme entsprechender Dienstleistungen untersucht werden. Für diese Ex-Ante-Analyse müssen zunächst die Sicherheitsaspekte und die Sicherheitsbündel definiert werden.

Sinn und Zweck des Notfallrechenzentrums ist die Bewältigung des Katastrophenfalls (K-Falls) infolge von Feuer, Wasser, Blitz, Erdbeben, Terroranschlag, Flugzeugabsturz usw. Man spricht vom K-Fall, wenn das Rechenzentrum für einen nicht absehbaren oder absehbar zu langen Zeitraum seine Dienste nicht erbringen kann. Als Ausgangssituation wird definiert, dass das Rechenzentrum in der Unternehmenszentrale zerstört ist. Für diesen Fall kann ein funktionierendes oder zur Funktion gebrachtes Notfallrechenzentrum bei einem Dienstleister die Schadenshöhe deutlich vermindern. Folgende vier Sicherheitsbündel werden betrachtet:

|               | <b>B<sub>0</sub></b>                      | <b>B<sub>1</sub></b> | <b>B<sub>2</sub></b> | <b>B<sub>3</sub></b> |
|---------------|---|----------------------|----------------------|----------------------|
| <b>Plan A</b> |   | X                    | X                    | X                    |
| <b>Plan B</b> |   |                      | X                    | X                    |
| <b>Plan C</b> |   |                      |                      | X                    |
|               | <b>Status Quo (keine redundante Site)</b> | <b>iSeries</b>       | <b>iSeries+B</b>     | <b>iSeries+B+C</b>   |

- B<sub>0</sub> = 0-Bündel (Status Quo)
- B<sub>1</sub> = Plan A >> iSeries Betrieb
- B<sub>2</sub> = Plan B (iSeries+B) >> zusätzliche Programme / Dienste
- B<sub>3</sub> = Plan C (iSeries+B+C) >> noch mal zusätzliche Programme / Dienste

Beginnen wir für die Berechnung des Netto-Nutzens mit den Kosten:

|                           | <b>B<sub>0</sub></b> | <b>B<sub>1</sub></b>  | <b>B<sub>2</sub></b>  | <b>B<sub>3</sub></b>  |
|---------------------------|----------------------|---|---|---|
| <b>Investitionskosten</b> | keine                | Hardware für IBM iSeries: 0,-EUR;<br>Lizenzen Betriebssystem: 0,-EUR                  | Zusätzliche Hardware und Lizenzen: 0,-EUR   | Zusätzliche Hardware und Lizenzen: 0,-EUR                             |
| <b>Betriebskosten</b>     | keine                | 3.360,-EUR Grundgebühr inklusive Recovery-Übung<br>Netzanbindung: 4.800,-EUR pro Jahr | <u>Zusätzlich:</u><br>Server und Windows-Lizenzen jährlich 14.000,-EUR<br>Jährliche vollständige K-Fall-Übung: 1.440,-EUR<br>Lagerung und Verwaltung von Speichermedien: 1.380,-EUR | <u>Zusätzlich:</u><br>Server und Windows-Lizenzen jährlich 2.000,-EUR |

Als nächstes ist ALE<sub>0</sub> (zum Bündel B<sub>0</sub>) zu ermitteln. Der K-Fall führt zur weitgehenden Geschäftsunterbrechung. Daraus folgen interne Personalkosten für die Mitarbeiter, die nicht arbeiten können. Außerdem entgehen dem Unternehmen in erheblichem Maße Umsätze:

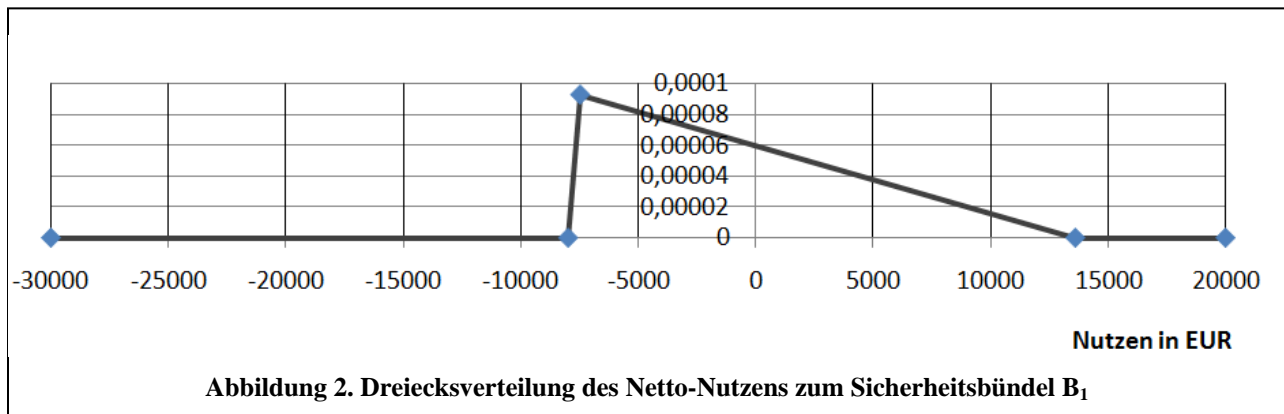


Abbildung 2. Dreiecksverteilung des Netto-Nutzens zum Sicherheitsbündel B<sub>1</sub>

Schaden pro Tag in EUR = (a;c;b) = (160200;209700;259200).

Da kein Notfallrechenzentrum vorhanden ist, müsste zunächst eine entsprechende Fläche gesucht und Hardware beschafft werden. Unter der Annahme, dass die Daten und die Datenträger für die Software weiterhin vorhanden sind, ist eine MTTR (Mean Time to Repair) von mindestens 8 Tagen, höchstens 30 Tagen, wahrscheinlich 16 Tagen realistisch.

Somit ist die Schadenshöhe

$$I(O_0) = (160200;209700;259200) * (8;16;30) = (1281600;3355200;7776000).$$

In [OcCC2003] wurden Statistiken zu Elementarschäden veröffentlicht, die die Wiederkehrperioden von solchen Schäden bei Gebäuden und den jährlichen Gesamtschaden ausweisen. Umgerechnet auf einzelne Gebäude bzw. Gebäudeteile und auf Eintrittswahrscheinlichkeiten ergibt sich für das Rechenzentrum des Unternehmens eine jährliche Elementarschadenwahrscheinlichkeit von 0,78‰. Das entspricht einer Wiederkehrperiode (WP) von 1280 Jahren. Berücksichtigt man Minimum und Maximum dieser Statistik und eine weitere Statistik<sup>2</sup>, so ergibt sich für die Dreiecksverteilung der Eintrittswahrscheinlichkeit:

$$P_1 = (0,00036;0,00082;0,0084).$$

Somit ergibt sich in der Schreibweise der Dreiecksverteilung:

$$ALE_0 = (1281600; 3355200; 7776000) * (0,00036;0,00082;0,0084) = (461;2751;65318)$$

### Nutzenermittlung zum Sicherheitsbündel B<sub>1</sub>

Für ALE<sub>1</sub> (zum Bündel B<sub>1</sub>) lässt sich folgende Schätzung durchführen: Da ein Notfallrechenzentrum zur Verfügung steht, reduziert sich die MTTR für die iSeries-Anwendungen im Sinne der Dreiecksverteilung erheblich, für die anderen Anwendungen nicht:

MTTR<sub>1</sub> = (5;12;20), also Schadenshöhe I(O<sub>1</sub>) = (160200;209700;259200) \* (5;12;20) = (801000;2516400;5184000). Somit folgt für die jährliche Verlusterwartung bei Realisierung des Sicherheitsbündels B<sub>1</sub>

$$ALE_1 = (801000;2516400;5184000) * (0,00036;0,00082;0,0084) = (288;2063;43546)$$

Nun lässt sich der jährliche Nutzen berechnen:

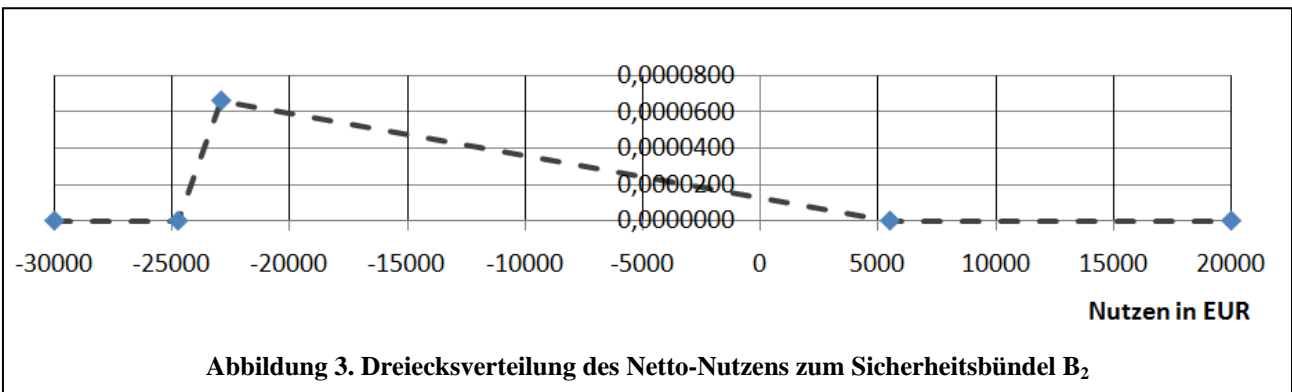
$$\text{Nutzen}_1 = ALE_0 - ALE_1 = (173; 688; 21772).$$

Der **jährliche Netto-Nutzen** wird zunächst konservativ berechnet, d.h. der Zusatznutzen wird nicht berücksichtigt: ZNutzen<sub>1</sub>=0.

Es verbleibt also die Berechnung der jeweiligen Kosten: Kosten<sub>0</sub> = 0; Kosten<sub>1</sub> = 3360+4800 = 8160.

NNutzen<sub>1</sub> = Nutzen<sub>1</sub> - Kosten<sub>1</sub> + ZNutzen<sub>1</sub> = (173; 688; 21772) - 8160 + 0, also

<sup>2</sup> Geschäftsdaten der Gebäudeversicherung Bern für die Jahre 2004 und 2005



**NNutzen<sub>1</sub> = (-7987; -7472; 13612).**

Mit a= -7987, b= 13612 und c= -7472 ergibt sich als kumulative Verteilungsfunktion F<sub>1</sub> zwischen a und c

$$F_{11}(x) = \frac{(x + 7987)^2}{21599 \cdot 515} = 8,99 \cdot 10^{-8} (x + 7987)^2$$

und zwischen c und b

$$F_{12}(x) = 1 - \frac{(13612 - x)^2}{21599 \cdot 21084} = 1 - 2,2 \cdot 10^{-9} (13612 - x)^2$$

Der Wendepunkt von F<sub>1</sub>(x) ist bei x=c.

F<sub>1</sub>(0) = P(Nutzen ≤ 0) = F<sub>12</sub>(0) = 1 - 2,2 · 10<sup>-9</sup> · (13612)<sup>2</sup> = 0,592 bzw. 59,2%. **Die Wahrscheinlichkeit, dass das Sicherheitsbündel B<sub>1</sub> einen Netto-Nutzen bringt, beträgt also 40,8%.** Hauptgrund für das mäßig günstige Nutzenergebnis ist die geringe Schadenseintrittswahrscheinlichkeit, aus der ein relativ geringer ALE resultiert.

Der statistische Erwartungswert für den Nettonutzen lässt sich mit der in Abschnitt 3. angegebenen Formel ermitteln:

$$E(\text{NNutzen}_1) = \frac{x_{\min} + x_w + x_{\max}}{3} = \frac{-7987 + (-7472) + 13612}{3} = -616 \text{ EUR}$$

Das bedeutet, der wahrscheinlichste Wert für den Nettonutzen bei Anwendung des Sicherheitsbündels B<sub>1</sub> beträgt -616 EUR, ist also knapp negativ.

### Nutzenermittlung zum Sicherheitsbündel B<sub>2</sub>

Für ALE<sub>2</sub> (zum Bündel B<sub>2</sub>) reduziert sich die MTTR weiter: MTTR<sub>2</sub> = (4;10;16), folglich ist

$$I(O_0) = (160200; 209700; 259200) * (4; 10; 16) = (640800; 2097000; 4147200).$$

Da P<sub>2</sub>=P<sub>1</sub> ist, ergibt sich als jährliche Verlusterwartung

$$\text{ALE}_2 = (640800; 2097000; 4147200) * (0,00036; 0,00082; 0,0084) = (231; 1720; 34836)$$

$$\text{Nutzen}_2 = \text{ALE}_0 - \text{ALE}_2 = (230; 2063; 30482), \text{Kosten}_2 = \text{Kosten}_1 + 14000 + 1440 + 1380 = 24980.$$

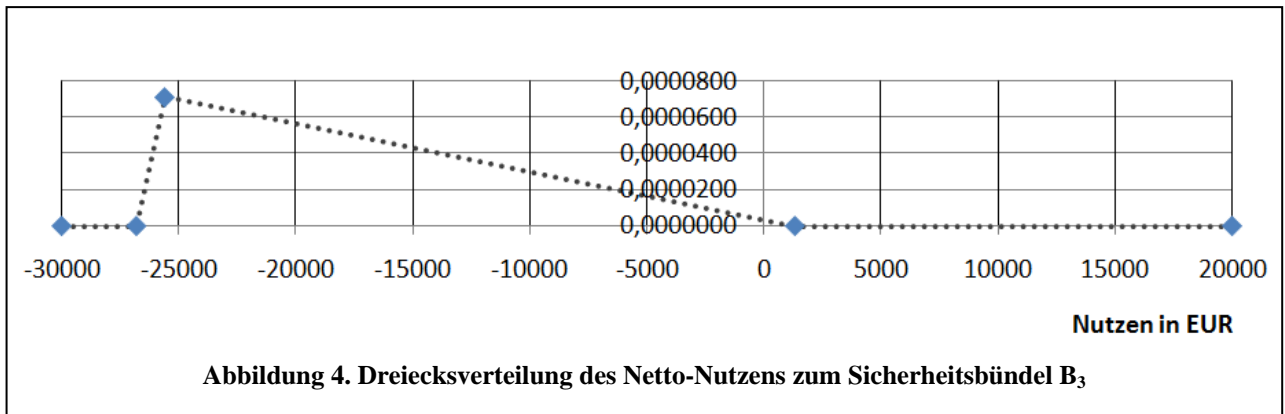
$$\text{NNutzen}_2 = \text{Nutzen}_2 - \text{Kosten}_2 + \text{ZNutzen}_2 = (230; 2063; 30482) - 24980 + 0, \text{ also}$$

$$\text{NNutzen}_2 = (-24750; -22917; 5502).$$

Als kumulative Verteilungsfunktion F<sub>2</sub> ergibt sich zwischen a=-24750 und c=-22917

$$F_{21}(x) = \frac{(x + 24750)^2}{30252 \cdot 1833} = 1,80 \cdot 10^{-8} (x + 24750)^2$$

und zwischen c=-22917 und b =5502



$$F_{22}(x) = 1 - \frac{(5502 - x)^2}{30252 \cdot 28419} = 1 - 1,16 \cdot 10^{-9} (5502 - x)^2$$

$F_2(0) = P(\text{Nutzen} \leq 0) = F_{22}(0) = 1 - 1,16 \cdot 10^{-9} \cdot 5502^2 = 0,96$  bzw. 96%. **Die Wahrscheinlichkeit, dass das Sicherheitsbündel B<sub>2</sub> einen Netto-Nutzen bringt, beträgt also nur 4%.**

Der Erwartungswert für den Nettonutzen ist deutlich negativ:

$$E(\text{NNutzen}_2) = \frac{x_{\min} + x_w + x_{\max}}{3} = \frac{-24750 + (-22917) + 5502}{3} = -14055 \text{ EUR}$$

### Nutzenermittlung zum Sicherheitsbündel B<sub>3</sub>

Für ALE<sub>3</sub> (zum Bündel B<sub>3</sub>) beträgt die MTTR nur noch MTTR<sub>3</sub> = (3;8;13), also also I(O<sub>0</sub>) = (160200;209700;259200) \* (3;8;13) = (480600; 1677600; 3369600).

Da P<sub>3</sub> = P<sub>1</sub> ist, ergibt sich als jährliche Verlusterwartung

$$\text{ALE}_3 = (480600; 1677600; 3369600) * (0,00036; 0,00082; 0,0084) = (173; 1375; 28305)$$

$$\text{Nutzen}_3 = \text{ALE}_0 - \text{ALE}_3 = (173; 1375; 28305), \text{Kosten}_3 = \text{Kosten}_2 + 2000 = 26980.$$

$$\text{NNutzen}_3 = \text{Nutzen}_3 - \text{Kosten}_3 + \text{ZNutzen}_3 = (173; 1375; 28305) - 26980 + 0, \text{ also}$$

$$\text{NNutzen}_3 = (-26807; -25605; 1325)$$

Als kumulative Verteilungsfunktion F<sub>3</sub> ergibt sich zwischen a=-26807 und c=-25605

$$F_{31}(x) = \frac{(x + 26807)^2}{28132 \cdot 1202} = 2,96 \cdot 10^{-8} (x + 26807)^2$$

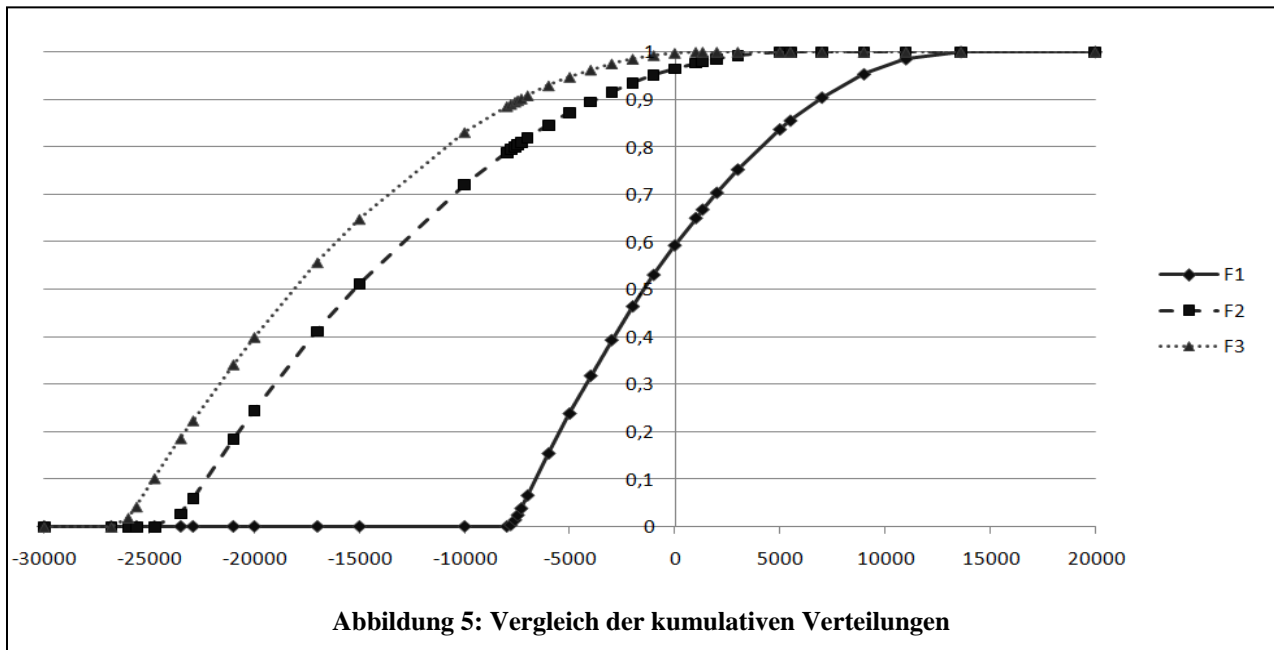
und zwischen c=-25605 und b = 1325

$$F_{32}(x) = 1 - \frac{(1325 - x)^2}{28132 \cdot 26930} = 1 - 1,32 \cdot 10^{-9} (1325 - x)^2$$

$F_3(0) = P(\text{Nutzen} \leq 0) = F_{32}(0) = 1 - 1,32 \cdot 10^{-9} \cdot 1325^2 = 0,998$  bzw. 99,8%. **Es bleibt nur eine Wahrscheinlichkeit von 0,2% für einen (positiven) Netto-Nutzen bei Anwendung des Sicherheitsbündels B<sub>3</sub>.**

Der Erwartungswert für den Nettonutzen von B<sub>3</sub> ist im Vergleich dementsprechend klein:

$$E(\text{NNutzen}_3) = \frac{x_{\min} + x_w + x_{\max}}{3} = \frac{-26807 + (-25605) + 1325}{3} = -17029 \text{ EUR}$$



Anhand von Abbildung 5 ist leicht zu erkennen, dass F1 F2 stochastisch dominiert und dass F2 F3 stochastisch dominiert. F1 ist also die stochastisch dominante Verteilungsfunktion. Dieses Ergebnis ist konsistent mit den berechneten Erwartungswerten:

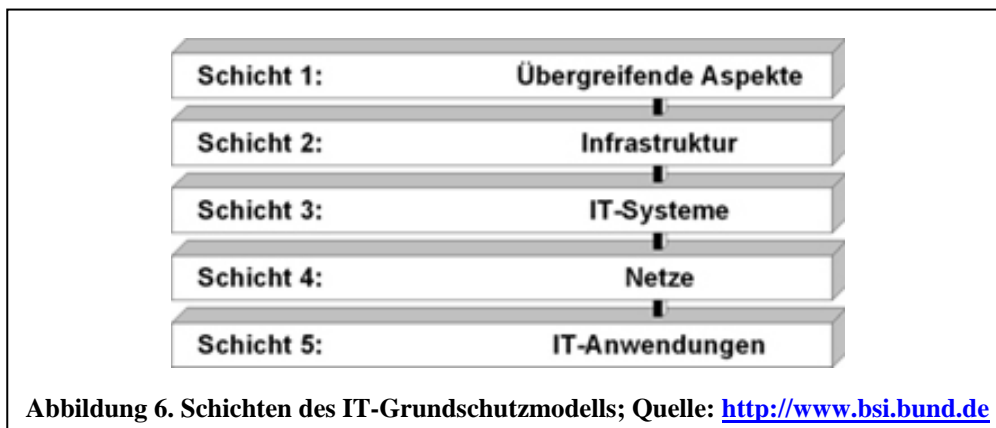
$$E(\text{Nutzen}_1) > E(\text{Nutzen}_2) > E(\text{Nutzen}_3) .$$

## 4.2 Fallbeispiel Grundschutzprojekt

Bei der hier betrachteten Organisation handelt es sich um die IT-Tochter eines kommunalen Unternehmens aus Mecklenburg-Vorpommern, die Dienstleistungen aus dem IT-TK-Bereich erbringt. Das IT-Grundschutzprojekt umfasste die Infrastruktur, Anlagen und Leistungen des Dienstleisters, wobei Server, Netze, Netzkomponenten und Arbeitsplatzsysteme untersucht wurden. Im weiteren Verlauf soll exemplarisch ein Baustein und ausgewählte Maßnahmen bezüglich ihres Nutzens untersucht werden. Der Baustein ist aus der Schicht 3 „IT-Systeme“ des BSI-Schichtenmodells ausgewählt, da hier anschauliche Bausteine zu finden sind: Baustein B 3.302 Router und Switches stellt die Gefährdungslage für aktive Netzkomponenten, also IT-Systeme dar und begegnet diesen Risiken mit angemessenen Maßnahmen. Folgender Sicherheitsvorfall  $O_1$  soll aus der Menge der Sicherheitsvorfälle ausgewählt werden:

*Der Switch für die Anbindung der Arbeitsplatzinfrastruktur der Kunden an den Serverraum ist aufgrund eines Hardwaredefektes nicht verfügbar und nicht wiederherstellbar.*

Die Schadenseintrittswahrscheinlichkeit  $P$  wurde im Rahmen einer Expertenbefragung mit (0,5 %; 1%; 1,25%) ermittelt. Die Untersuchung der Schadensauswirkung im Rahmen des IT-Grundschutzprojektes ergab 200.000 EUR pro Tag. Diese monetäre Schadensauswirkung ist in der Definition der Schutzbedarfskategorien des Unternehmens mit der Schutzbedarfskategorie „Sehr hoch“ klassifiziert. Sollten für den Switch keine weiteren Maßnahmen eines Sicherheitsbündels ergriffen werden, hat eine unternehmensinterne Expertenschätzung folgende wahrscheinliche Ausfallzeiten ergeben, die zu den dargestellten Schadensauswirkungen führen. Die Bandbreite der Werte ergibt sich aus dem minimalen (min), maximalen (max) und wahrscheinlichsten (mvl) Wert der geschätzten Ausfallzeit.



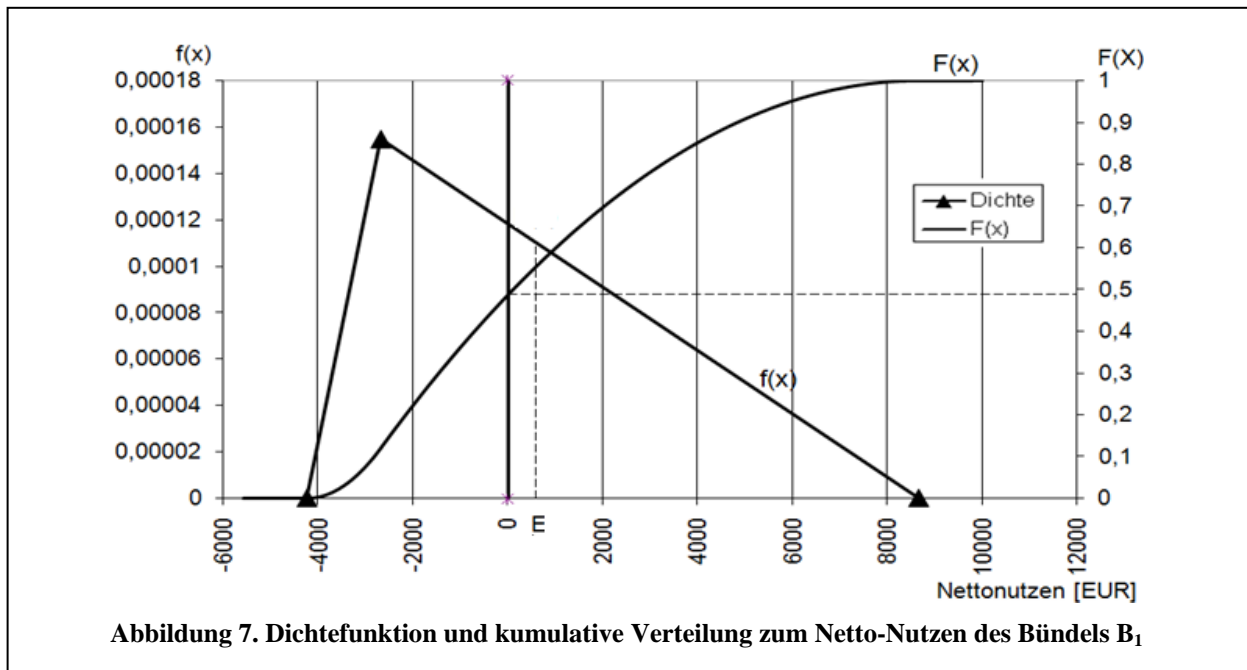
|     | Ausfall [d] | P [%] | Schadensauswirkung [EUR] |
|-----|-------------|-------|--------------------------|
| min | 0,25        | 0,50  | 25.000                   |
| mvl | 1,00        | 1,00  | 200.000                  |
| max | 5,00        | 1,25  | 1.250.000                |

Diesem möglichen Sicherheitsvorfall soll nun mit Maßnahmen begegnet werden. Diese sind an die Modellierung nach IT-Grundschutz angelehnt. Maßnahmen wie „M 1.43 Gesicherte Aufstellung aktiver Netzkomponenten“, die nicht im Rahmen des IT-Grundschutz-Projektes realisiert worden sind, sondern bereits umgesetzt waren, werden für dieses Sicherheitsbündel nicht berücksichtigt. Für jede Maßnahme ist  $E_f$  die anteilige Reduktion der *Häufigkeit des Auftretens* des Sicherheitsvorfalles  $O_1$  als Ergebnis der Einführung des Maßnahmenbündels  $B_1 = \{S_1, \dots, S_{11}\}$  sowie  $E_d$  die anteilige Reduktion der *Folgen des Auftretens* des Sicherheitsvorfalles  $O_1$  als Ergebnis der Einführung des Maßnahmenbündels  $B_1$  zu ermitteln.

| Maßnahme j für $O_1$ | Bezeichnung   | $E_f(O_1, S_j)$ [%] | $E_d(O_1, S_j)$ [%] | Kosten [EUR/a] |
|----------------------|---|---------------------|---------------------|----------------|
| 1 (M 2.279)          | Erstellung einer Sicherheitsrichtlinie für Router und Switches              | 1                   | 1                   | 144            |
| 2 (M 2.280)          | Kriterien für die Beschaffung und geeignete Auswahl von Router und Switches | 10                  | 0                   | 90             |
| 3 (M 2.281)          | Dokumentation der Systemkonfiguration von Routern und Switches              | 0                   | 10                  | 360            |
| 4 (M 2.282)          | Regelmäßige Kontrolle von Routern und Switches                              | 10                  | 10                  | 270            |
| 5 (M 2.283)          | Software-Pflege auf Routern und Switches                                    | 5                   | 0                   | 360            |
| 6 (M 3.38)           | Administratorenschulung für Router und Switches                             | 5                   | 5                   | 1000           |
| 7 (M 4.203)          | Konfigurations-Checkliste für Router und Switches                           | 0                   | 0                   | 90             |
| 8 (M 4.204)          | Sichere Administration von Routern und Switches                             | 5                   | 0                   | 45             |
| 9 (M 4.206)          | Sicherung von Switch-Ports  | 20                  | 0                   | 27             |
| 10 (M 6.91)          | Datensicherung und Recovery bei Routern und Switches                        | 0                   | 20                  | 360            |
| 11 (M 6.92)          | Notfallvorsorge bei Routern und Switches                                    | 0                   | 50                  | 1600           |

Die gesammelten Daten führen nun nach den Formeln von [SooHoo2000, S. 22 ff] zum Netto-Nutzen:

|     | Schadensauswirkung [EUR] | $ALE_0$ [EUR] | $ALE_k$ [EUR] | Nutzen [EUR] | Kosten [EUR] | Netto-Nutzen [EUR] |
|-----|--------------------------|---------------|---------------|--------------|--------------|--------------------|
| min | 25.000                   | 125,00        | 20,95         | 104,05       | 4.346,00     | <b>-4.241,95</b>   |
| mvl | 200.000                  | 2.000,00      | 335,21        | 1.664,79     | 4.346,00     | <b>-2.681,21</b>   |
| max | 1.250.000                | 15.625,00     | 2.618,82      | 13.006,18    | 4.346,00     | <b>8.660,18</b>    |



Die Zufallsvariable  $X$  repräsentiert hier den Nutzen der Anwendung des Sicherheitsbündels. Somit ergibt sich mit Hilfe der Dreiecksverteilung und der ermittelten Werte des Nettonutzens die Dichtefunktion  $f(x)$ , wobei hier  $f(-2681,21) = \frac{2}{\max - \min} = \frac{2}{8660,18 - (-4241,95)} \approx 0,000155$  (siehe Abbildung 7).

Der erwartete Nutzen für das Sicherheitsbündel  $B_1$  beträgt

$$E = E(\text{Nettonutzen}) = \frac{-4241,95\text{EUR} + (-2681,21\text{EUR}) + 8660,18\text{EUR}}{3} = 579,01 \text{ EUR.}$$

Der Verteilung des Nettonutzens für das Sicherheitsbündel wird in der kumulierten Wahrscheinlichkeitsverteilung deutlich, die neben der Dreiecksverteilung ebenfalls in Abbildung 7 dargestellt ist. Für den Praktiker besonders interessant ist  $F(0) = P(\text{NNutzen} \leq 0) \approx 0,49$ . **Durch die Schutzmaßnahmen  $S_1, \dots, S_{11}$  kann mit  $1 - 0,49 = 51\%$ -iger Wahrscheinlichkeit ein (positiver) Nettonutzen erzielt werden.**

Es ist fraglich, ob die Kombination der durchgeführten Maßnahmen optimal ist. Anhand eines entwickelten Werkzeuges auf Basis einer relationalen Datenbank kann die im Hinblick auf den Nutzen optimale Kombination der Maßnahmen ermittelt werden. Allerdings ist das angewendete Sicherheitsbündel bei einem durchgeführten Projekt nicht mehr änderbar, so dass nur Empfehlungen über die Fortführung bzw. Beendigung von Maßnahmen aufzeigt werden können.

## 5 Fazit und Ausblick

Der stochastische ROSI-Ansatz ist in der Praxis anwendbar und hinreichend aussagekräftig. Er wird der Tatsache, dass die Input-Daten bei der Risikoanalyse im Allgemeinen nicht genau sind, durch die Verwendung von Verteilungsfunktionen gerecht. Es werden nicht mehr scheinbar präzise Ergebnisse erzielt, sondern ein statistisches Ergebnisspektrum.

Im Einzelnen hat sich herausgestellt, dass die Vorhaltung eines Notfallrechenzentrums bei einem Unternehmen, wo bei Ausfall des Rechenzentrums kurzfristig nur mäßige Schäden anfallen, ohne Berücksichtigung von Zusatznutzen eher unwirtschaftlich ist. Andererseits ist die Höhe des Schadens, wenn der Sicherheitsvorfall eintritt, so groß, dass der Netto-Nutzen pro Jahr nicht das alleinige Entscheidungskriterium sein sollte.

Bei der Ex-Post-Analyse des Grundschutzbausteins hat sich hingegen ein leicht positiver Erwartungswert für den jährlichen Netto-Nutzen ergeben. Anhand dieses Beispiels ist gezeigt, dass es nicht unrealistisch ist, dass IT-Grundschutzprojekte auch insgesamt wirtschaftlich sein könnten. Hier sind weitere Untersuchungen erforderlich.

Auch bei einem stochastischen Ansatz ist weiterhin ein genaues Augenmerk auf die Inputdaten zu richten. Wenn die Schätzungen nicht hinreichend valide sind, kann der Erwartungswert für den Nutzen immer noch erheblich unzuverlässig sein.

Ein weiterer Schritt bei der Wirtschaftlichkeitsanalyse von IT-Sicherheitsmaßnahmen könnte die Prüfung der Anwendbarkeit des Verfahrens von Gordon und Loeb sein. In [GordonLoeb2002] wird ein ökonomisches Modell vorgestellt, mit dem sich unter Verwendung von Wahrscheinlichkeitsfunktionen und durch Anwendung von Differentialrechnung die optimale Höhe von Sicherheitsinvestitionen ermitteln lässt.

## 6 Literatur

[Berinato2002] Berinato, S.: Finally, a Real Return on Security Spending. In: CIO Magazine, Framingham, April 2002.

[Cavusoglu2004] Cavusoglu, H. et al.: A Model for Evaluating IT Security Investments, In: COMMUNICATIONS OF THE ACM, Vol. 47, No. 7, July 2004.

[GordonLoeb2002] Gordon, L.A.; Loeb, M. P.: The Economics of Information Security Investment. In: ACM Transactions on Information and System Security, Vol. 5, No. 4, S. 438–457. New York, 2002.

[OcCC2003] Organe consultatif sur les changements climatiques: Extremereignisse und Klimaänderung, Bern 2003.

[SooHoo2000] Soo Hoo, K.J.: How Much is Enough - a Risk Management Approach to Computer Security. Doctoral Thesis. Stanford, 2000.

[Zangemeister1976] Zangemeister, Christof: Nutzwertanalyse in der Systemtechnik – Eine Methodik zur multidimensionalen Bewertung und Auswahl von Projektalternativen. München, 1976