in: Sicherheit 2005. Beiträge der 2. Jahrestagung des GI-Fachbereichs Sicherheit, Lecture Notes in Informatics (P-62), Köllen-Verlag, Bonn 2005, 15-26

Ansätze zur Evaluierung von Sicherheitsinvestitionen

Thomas Nowey, Hannes Federrath, Christian Klein, Klaus Plößl

Lehrstuhl Management der Informationssicherheit,
Universität Regensburg, D-93040 Regensburg
{thomas.nowey, hannes.federrath, klaus.ploessl}@wiwi.uni-regensburg.de

Abstract: Das vorliegende Papier zeigt auf, welche besonderen Anforderungen für eine Kosten-Nutzen-Betrachtung von Sicherheitsinvestitionen bestehen und liefert eine Systematik, mit deren Hilfe Ansätze für ein objektiviertes Management von Sicherheitsinvestitionen diskutiert werden können. Bestehende Ansätze in diesem Umfeld, insbesondere das derzeit populäre ROSI-Konzept, werden vorgestellt. Aufbauend auf dieser Grundlage werden Empfehlungen zur Verbesserung des Vorgehens gemacht und Ansätze für weitere Forschungsarbeiten geliefert.

1 Einleitung

Sicherheitsmaßnahmen lassen sich erfahrungsgemäß leicht durch Gefährdungen motivieren. Dies erklärt, warum in der Vergangenheit das so genannte FUD-Prinzip (Fear, Uncertainty and Doubt) bei Entscheidungen über Investitionen in IT-Sicherheit dominierend war. Stark subjektiv geprägte Entscheidungen, die im Rückblick nur schwer nachzuvollziehen und zu überprüfen sind, waren die Folge. In Zeiten von Managed Security Services und Total Cost of Ownership bedarf es jedoch einer objektiveren Vorgehensweise in Form einer fundierten Kosten-Nutzen-Rechnung.

Nachdem es erste Ansätze bereits in den 80er Jahren gegeben hatte, wurde das Thema besonders in den vergangenen drei Jahren angesichts knapper werdender Budgets wieder verstärkt aufgegriffen. Das verdeutlicht vor allem das seit 2002 diskutierte und propagierte Schlagwort des Return on Security Investment (ROSI), das bereits durch die Namensanalogie zum klassischen ROI der Investitionsrechnung eine budgetmäßige Kontrolle und eine greifbare Nutzenmessung der IT-Sicherheit verspricht.

Die Kosten-Nutzen-Betrachtung verfolgt zwei Zielsetzungen. In der ex ante Betrachtung soll die Abwägung von Kosten und Nutzen einer Sicherheitsmaßnahme die objektive Entscheidung für oder gegen die Maßnahme ermöglichen. Ex post sollen die getroffenen Entscheidungen nachvollziehbar und überprüfbar sein. Aufgrund der besonderen Natur von Sicherheitsinvestitionen stößt man dabei aber schnell auf erhebliche Messprobleme, sowohl auf der Kosten- als auch auf der Nutzenseite.

Auf der Kostenseite müssen zunächst Ausgaben für Anschaffung, Einführung und laufenden Betrieb berücksichtigt werden (z.B. Kaufpreis, Installationsaufwand, Mitarbeitschu-

lungen und Wartungskosten). Daneben entstehen aber unter Umständen auch kaum quantifizierbare Kosten aus der Veränderung betrieblicher Abläufe und/oder veränderter Mitarbeitermotivation (z.B. durch mangelndes Verständnis für eine zusätzlich zu durchlaufende Sicherheitsprüfung). In der Praxis ist die budgetmäßige Erfassung der Sicherheitskosten noch nicht weit fortgeschritten (vgl. [VV02]).

Noch schwieriger als die Erfassung der Kosten von Sicherheitsmaßnahmen gestaltet sich die Quantifizierung ihres Nutzens. Dies ist vor allem in der unterschiedlichen Struktur der Zahlungsströme bei Investitionen in IT-Sicherheit gegenüber klassischen IT-Projekten begründet. Während in der klassischen Investitionsrechnung einer Anschaffungsauszahlung üblicherweise ein Strom von Einzahlungen als Nutzen gegenübersteht, liegt der Nutzen einer Sicherheitsmaßnahme in der Verhinderung drohender Auszahlungen, die durch entsprechende Schäden verursacht werden könnten. Der Nutzen einer Sicherheitsmaßnahme liegt also stets darin, die Verluste durch Sicherheitsvorfälle zu reduzieren. Dabei sind aber sowohl der Eintritt des Schadensereignisses als auch die Höhe der dann entstehenden Auszahlung ungewiss. Die Kosten beim Eintritt eines Schadensereignisses lassen sich in direkte Kosten, Wiederherstellungskosten und Kosten der Folgeschäden unterteilen. Während sich direkte Kosten und Wiederherstellungskosten in der Regel noch eher beziffern lassen, ist dies für Folgeschäden nahezu unmöglich. Neben Reputationsschäden sind in diesem Bereich auch Personenschäden, Störungen im Ablauf betrieblicher Prozesse oder sogar das Ende der Geschäftstätigkeit denkbar.

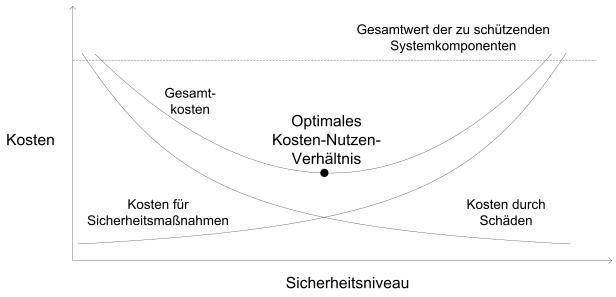

Abbildung 1: Kosten-Nutzen-Verhältnis von Sicherheitsmaßnahmen [HP03, S. 280]

Nach [HP03] verfolgt Sicherheitsmanagement vorrangig die „konfliktären Ziele maximales Sicherheitsniveau und minimale Kosten für Sicherheit“. Abbildung 1 macht diesen Zusammenhang deutlich. Es ist offensichtlich, dass die beiden Extremfälle, maximale mögliche Ausgaben für Sicherheitsmaßnahmen und keine Sicherheitsmaßnahmen, wirtschaftlich nicht sinnvoll sind. Ein Sicherheitsniveau nahe dem maximal erreichbaren ist mit sehr hohen Kosten verbunden (rechte Seite der Darstellung), da aufgrund eines abnehmenden Grenznutzens die Kosten für jede Steigerung im Sicherheitsniveau überproportional steigen. Minimale Ausgaben für Sicherheit können ebenfalls kein Ziel sein. Werden im Extremfall keine Maßnahmen getroffen, so bleibt das System ungeschützt und es sind unverhältnismäßig hohe Schäden zu erwarten (linke Seite der Darstellung). Gesucht wird also das Bündel aus Sicherheitsmaßnahmen, bei dem die Summe aus zu erwartenden Schäden und Kosten der Maßnahme minimal ist.

Das vorliegende Papier soll einen Beitrag zur Entwicklung einer Kosten-Nutzen-Betrachtung leisten, welche die oben dargestellten Anforderungen erfüllt. Zunächst werden in Kapitel 2 bestehende Ansätze vorgestellt. Als Basis für eine systematische Betrachtung des Themas und als Ausgangspunkt einer veränderten Vorgehensweise wird anschließend eine Risikomangement-Systematik vorgestellt. Kapitel 4 liefert ausgehend von der entwickelten Systematik Anregungen für ein praktikables Vorgehen. Kapitel 5 diskutiert offene Fragen und zeigt weitere Schritte auf.

2 Bisherige Arbeiten

2.1 Basisvarianten

Soo Hoo [SH00] unterscheidet bei den vor dem Erscheinen seiner eigenen Arbeit im Jahr 2000 veröffentlichten Ansätzen zwei Generationen. Diese stellen gewissermaßen die beiden möglichen Extreme bezüglich der Untersuchungsintensität dar und sollen deshalb als Basisvarianten kurz dargestellt werden.

Als erste Generation bezeichnet er die Ansätze, die auf dem Konzept der ALE (Annual Loss Expectancy), der jährlichen Verlusterwartung, basieren. Dieses Konzept ist im klassischen Risikomangement häufig anzutreffen. Vor der Berechnung muss zunächst ein Bedrohungsmodell erarbeitet werden, das heißt, es müssen alle möglichen Schadensereignisse identifiziert werden. Diese sind anschließend jeweils bezüglich Schadenshöhe und jährlicher Schadenshäufigkeit zu bewerten. Die jährliche Verlusterwartung berechnet sich dann als Produkt dieser beiden Größen. Diese quantitativen Ansätze decken den kompletten Risikomangement-Zyklus ab. Der Einsatz der ALE-Ansätze für Sicherheitsinvestitionen wurde in Amerika in den 80er Jahren vor allem aufgrund der Förderung durch das NIST stark vorangetrieben. Nach dem Ende dieser Projekte verschwanden ALE-Konzepte nahezu völlig von der Bildfläche. Für das Scheitern macht Soo Hoo drei Gründe aus: Die zu große Komplexität des Bedrohungsmodells, die vollständig deterministischen Modelle, die voraussetzten, dass alle Größen im Voraus genau bekannt sind, sowie eine zu große Abhängigkeit von einer fundierten Datenbasis.

Als Reaktion auf die hohe Komplexität der Modelle der ersten Generation nahmen die Modelle der zweiten Generation zum Teil starke Vereinfachungen vor, indem Unsicherheiten ausgeblendet wurden oder rein qualitativ orientierte Analysen durchgeführt wurden. Zu diesen Ansätzen zählt Soo Hoo

- das Integrated Business Risk-Management Framework, ein nicht-technisches Modell, welches hauptsächlich von Management Consulting Firmen propagiert wurde und wird,
- rein wertorientierte Methoden, die sich unter Ausblendung des Risikos ausschließlich am Wert der zu schützenden Assets orientieren,
- Szenario-Analysen, welche bestimmte Bedrohungsszenarien durchspielen,

- Best Practice Ansätze, die Standard-Empfehlungen geben, ohne individuelle Gegebenheiten zu berücksichtigen.

Soo Hoo sieht in diesen Ansätzen lediglich eine Zwischenlösung. Er kritisiert insbesondere das Ausblenden von technologischen Aspekten und die mangelnde Fähigkeit, Schutzmaßnahmen ökonomisch zu rechtfertigen oder deren Effektivität überprüfbar zu machen.

2.2 Neuere konzeptionelle Arbeiten

Sicherheitsinvestitionsentscheidungen erweisen sich als äußerst komplex und ihre Determinanten sind weder präzise vorhersagbar noch sind die Entscheidungen rein technischer Natur (vgl. z.B. [And01]). So wurden in den letzten Jahren verschiedene konzeptionelle Arbeiten publiziert, die versuchen, neue Einsichten in die Thematik zu gewinnen. Die unseres Erachtens wichtigsten Konzepte werden im Folgenden kurz vorgestellt.

Soo Hoo Soo Hoo selbst entwirft in seiner Arbeit ein entscheidungsbasiertes Modell, mit dem er versucht, die Unzulänglichkeiten der ersten beiden Generationen zu überwinden. Dazu bedient er sich der Technik der „Decision Analysis“ verbunden mit einer Modellierungstechnik, die auf so genannten „Influence Diagrams“ basiert. Mit dem Modell von Soo Hoo lassen sich verschiedene Bündel von Sicherheitsmaßnahmen – im Modell als Policies bezeichnet – auf ihren Netto-Nutzen hin vergleichen. Dieser Nutzen ergibt sich im Wesentlichen als Differenz der jeweiligen ALE-Werte. Neben einer reinen ALE-Betrachtung wird mit den Hilfsmitteln der „Decision Analysis“, wie beispielsweise Sensitivitätsanalysen, geprüft, wie sich das Modell und damit die Dominanz bestimmter Alternativen bei leicht variierten Annahmen und Parametern ändert.

Das Modell ermöglicht verschiedene Grundannahmen und lässt die Integration von Vergangenheitsdaten und Expertenurteilen zu. Die Zielgrößen sind quantiativer Natur, die Modellkonzeption ermöglicht aber variierende Detaillierungsgrade der Modellierung für die einzelnen Bereiche. In einem ersten Modellierungsschritt können so für alle Parameter grobe Schätzwerte verwendet werden. In weiteren Iterationen können einzelne Aspekte dann detailliert betrachtet werden. Die Schwierigkeit, geeignete Ausgangsdaten zu finden, die dem Modell mit allen andern gemein ist, wird durch die Integration von Wahrscheinlichkeitsverteilungen abgemildert, jedoch nicht beseitigt. In seinem Beispiel verzichtet Soo Hoo zudem darauf, schwierig darstellbare Aspekte wie Opportunitätskosten, Vertrauensschäden, etc. einzubeziehen.

Sicherheitsmaßnahmen können sich im Modell sowohl auf die Häufigkeit der Schadensereignisse als auch auf die Höhe des eintretenden Schadens auswirken. Diese Parameter müssen unternehmensindividuell als Prozentgröße geschätzt werden. Weiterhin muss eine Annahme über die zukünftige Entwicklung von Schadensereignissen getroffen werden. Zur Ermittlung des besten Bündels aus Sicherheitsmaßnahmen gibt es derzeit keine Alternative zur vollständigen Enumeration sämtlicher Möglichkeiten. Alle Maßnahmen werden isoliert betrachtet, wechselseitige Beeinflussungen werden ignoriert. Das Modell ist rein quantitativ orientiert und basiert letztlich auf einer ALE-Betrachtung mit erweiter-

ten Analysetechniken. Ein besonderer Zusatznutzen entsteht für den Anwender durch die Modellierung der verschiedenen Einflussfaktoren der Entscheidung, die wertvolle Einblicke in Ursache-Wirkungs-Zusammenhänge geben kann. Wie diese Zusammenhänge sich darstellen, muss aber letztlich durch das Unternehmen selbst ermittelt werden.

Das Modell hat nach Kenntnis der Autoren bislang keine nennenswerte Verbreitung gefunden. Dennoch erscheint die Grundidee mit graphischer Modellierung, wählbarem Detaillierungsgrad und ausgefeilten Analysetechniken sinnvoll.

Gordon / Loeb Gordon und Loeb haben ein abstraktes ökonomisches Modell entwickelt [GL02], mit dem sich auf Basis von Verteilungsfunktionen die optimale Höhe von Sicherheitsinvestitionen zum Schutz einer bestimmten Information ermitteln lässt. Für eine Information müssen dazu die Verletzlichkeit der Information und der mögliche Schaden im Falle eines Sicherheitsvorfalls bekannt sein. Wie alle ökonomischen Modelle, basiert auch jenes von Gordon und Loeb auf zahlreichen Annahmen, wie z.B. Risikoneutralität der Unternehmen oder Einperiodigkeit der Betrachtung. Die wesentlichen Erkenntnisse des Modells sind:

- Unter den getroffenen Modell-Annahmen kann es für Unternehmen ökonomisch sinnvoll sein, nur in Sicherheitsmaßnahmen zum Schutz von Informationen mit mittlerer Verletzlichkeit zu investieren. Bei extrem hoher oder extrem niedriger Verletzlichkeit kann es dagegen ökonomisch gerechtfertigt sein, keine oder nur geringe Investitionen in IT-Sicherheitsmaßnahmen zu tätigen.
- Auch im Bereich der ökonomisch sinnvollen Sicherheitsinvestitionen sollte die Höhe der Sicherheitsinvestitionen nur einen bestimmten Anteil des maximal möglichen Schadens betragen. Für die betrachteten Modelle sollte dieser Anteil laut Gordon und Loeb nie über 37 % des maximalen Verlustes liegen.

Das Modell ist eher theoretischer Natur und enthält keine Hinweise für die praktische Umsetzung. Auch für die Ermittlung der relevanten Parameter, Verletzlichkeit, Wahrscheinlichkeit einer Bedrohung und möglicher Schaden bei einem Sicherheitsvorfall, wird kein Weg vorgeschlagen. Eine Kritik des Modells findet sich zusmmen mit Erweiterungsvorschlägen bei Matsuura [Mat03].

Cavusoglu et al. Nachdem von verschiedenen Autoren (vgl. [GL02],[SH00]) eine spieltheoretische Untersuchung der Thematik im Hinblick auf das Wechselspiel zwischen Angreifer und Unternehmen angeregt wurde, haben Cavusoglu et al. [CMR04] ein entsprechendes Modell entwickelt. Es orientiert sich an einer dreischichtigen Sicherheitsarchitektur: Eine präventive Ebene, die in Form einer Firewall realisiert ist, eine detektive Ebene, realisiert durch ein IDS und schließlich eine reaktive Ebene, welche für die manuelle Inspektion steht. Um Sicherheitsinvestitionen zu evaluieren bestimmt das Unternehmen die optimale Häufigkeit für manuelles Monitoring bei verschiedenen Firewall- und IDS-Systemen und Konfigurationen. Dabei repräsentiert die Differenz aus den Kosten für dieses Monitoring ohne Firewall und IDS und den Kosten mit dem betrachteten System den

Wert des Systems für die Firma. Das Unternehmen wählt dann diejenige Technologie aus, bei der die Ersparnis relativ zu den Anschaffungskosten maximal ist. Zur Berechnung der jeweiligen Kosten müssen Parameter bestimmt werden, die dann in ein Modell der Spieltheorie eingehen. Das Modell enthält keine Elemente zur Identifikation der Bedrohungen.

Hat man die benötigten Parameter einmal bestimmt, lassen sich mit dem Modell relativ leicht Berechnungen und auch Was-wäre-wenn-Analysen für verschiedene Szenarien durchführen. Die Integration der spieltheoretischen Aspekte trägt zu einer umfassenderen Sicht der Thematik bei. Problematisch für die praktische Anwendbarkeit ist vor allem die Vielzahl an Parametern. So müssen Kosten- und Qualitätsparameter bekannt sein, beispielsweise die Wahrscheinlichkeit, dass ein Angreifer die Firewall überwinden kann. Zudem müssen bezüglich eines möglichen Hackers und der Firma ingesamt zehn Parameter geschätzt werden, die das Modell entscheidend beeinflussen. Sind all diese Parameter bekannt, so lassen sich zwar mit Hilfe der Spieltheorie präzise und nachvollziehbar verschiedene Technologien auf ihr Kosten-Nutzen-Verhältnis für das Unternehmen hin analysieren, letztlich hängt die Aussagekraft jedoch von den zuvor bestimmten Parametern ab. Zu deren Ermittlung geben die Autoren in ihrer Publikation jedoch keine Hilfestellung.

Ansätze von Beratungsunternehmen Besonders in den letzten Jahren werben zahlreiche Beratungs- und Sicherheitsunternehmen mit Vorgehensmodellen für das Management von Sicherheitsrisiken. Dabei handelt es sich aber in der Regel um selbst entwickelte Modelle, die nicht oder nur teilweise offen gelegt werden. Für einen kurzen Einblick in die Ansätze von KPMG und PwC zur Identifikation und Analyse von Risiken im IT-Bereich vgl. [RD04].

2.3 ROSI

Der ROSI steht seit dem Jahr 2002 bei Diskussionen um die Wirtschaftlichkeit von Sicherheitsinvestitionen im Mittelpunkt und verspricht eine solide Basis für Investitionsentscheidungen. Diese Denkweise stößt vor allem beim IT-Management auf Interesse und wird von Sicherheits-Anbietern verstärkt für den Marktauftritt genutzt.

Bei der Entwicklung des Ansatzes stand die Wirtschaftlichkeitsanalyse von *Intrusion Detection Systemen (IDS)* im Mittelpunkt. Als Basis für ROSI diente die ALE, die wie erwähnt bereits in den 70er Jahren entwickelt wurde (vgl. [FIP74]). Das Konzept in seiner bisherigen Form hat seinen Ursprung in zwei Projekten, die in den Jahren 2000 und 2001 an der *University of Idaho* und der *Stanford University* unabhängig voneinander durchgeführt wurden. Nach der Veröffentlichung eines Artikels im CIO Magazine [Ber02] stieß die Kennzahl rasch auf Interesse.

Bisher bestehen keine Standards für die Berechnung. So ist unklar, ob die Zahl absolut oder relativ ist und welche Parameter in den ROSI eingehen. Tabelle 1 zeigt das einfache Rechenbeispiel, das beim Experiment in Idaho [W$^+$01] aufgestellt wurde. Der jährlich zu erwartende Verlust durch einen Netzwerkeindringling beträgt $100.000 (Schadenshöhe $200.000, Schadenshäufigkeit einmal in zwei Jahren). Die jährlichen Kosten für

ein IDS, welches den Schaden mit 85 %-iger Wahrscheinlichkeit verhindern kann betragen $40.000. Somit ergibt sich für das IDS ein ROSI von $45.000.

ALE ohne IDS:	$200.000 x 1/2	$100.000
− ALE mit IDS:	$200.000 x 1/2 x (1 − 0,85)	$15.000
− Kosten des IDS:		$40.000
ROSI		$45.000

Tabelle 1: Beispielrechnung für ROSI

Bewertung Der ROSI besticht zunächst durch seine einfache, klare Aussage. Die nähere Betrachtung der Kennzahl macht jedoch deutlich, dass die Diskussion der Methode mangels einer standardisierten Vorgehensweise nur sehr oberflächlich stattfindet. Der ROSI selbst stellt lediglich die Verdichtung vorheriger quantitativer Betrachtungen in Form einer Spitzenkennzahl dar. Diese ist aber in ihrem Steuerungsgehalt eingeschränkt, da Wahrscheinlichkeitsverteilungen der Größen gänzlich ausgeklammert werden. Zudem wird vorausgesetzt, dass alle relevanten Einflussfaktoren in monetäre Größen überführt werden können. Die durch den Begriff versprochene „Return-Aussage“ kann durch die bisher bekannten Verfahren nicht gehalten werden. Eine solche ist aus Sicht der Autoren aufgrund der eingangs dargestellten Charakteristika von Sicherheitsinvestitionen auch gar nicht möglich. Letztlich handelt es sich beim ROSI um eine Standard-ALE-Methode, die keine wesentlichen Neuerungen enthält.

2.4 Fazit

Wie die Ausführungen zu existierenden Arbeiten zeigen, gibt es eine gewisse Zahl von Ansätzen im Bereich der Evaluation von Sicherheitsinvestitionen. Jedoch konnte sich bislang noch keiner durchsetzen. Jede Vorgehensweise hat gewisse Unzulänglichkeiten und ist nur unter Restriktionen anwendbar. Da viele Ansätze nur auf Teilbereiche des Risikomangementkreislaufes fokussieren, gibt es kaum durchgängige Konzepte. Ein gemeinsames Problem aller Vorschläge ist das Fehlen einer geeigneten Datenbasis. Die Datengewinnung wird entweder gänzlich ausgeklammert, oder es wird vorausgesetzt, dass geeignete Daten bereits vorliegen.

3 Risikomangement-Systematik

3.1 Matrix zur Systematisierung

Die vorgestellten Ansätze konzentrieren sich auf unterschiedliche Bereiche der Kosten-Nutzen-Abwägung und führen diese mit unterschiedlichem Detaillierungsgrad durch. Aus diesem Grund soll im Folgenden eine Systematisierung von möglichen Ansätzen im Umfeld der Evaluation von Sicherheitsrisiken entwickelt werden. Diese ermöglicht eine Be-

trachtung entlang der Schritte des Risikomangements kombiniert mit drei unterschiedlichen Detaillierungsgraden und dient gleichzeitig als Grundlage für ein neues Vorgehen. Abbildung 2 zeigt die Kombination der beiden Dimensionen in einer Matrix.

Abbildung 2: Risikomangement-Systematik für Sicherheitsinvestitionen

3.2 Schritte des Risikomangements

Bei der Kosten-Nutzen-Betrachtung von IT-Sicherheitsinvestitionen, geht es letztlich um das optimale Management der IT-Sicherheitsrisiken. Es ist daher nur konsequent, sich für die Entscheidung, ob und wie ein bestimmtes Sicherheitsrisiko behandelt werden soll, der Methoden des Risikomangements zu bedienen.

Nach [GK03] lässt sich Risikomangement in vier Teilschritte unterteilen, nämlich in Risikoidentifikation, Risikobeurteilung, Risikosteuerung und Risikoüberwachung. Risikoidentifikation bezeichnet die Erfassung der relevanten Risiken einer Organisation sowie deren Interdependenzen. Im Schritt der Risikobeurteilung werden die identifizierten Risiken nach der vorgegebenen Zielsetzung bewertet und gegebenenfalls aggregiert. Ziel der Risikosteuerung ist die Auswahl der Sicherheitsmaßnahmen, die das eingangs dargestellte Optimierungsproblem lösen. Diese vier Schritte bilden die erste Dimension der vorliegenden Systematik, wobei der Schritt der Risikoüberwachung in Form einer wiederholten Anwendung der drei vorhergehenden Schritte integriert wird.

3.3 Detaillierungsgrad des Risikomanagements

Nicht immer ist eine quantitative Erfassung aller Einflussfaktoren auf Kosten oder Nutzen von Sicherheitsinvestitionen möglich oder sinnvoll. Dies liegt zum Einen daran, dass verschiedene Faktoren einfach nicht präzise mess- oder vorhersagbar sind, zum Anderen aber auch an dem hohen Aufwand zur Ermittlung aussagekräftiger Messergebnisse, welcher nicht immer gerechtfertigt ist. So haben sich im Laufe der Zeit neben quantitativen auch

qualitative und Best-Practice- oder Grundschutzansätze entwickelt.

Grundschutzmaßnahmen ermöglichen Risikosteuerung auf Basis von Best-Practice. Auf eine individuelle Abwägung von Kosten und Nutzen der Sicherheitsmaßnahmen wird verzichtet. Stattdessen erfolgt der Kosten-Nutzen-Vergleich implizit bei der Erstellung der Best-Practice-Empfehlungen. Für Entscheidungen über alternative Sicherheitsmaßnahmen gleicher Art, z.B. von verschiedenen Herstellern, geben Grundschutzverfahren keine Hilfestellung. Es werden lediglich Maßnahmenkategorien empfohlen. Der Best-Practice-Ansatz stellt einen praktikablen Lösungsweg vor, der im Vergleich zu einer detaillierten Risikoanalyse nur wenig Planungsaufwand erfordert und Unternehmen zumindest die Gewissheit gibt, ein allgemein anerkanntes Sicherheitsniveau erreicht zu haben.

Qualitative Risikoanalyse ermöglicht die eingehende Untersuchung eines IT-Teilsystems mit vertretbarem Aufwand. Der qualitative Ansatz berücksichtigt bestehende Gefährdungen und Werte und bildet damit die individuelle Risikosituation besser ab als der Grundschutzansatz. Anders als bei der quantitativen Risikoanalyse erfolgt jedoch keine Bewertung mit monetären Größen. Die Verfahrensweise eignet sich besonders gut zur Bewertung subjektiver Einflussfaktoren oder für Systeme mit mittlerem bis hohem Schutzbedarf. Als Methoden kommen beispielsweise Szenariokonzepte, Simualtionskonzepte (vgl. [Ste02]) oder der Analytic Hierarchy Process (vgl. [Saa94]) in Frage. Qualitatve Risikoanalyse ist als Ergänzung zum Grundschutzansatz geeignet, ist aber auch mit zusätzlichem Aufwand verbunden. Im Gegensatz zum Grundschutzansatz ist die Auswahl technischer Alternativen möglich.

Quantitative Risikoanalyse bezeichnet den umfassendsten Ansatz, Risiken zu messen und zu bewerten. Das erreichte Sicherheitsniveau wird mit rechenbaren Größen dargestellt und darauf basierend präzise Risikosteuerung mit hoher Informationsqualität ermöglicht. Zu den bedeutendsten Vertretern gehören die auf der *ALE (Annualized Loss Expectancy)* basierenden Verfahren. Das Ergebnis in Form von monetären Größen überzeugt durch leichte Verständlichkeit. Durch eine Bewertung von Kosten und Nutzen der Sicherheitsmaßnahmen mit Geldeinheiten bietet die quantitative Risikoanalyse gute Voraussetzungen für eine Wirtschaftlichkeitsanalyse. Der Einsatz solcher Instrumente lohnt sich allerdings nur, wenn die zu erwartende Effizienzsteigerung den zusätzlichen Aufwand rechtfertigt. Dies trifft in der Regel für IT-Systeme zu, die den Kernbereich der Geschäftstätigkeit bilden und großteils aus individuellen IT-Lösungen bestehen.

4 Verbesserungsvorschläge für ein praktikables Vorgehen

4.1 Integration aller drei Detaillierungsebenen

Den leicht zu realisierenden Grundschutzansätzen fehlt die individuelle Anpassbarkeit, während aufwendige quantitative Modelle in ihrer Komplexität kaum beherrschbar sind. Dieses Dilemma lässt sich unserer Ansicht nach nur durch die geschickte Kombination aller drei Detaillierungsebenen lösen. Ein solches Vorgehen ist besonders dann attraktiv, wenn der Übergang zwischen den einzelnen Detaillierungsgraden einfach erfolgen kann

und bestehende Daten weiterverwendet werden können.

Eine solche Integration der verschiedenen, unterschiedlich detaillierten Daten erfordert spezielle Techniken. Zwar wird mit der Kosten-Nutzen Analyse (KNA), die in der Praxis auch zur Bewertung von Sicherheitsinvestitionen genutzt wird (vgl. [Mer03]), bereits eine Kombination quantitativer und nicht-quantitativer Faktoren möglich, jedoch erfolgt der Einbezug qualitativer Daten erst in einem nachgelagerten Analyseschritt. Als Alternative bietet sich beispielsweise der Analytic Hierarchy Process an. Eine Gesamtsicht, die nicht nur Steuerungs- sondern auch Kontrollcharakter hat, wäre mit Hilfe einer zu entwickelnden Scorecard in Anlehnung an das Balanced Scorecard Konzept zu realisieren. In vielen Unternehmen sind nicht alle Prozesse und damit auch nicht alle Systeme in gleichem Maße gefährdet. Auf einer niedrigen Detaillierungsebene können mit geringem Aufwand die Bereiche bestimmt werden, für die eine tiefer gehende qualitative oder quantitative Betrachtung überhaupt notwendig ist.

Das Risikoportfolio als grafisches Hilfsmittel erscheint uns geeignet eine solche Komplexitätsreduktion zu erreichen. Es ordnet Risiken anhand der Dimensionen Häufigkeit und Schadenshöhe ein. [JR02, S. 80] verbindet Risikoportfolios mit Empfehlungen für die Risikosteuerung (vgl. Abbildung 3). Hierzu werden die möglichen Schadensereignisse auf jeder Dimension einer von zwei Gruppen zugeordnet. Bei der Schadenshäufigkeit unterscheidet man Low Frequency (LF) und High Frequency (HF), während bei der Schadenshöhe zwischen Low Impact (LI) und High Impact (HI) differenziert wird. Somit ergeben sich vier verschiedene Schadenstypen denen jeweils eine Empfehlung für die Behandlung des jeweiligen Risikos zugeordnet wird. Damit eignen sich Risikoportfolios für einen Überblick über die Risikosituation und zusätzlich zur Vorauswahl von Maßnahmen auf strategischer Ebene. So kann leicht ermittelt werden, für welche Risiken eine genauere Betrachtung – mit Hilfe von qualitativen und quantitativen Methoden – lohnt. Für die übrigen Risiken können auf Basis des Risikoportfolios andere Risikobehandlungsstrategien, insbesondere Versicherungen, gewählt werden.

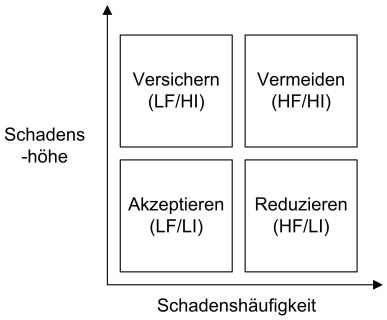

Abbildung 3: Risikoportfolio mit Handlungsempfehlungen nach [JR02, S. 80]

4.2 Neuorientierung bei der Risikoidentifikation

Wie der Blick auf bestehende Ansätze gezeigt hat, ist eine aussagekräftige Datenbasis die Voraussetzung für die weiteren Schritte des Risikomangements. Gerade an solchen Daten mangelt es aber derzeit noch. Für den Bereich des Grundschutzes sollte eine solche Datenbasis zumindest eine differenzierte Kategorisierung der Unternehmen ermöglichen. Als sinnvolle Dimensionen erscheinen hier einerseits die IT-Abhängigkeit der Prozesse im Unternehmen (je höher die Abhängigkeit, desto geschäftskritischer ist ein möglicher Schadensfall) und andererseits die Unternehmensgröße (je größer ein Unternehmen, desto größer die Komplexität der Infrastruktur). Mit Hilfe der Cluster-Analyse könnten verschiedene Gruppen bestimmt werden, für die dann jeweils Grundschutzempfehlungen erstellt werden. Für Unternehmen, die diesen Grundschutzansatz nutzen wollen, besteht die Aufgabe dann lediglich in der Zuordnung zur entsprechenden Gruppe.

Quantitative Ansätze sind in der Vergangenheit an einer manglenden Datenbasis und zu großer Komplexität bei der Identifikation der Risiken gescheitert. Deshalb muss es in Zukunft ein vorrangiges Ziel sein, eine geeignete Datenbasis zu schaffen. Dazu werden inbesondere empirische Daten zu Schadensereignissen (Art, Häufigkeit), Schadenshöhen und deren Determinanten benötigt. Hierzu bedarf es eines entsprechenden Anreizsystems (vgl. [GOG04]) und einer Architektur, die den teilnehmenden Unternehmen garantiert, dass die gemeldeten Daten nur aggregiert bzw. anonymisiert weitergegeben werden.

Bislang orientierte sich die Identifikation von Schadensereignissen meist an einem baumartigen Vorgehen. Dieses erweist sich jedoch als sehr komplex und produziert unter Umständen auf Ebenen mit hohem Detaillierungsgrad zahlreiche Überschneidungen und Redundanzen. Wir schlagen daher eine Orientierung an den Prozessen vor. Besonders in großen Unternehmen liegen prozessorientierte Modelle der Abläufe und der IT-Infrastruktur vor. Modelliert man nun Sicherheitsmaßnahmen in ähnlicher Art und Weise, lassen sich direkte Bezüge als Basis für eine Risikoanalyse herstellen. Dabei werden neben technischen auch organisatorische Aspekte integriert, was zu einer ganzheitlichen Sicht beiträgt. Der Wert solcher Prozesse kann dabei auch eine sinnvolle Größenordnung für den jeweils maximal möglichen Schaden darstellen.

5 Fazit und weitere Schritte

Die bestehenden Modelle bieten bereits eine Reihe sinnvoller Techniken zur Kosten-Nutzen-Abwägung von Sicherheitsinvestitionen. Verbleibende Unzulänglichkeiten und Verbesserungsmöglichkeiten wurden aufgezeigt. Wie das Schlagwort ROSI eindrucksvoll demonstriert hat, werden für den praktischen Einsatz leicht verständliche Konzepte benötigt. Daher besteht ein wichtiges Ziel nun in der Erstellung von Referenzmodellen und Anwendungsbeispielen für das Vorgehen, welches alle drei Detaillierungsebenen integriert. Als Ausgangsbasis für die Anwendung eines jeden Modells ist der Aufbau einer aussagekräftigen Datenbasis verbunden mit einer geeigneten Systematisierung von Schadensereignissen, Schutzmaßnahmen, Schäden und deren Determinanten für alle Detaillie-

rungsbereiche der Untersuchung geplant. Ist eine solche Basis einmal geschaffen, kann man sich der Verbesserung der Steuerungsphase, z.B. mit Hilfe von Value at Risk Konzepten (vgl. [Adk04]) oder Sensitivitätsanalysen zuwenden.

Literatur

[Adk04] Roger Adkins. An Insurance Style Model for Determining the Appropriate Investment Level against Maximum Loss arising from an Information Security Breach. *Proceedings of the The Third Annual Workshop on Economics and Information Security, May 13-14, University of Minnesota*, 2004.

[And01] Ross Anderson. Why Information Security is Hard - An Economic Perspective. *Proceedings of 17th Annual Computer Security Applications Conference (ACSAC)*, Seiten 10–14, 2001.

[Ber02] Scott Berinato. Finally, a Real Return on Security Spending. *CIO Magazine*, Feb 2002. http://www.cio.com/archive/021502/security.html (2005-01-14).

[CMR04] Huseyin Cavusoglu, Birendra Mishra und Srinivasan Raghunathan. A Model for Evaluating IT Security Investments. *Communications of the ACM*, 47(7):87–92, Juli 2004.

[FIP74] FIPS-31. Guidelines for Automatic Data Processing Physical Security and Risk Management. Standard, Juni 1974. http://csrc.nist.gov/publications/fips/fips31/fips31.pdf (2005-01-14).

[GK03] Walter Gora und Thomas Krampert. *Handbuch IT-Sicherheit*. Addison-Wesley, München, 2003.

[GL02] Lawrence A. Gordon und Martin P. Loeb. The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5(4):438–457, November 2002.

[GOG04] Esther Gal-Or und Anindya Ghose. The Economic Incentives for Sharing Security Information. *Working Paper*, März 2004. http://www.pitt.edu/∼esther/papers/Infosec.pdf (2005-01-14).

[HP03] Gabriela Hoppe und Andreas Prieß. *Sicherheit von Informationssystemen*. NWB-Studienbücher, Herne/Berlin, 2003.

[JR02] Melanie Jörg und Peter Roßbach. Messung und Bewertung operationeller Risiken. In Peter Roßbach/Hermann Locarek-Junge (Hg.), Hrsg., *IT-Sicherheitsmanagement in Banken*, Seiten 71–93. Bankakademie-Verlag GmbH, 2002.

[Mat03] Kanta Matsuura. Information Security and Economics in Computer Networks: An Interdisciplinary Survey and a Proposal of Integrated Optimization of Investment. (48), August 2003.

[Mer03] Rebecca Mercuri. Analyzing security costs. *Communications of the ACM*, 46(6):15–18, 2003.

[RD04] Thomas Rauschen und Georg Disterer. Identifikation und Analyse von Risiken im IT-Bereich. *Praxis der Wirtschaftsinformatik*, Seiten 19–32, April 2004.

[Saa94] Thomas L. Saaty. How to Make a Decision: The Analytical Hierarchy Process. *Interfaces*, Seiten 19–43, 1994.

[SH00] Kevin J. Soo Hoo. How Much is Enough? A Risk-Management Approach to Computer Security. 2000.

[Ste02] Dirk Stelzer. Risikoanalysen als Hilfsmittel zur Entwicklung von Sicherheitskonzepten in der Informationsverarbeitung. In *IT-Sicherheitsmanagement in Banken*, Seiten 37 – 54. Peter Roßbach / Hermann Locarek-Junge (Hg.), Frankfurt am Main, 2002.

[VV02] Reinhard Voßbein und Jörn Voßbein. Lagebericht zur Informationssicherheit. *kes online*, 2002. http://www.kes.info/archiv/online/02-03-14-studie1.htm (2005-01-14).

[W$^+$01] Huaqiang Wei et al. Cost-Benefit Analysis for Network Intrusion Detection Systems. CSI 28th Anual Computer Security Conference, Oktober 2001. http://wwwcsif.cs.ucdavis.edu/∼balepin/new_pubs/costbenefit.pdf (2005-01-14).