Dirk Fox

Betriebswirtschaftliche Bewertung von Security Investments in der Praxis

Betriebswirtschaftliche Aspekte spielen bei Investitionsentscheidungen über IT-Sicherheitsmaßnahmen häufig keine systematische Rolle. Tatsächlich können sie jedoch nicht nur helfen, die „Sprachbarriere" zwischen Unternehmensleitung und IT Security zu überwinden, sondern auch die Wirtschaftlichkeit einer Maßnahme zu bewerten.

Einleitung

Unternehmerisches Handeln ist zu einem erheblichen Teil Risikomanagement: Jede unternehmerische Entscheidung soll Chancen ergreifen und zielt zugleich auf die Minimierung ganz unterschiedlicher Arten von Risiken. Dabei stehen vor allem Marktrisiken im Fokus; aber auch finanzielle Risiken (Kreditrisiko, Liquiditätsrisiko, Zahlungsausfälle) und rechtliche Risiken (Patente, gesetzliche Anforderungen, Prozessrisiken) spielen im Kontext der Globalisierung und steigender Erwartungen der Marktteilnehmer an den unternehmerischen Erfolg eine immer wichtigere Rolle.

Das gilt insbesondere, wenn Unternehmen betriebswirtschaftlich bewertet werden, z. B. im Vorfeld eines Unternehmensverkaufs oder Börsengangs. Dabei kommt der Bewertung der bestehenden Risiken und der Einschätzung der diesbezüglichen Stärke des Unternehmens ein erhebliches Gewicht zu. Seit einigen Jahren spielen dabei neben externen Risiken auch so genannte operationelle Risiken eine wachsende Rolle. Darunter werden alle betriebswirtschaftlichen Risiken innerhalb eines Unternehmens verstanden. In der Eigenkapitalvereinbarung Basel II, nach der seit Inkrafttreten von Kreditinstituten erstmals auch operationelle Risiken bei der Eigenkapitalhinterlegung zu berücksichtigen sind, werden diese definiert als „die Gefahr von Verlusten, die in Folge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder in Folge von externen Ereignissen eintreten." In diese Kategorie fallen insbesondere alle Ausfälle und Fehler der Informationstechnik – unabhängig davon, ob diese durch technisches Versagen, durch gezielte oder ungezielte, externe oder interne Manipulation verursacht werden.

Alle Arten von Bedrohungen der Informationssicherheit zählen zu den operationellen Unternehmensrisiken. Daher wird – auch vor dem Hintergrund zunehmender Compliance-Anforderungen – die Informationssicherheit inzwischen in vielen Unternehmen als aktives Risikomanagement verstanden – zum Einen, weil in einer globalisierten Wirtschaft ein unkontrollierter Abfluss von Informationen irreparable wirtschaftliche Schäden verursachen kann, zum Anderen, weil immer mehr Geschäftsprozesse von dem störungsfreien Funktionieren der Informationstechnik abhängen.

Dirk Fox

Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.
E-Mail: dirk.fox@secorvo.de

1 Betriebswirtschaftliche Bewertungen

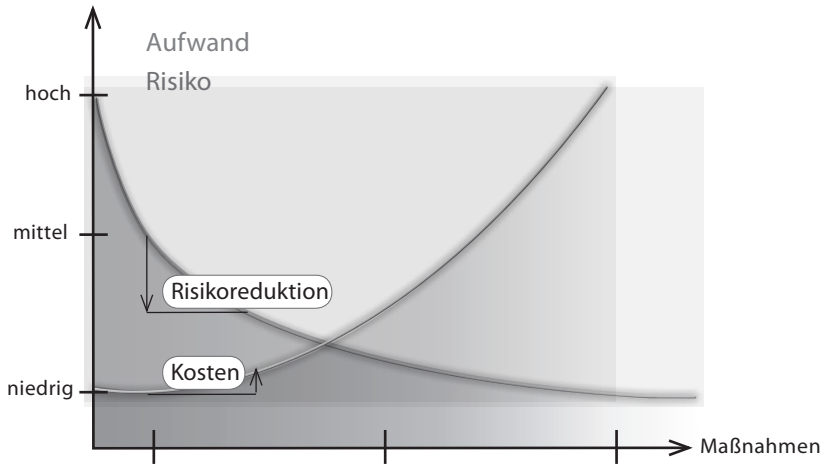
Damit hat auch die betriebswirtschaftliche Bewertung von Maßnahmen der Informationssicherheit an Bedeutung gewonnen. Der Schlüssel zu einer angemessenen betriebswirtschaftlichen Betrachtung der Informationssicherheit ist dabei einerseits die vollständige Erfassung und eine adäquate Quantifizierung der bestehenden Risiken sowie andererseits der Kosten und Wirksamkeit von Schutzmaßnahmen. Unternehmerisch lässt sich nur auf der Grundlage möglichst konkreter, quantitativ unterlegter Bedrohungsszenarien und Lösungsalternativen entscheiden, wie mit bestimmten Risiken zu verfahren ist: ignorieren, verringern, versichern oder verhindern.

Eine solche Quantifizierung liefert zugleich eine einfache Bewertung des erreichten Sicherheitsniveaus: Dieses ist angemessen, wenn alle nicht-akzeptablen Risiken durch geeignete Sicherheitsmaßnahmen ausgeschlossen und alle verbleibenden durch passende Maßnahmen in ihren Auswirkungen begrenzt werden. Leider scheitert dieser Ansatz an zwei praktischen Schwierigkeiten:

- So ist erstens in den meisten Fällen eine hinreichend präzise Quantifizierung der Risiken nicht möglich, und
- es gelingt zweitens nur mit wenigen Sicherheitsmaßnahmen, ein bestimmtes Risiko mit vertretbarem Aufwand gezielt und vollständig auszuschließen.

Die folgenden Abschnitte zeigen, dass die Betrachtung der Informationssicherheit aus betriebswirtschaftlicher Perspektive trotz verschiedener praktischer Schwierigkeiten dennoch einige wertvolle Ansätze bereithält. Unvermeidlich ist die Beschäftigung mit dieser Perspektive ohne-

Abbildung 1 | Verhältnis von Risikoreduktion und Kosten



hin, da mit der steigenden Bedeutung der Informationstechnik die Informationssicherheit zu einem immer wichtigeren Element des Risikomanagements wird.

Aus betriebswirtschaftlicher Perspektive muss jeder Schutzmaßnahme eine angemessene und nachhaltige Risikoreduktion gegenüber stehen – der für die Umsetzung der Maßnahme erforderliche Aufwand muss sich „lohnen". Für diese betriebswirtschaftliche Abwägung und Maßnahmenbewertung wurden Berechnungsmodelle zur Bestimmung eines quantitativen *Return on Security Investment* (ROSI) entwickelt.

Risiken und Sicherheitsmaßnahmen lassen sich betriebswirtschaftlich als Kosten ausdrücken: Risiken werden im Falle ihres Eintretens zu einem quantifizierbaren Schaden; Sicherheitsmaßnahmen hingegen verursachen unmittelbare direkte Kosten.

Betriebswirtschaftliches Ziel einer Sicherheitsmaßnahme ist, eine gewünschte Risikoreduktion mit moderaten Kosten zu erreichen. Denn übersteigen die Kosten einer Schutzmaßnahme das tatsächliche Risiko, ist es wirtschaftlicher, auf die Schutzmaßnahme zu verzichten und das Risiko billigend in Kauf zu nehmen.

Abbildung 1 zeigt in einer vereinfachten Schemagrafik das idealtypische Verhältnis von Risiken, Kosten (Aufwand) und Sicherheitsmaßnahmen. Dabei wurde angenommen, dass die Maßnahmen nach „Wirkungsgrad" ergriffen wurden: Maßnahmen mit hoher Risikoreduktion, aber geringen Kosten wurden zuerst ergriffen, Maßnahmen mit hohen Kosten und geringer Risikoreduktion später – daher der stetige Verlauf der Kurven. Tatsächlich werden die Maßnahmen in der Praxis nicht in solcherart idealisierter Reihenfolge (die wirksamsten Maßnahmen zuerst) umgesetzt – einerseits aufgrund von Abhängigkeiten der Maßnahmen untereinander, andererseits wegen der Abhängigkeit von externen Faktoren. Ein „realer" Kurvenverlauf wird in der Praxis daher nicht so stetig ausfallen.

In den folgenden Abschnitten werden Modelle zur Quantifizierung der Kosten von Risiken und Maßnahmen vorgestellt.

1.1 Kosten von Risiken

Die Festlegung eines akzeptablen Risikolevels ist eine unternehmerische Frage, die im Zweifel nur von der Geschäftsleitung beantwortet werden kann. Eine vernünftige Einschätzung ist allerdings nur dann möglich, wenn es gelingt, das Risiko in einer finanziellen Größenordnung auszudrücken. Im Risikomanagement wird dafür meist der zu erwartende jährliche Verlusts (*Annual Loss Expectancy*, ALE) bestimmt. Der ALE errechnet sich aus der finanziellen Höhe (*Loss*, L) und der Eintrittswahrscheinlichkeit (*Probability*, P) eines möglichen Schadens:

$$ALE = L \bullet P$$

Der erwartete Gesamtverlust ergibt sich als Summe der Erwartungswerte aller betrachteten Einzelrisiken:

$$ALE_{tot} = \sum L_i \bullet P_i \text{ für } i=1..n$$

Die Anwendung der Berechnung des ALE für Bedrohungen der Informationstechnik geht auf die (inzwischen zurückgezogene) Richtlinie FIPS PUB 65 des NIST aus dem Jahr 1979 zurück [7]. Sie bildet die Grundlage für zahlreiche Ansätze von Kosten-Nutzen-Modellen der Informationssicherheit, insbesondere auch des ROSI-Ansatzes (siehe unten).

Die Reduktion eines spezifischen Risikos kann danach auf zweierlei Weise erfolgen:

- Entweder wird durch geeignete Gegenmaßnahmen die Eintrittswahrscheinlichkeit des Schadens verringert, z. B. durch einen Virenscanner auf einem E-Mail-Server oder den Betrieb einer Firewall;
- oder es werden Maßnahmen getroffen, die die Auswirkungen des Schadens begrenzen, z. B. die konsequente Umsetzung des „*need-to-know*"-Prinzips bei der Berechtigungsvergabe oder durch ausgearbeitete und trainierte Notfallpläne, betriebsbereite Ersatzsysteme und ausgefeilte Wiederanlaufprozesse.

Damit ist das Problem der Quantifizierung eines Risikos jedoch noch nicht gelöst, denn

- für die Eintrittswahrscheinlichkeit eines Schadens in der Informationstechnik existieren – anders als für viele andere, versicherbare Schäden – keine belastbaren Erfahrungswerte;
- durch die Schnelllebigkeit und die kurzen Innovationszyklen der Informationstechnik ändern sich sowohl die tatsächlichen Risiken als auch die möglichen Auswirkungen und deren Eintrittswahrscheinlichkeiten in sehr kurzen Zeiträumen;
- der errechnete erwartete Verlust ist eine rein statistische Größe (Erwartungswert) – er kann im Einzelfall erheblich über- oder unterschritten werden.

Da sich mit diesem Berechnungsansatz nur ein einzelnes Risiko betrachten lässt, geht das ALE-Modell außerdem implizit von der Annahme aus, dass einzelne Bedrohungen und Gegenmaßnahmen isoliert betrachtet werden können. Das ist in der Praxis jedoch in den meisten Fällen eine grobe Vereinfachung. So gibt es Gegenmaßnahmen, die Schutz vor mehreren Bedrohungen bieten, wie z. B. eine Firewall (externer *Denial-of-Service*-Angriff auf Client-Systeme, Missbrauch des E-Mail-Servers, unberechtigter externer Zugriff auf vertrauliche Daten), und es gibt Maßnahmen, die neue Risiken verursachen, wie z. B. die Auslagerung von Backups.

Schließlich berücksichtigt das ALE-Modell keine kumulativen Effekte: die Einzelrisiken werden einfach addiert. In der Praxis aber wird sich die Zahl der ver-

lorenen Kunden aufgrund eines einstündigen Ausfalls des Online-Bankings bei einem Kreditinstitut in Grenzen halten; kommt es hingegen in kurzer Zeit wiederholt zu solchen Ausfällen, kann dies einen erheblichen Image-Schaden mit schmerzlichem Kundenverlust zur Folge haben – und einen Schaden verursachen, der die Summe der erwarteten Einzelschäden erheblich übersteigt.

Und nicht zuletzt kann in dem Modell nicht zwischen großen Schäden mit geringer Eintrittswahrscheinlichkeit und geringen Schäden mit hoher Eintrittswahrscheinlichkeit unterschieden werden – obwohl sich letztere meist sehr gut kontrollieren lassen, erstere aber existenzbedrohend sein können und ihr Eintritt daher durch geeignete Maßnahmen in jedem Fall verhindert werden muss.

Daher wurde das ursprüngliche ROSI-Modell mehrfach verfeinert, um verwertbarere Aussagen zu erhalten.

1.2 Kosten von Sicherheitsvorfällen

Die Kosten eines Sicherheitsvorfalls sind meist – insbesondere, wenn es tatsächlich zum Eintritt eines Schadens gekommen ist – deutlich einfacher zu quantifizieren. Leider bestimmen und dokumentieren nur die wenigsten Unternehmen die tatsächlichen Kosten eines Schadensfalls hinreichend genau, und das oft nicht einmal wegen des damit verbundenen Aufwands. Dabei ergäben sich aus diesen Erfahrungswerten sowohl eine hilfreiche Datenbasis für die finanzielle Abschätzung bestimmter Schäden als auch die Chance, geeignete Maßnahmen zu ergreifen, mit denen sich bei ähnlichen Vorfällen zukünftig das Schadensausmaß gezielt verringern ließe.

Die Kosten eines Sicherheitsvorfalls setzen sich aus den folgenden Einzelkosten zusammen:

- **Umsatzeinbußen** und **Wertverlust**: unmittelbar durch Ausfallzeiten (diese Kosten sind in der Regel größer als die Gemeinkosten, d. h. die Betriebskosten während der Ausfallzeit) und mittelbar durch den Verlust von Kunden oder Aufträgen, beispielsweise aufgrund eines nachfolgenden Image-Schadens, sowie die Wertminderung durch „Alterung“ eines Produkts.[1] Wertverlust und Umsatzrückgang (oder -ausfall) lassen sich in Abhängigkeit von der Dauer der Wirkung ausdrücken:

$$L_i(t)$$

- **Wiederherstellungskosten**: Ersetzung oder Wiederanlauf der betroffenen Systeme, Wiedereinspielen von Images, Betriebssystemen oder Daten von Backups, ggf. Rettung teildefekter Datenträger. Die Wiederherstellungskosten setzen sich aus externen (exakt quantifizierbaren) Kosten (*Recovery*, R_e) für Unterstützungsleistungen beim Wiederanlauf und internem Aufwand (überwiegend investierte Arbeitszeit, also Personalkosten) $R_i(t)$ zusammen.
- **Schadensersatzleistungen**: Vertragsstrafen bei Lieferverzögerungen infolge eines Defekts oder Systemausfalls, Kosten für Rückrufe und Ersatzlieferungen, Haftung für verursachte Schäden Dritter (bspw. durch ungewollte Verbreitung von Schadsoftware). Dies sind leicht quantifizierbare Einmalkosten (*Fine*, F), deren Höhe unabhängig ist von der Dauer des Vorfalls.

Daraus ergibt sich eine einfache Formel für den Gesamtverlust (L) in Abhängigkeit von der Dauer eines Vorfalls (respektive seiner Auswirkungen):

$$L_{tot}(t) = L_i(t) + R_e + R_i(t) + F$$

Weitere, manchmal „immateriell“ genannte Schäden sind betriebswirtschaftlich nicht relevant. Denn sofern sie Kosten verursachen, fließen sie „automatisch“ in eine der drei oben genannten Schadenskategorien ein. So ist z. B. ein Imageschaden, der keine Umsatzeinbußen zur Folge hat, kein betriebswirtschaftlich zu berücksichtigender Schaden – sondern eine (wenn auch ungeplante) Marketingmaßnahme. Führt er hingegen zu Umsatzausfällen, ist er in $L_i(t)$ bereits berücksichtigt. Anders ausgedrückt: Jeder relevante Schaden ist ein materieller Schaden – und lässt sich daher einer der drei Schadenskategorien zuordnen.

1.3 Kosten von Sicherheitsmaßnahmen

Auch die Kosten einer Schutzmaßnahme setzen sich aus unterschiedlichen Elementen zusammen. Dabei sollte eine Gesamtkostenbetrachtung angestellt werden (*Total Cost of Ownership*, TCO), die nicht nur die Anschaffungskosten, sondern auch alle weiteren direkten und indirekten (Folge-) Kosten einer Sicherheitsinvestition berücksichtigt:

- **Konzeptionskosten** C_c: Architektur, Lösungsauswahl, Testbetrieb, ggf. Anpassungen an der eigenen Infrastruktur (Konfiguration, Dokumentation) oder der gewählten Lösung
- **Investitionskosten** C_i: Hardware, Software, Installation und Konfiguration, Dokumentation, Inbetriebnahme und Mitarbeiterschulungen (Administratoren, Benutzer)
- **Betriebskosten** C_m: Support, Updates, jährliche Lizenzkosten, Betriebsprozesse (Betreuung, Hotline)

Aus diesen drei Kostenblöcken werden die Gesamtkosten der Sicherheitsinvestition SI (TCO_{SI}) berechnet. Dabei werden die Einmalkosten (Konzeption, Investition) über den Betriebszeitraum y (in Jahren) abgeschrieben, während die Betriebskosten jährlich anfallen:

$$TCO_{SI} = (C_c+C_i)/y+C_m$$

Sonnenreich und seine Mitautoren weisen in [8] zu Recht darauf hin, dass in der Regel mit der Einführung einer Sicherheitsmaßnahme auch Produktivitätsverluste bei den Anwendern einhergehen. So kann sich das Starten des Rechners verlangsamen, die Eingabe eines zusätzlichen Passworts oder längere Reaktionszeiten beim Zugriff auf verschlüsselte Daten Bearbeitungsprozesse verlängern und regelmäßige Backups wertvolle Arbeitszeit binden. Eine faire Berechnung sollte daher auch Produktivitätsverluste als Teil der „Betriebskosten“ einer Sicherheitsmaßnahme in der Kalkulation berücksichtigen.

2 Das ROSI-Modell

Nach dem Platzen der „Dotcom-Blase“ im Jahr 2000 sahen sich IT-Verantwortliche angesichts der (steigenden) Kosten der Informationstechnik zunehmend dem kritischen Blick der Controller ausgesetzt. Die Grundforderung: Übersteigen die Kosten einer Schutzmaßnahme die Kosten eines tatsächlichen Risikos, ist eine solche Maßnahme unwirtschaftlich und damit unsinnig.

2.1 ROI

Wie aber lässt sich die Wirtschaftlichkeit einer Maßnahme bestimmen? Wie bei anderen Investitionen auch wurde in vielen Unternehmen die Berechnung eines *Re-*

1 Jedes Produkt lässt sich nur über einen begrenzten Zeitraum zu einem angemessenen Preis verkaufen, bis entweder die Nachfrage gedeckt oder eine Überarbeitung oder Aktualisierung erforderlich ist. Diese „Alterung“ findet auch statt, wenn weder Verkauf noch Produktion möglich sind.

turn on Investment (ROI) als Bewertungsverfahren für die Wirtschaftlichkeit einer IT-Investition eingefordert. Die Kennzahl ROI geht auf Donaldson Brown zurück, der sie im Jahr 1913 einführte. Sie sollte die Bewertung der Wirtschaftlichkeit (Rendite) einer unternehmerischen Investition ermöglichen und ist definiert als das Produkt aus Umsatzrendite (= Gewinn/Nettoumsatz • 100) in Prozent und dem Kapitalumschlag (= Nettoumsatz/Gesamtkapital). Daraus ergibt sich die folgende einfache Berechnungsformel:

ROI = Gewinn/Gesamtkapital • 100 [%]

Der ROI gibt also das prozentuale Verhältnis des Gewinns zum Kapitaleinsatz an. Diese Kennzahl kann sowohl zur Bestimmung der Wirtschaftlichkeit einer Gesamtinvestition (Unternehmen) als auch zur Bewertung des betriebswirtschaftlichen Erfolgs einer Periode (Monat, Quartal, Jahr) verwendet werden.

Ein erweitertes Verständnis des ROI erlaubt außerdem Wirtschaftlichkeitsbetrachtungen von Einzelinvestitionen, sofern der einer bestimmten Investition anteilig zuzurechnende Gewinn separiert werden kann:

ROI = Gewinnanteil/Kapitaleinsatz • 100

Dabei wird der Gewinnanteil über die Nutzungsdauer der getätigten Investition berechnet.

2.2 ROSI

Auf dieser Formel basiert der Ansatz zur Berechnung eines *Return on Security Investment* (ROSI), der auf Arbeiten von Kevin J. Soo Hoo an der Stanford University [3] und (unabhängig von Hoo) Huaqiang Wei an der University of Idaho zurück geht [9]. Darin stellen die Autoren eine Risk-Management basierte Kosten-Nutzen-Berechnung für Sicherheitsinvestitionen vor. Wei gibt ein Rechenbeispiel für ein *Intrusion Detection System*, Hoo berechnet die Einsparungen für ein ganzes Bündel von Sicherheitsmaßnahmen. Bekannt wurde das ROSI-Konzept im Jahr 2002 insbesondere durch eine Veröffentlichung von Scott Berinato im CIO Magazin [1].

Der Kern des ROSI-Berechnungsmodells ist einfach: Jede wirksame Sicherheitsinvestition (SI) reduziert entweder die Eintrittswahrscheinlichkeit (P) oder die Höhe eines bestimmten Schadens (L). Damit sinkt der erwartete Schaden, die *Annual Loss Expectancy* (ALE). Der „Gewinn" einer Sicherheitsmaßnahme ergibt sich damit aus der Verringerung dieses Erwartungswertes minus den Gesamtkosten der Maßnahme (TCO_{SI}), und die Kennzahl $ROSI_{SI}$ als Quotient aus Gewinn und Kosten:

$$ALE_{neu} = L_{neu} \bullet P_{neu}$$
$$\text{"Gewinn"} = ALE_{alt} - ALE_{neu} - TCO_{SI}$$
$$ROSI_{SI} = (ALE_{alt} - ALE_{neu} - TCO_{SI})/TCO_{SI}$$

2.3 Grenzen

Eine grundsätzliche Schwierigkeit ist zunächst einmal, dass der „Gewinn" einer Sicherheitsinvestition selten in eine messbare Verminderung von Ausgaben oder eine Erhöhung von Einnahmen mündet. Der Gewinn besteht in einer Verminderung eines operationellen Risikos, also eines Erwartungswertes für die Kosten von Sicherheitsvorfällen – ob dadurch tatsächlich Einsparungen erzielt worden sind, lässt sich selbst ex post nicht zuverlässig feststellen. Denn auch wenn – beispielsweise bei häufigen Schadensereignissen – ein Rückgang beobachtet werden kann, ist der ursächliche Zusammenhang mit der Schutzmaßnahme in der Regel nicht beweisbar, und die Zahl der Schadensereignisse, die ohne die Maßnahme eingetreten wären, nicht feststellbar..

- *Beispiel 1*: Sie investieren in ein modernes, mehrstufiges Firewall-System. Wenn anschließend die Zahl der Angriffsversuche sinkt, kann das auch daran liegen, dass andere Angriffsziele viel versprechender waren, oder schlicht die Zahl der breit gestreuten Angriffe insgesamt abgenommen hat.
- *Beispiel 2*: Sie führen eine Security Awareness Kampagne durch, die insbesondere für einen sicherheitssensiblen Umgang mit mobilen Geräten wirbt. Wenn anschließend die Zahl der entwendeten Laptops zurückgeht, kann das auf die Kampagne zurückzuführen sein – oder aber darauf, dass Ihre Laptop-Modelle inzwischen einen geringeren Diebstahlanreiz bieten.

Aber auch die berechneten Erwartungswerte besitzen eine systematische Schwäche: Sie beruhen – anders als bei der Berechnung von zahlreichen anderen, versicherbaren Risiken – auf keinen verlässlichen und ausreichend vergleichbaren Daten aus der Vergangenheit. Damit sind sie zumeist sehr grobe „Bauchschätzungen". Je geringer die Schadenswahrscheinlichkeit, desto weniger Erfahrungswerte gibt es und dementsprechend größer ist die Ungenauigkeit der Schätzung.

Zudem besitzen die Schätzungen der Höhe der Kosten eines Vorfalls eine sehr große „Unschärfe" (Varianz). So hängen beispielsweise die Kosten eines Recovery von Client-Systemen u. a. davon ab, ob mit virtuellen Maschinen, vereinheitlichten Images oder sehr heterogenen, individuell konfigurierten oder dezentral betreuten Systemen gearbeitet wird. Auch gibt es insbesondere bei der Erfassung tatsächlicher Angriffe eine hohe Dunkelziffer: Die Zahl erfolgreicher Angriffe, entdeckter erfolgreicher Angriffe und berichteter erfolgreicher Angriffe differieren erheblich (siehe z. B. [3]).

Schließlich liegt dem Modell eine vereinfachende Annahme zu Grunde, durch die die durchgeführten Kalkulationen im Einzelfall Makulatur werden können. So werden im ROSI-Modell Einzelrisiken und darauf bezogene Schutzmaßnahmen jeweils isoliert betrachtet – dabei wirken Schutzmaßnahmen in der Praxis häufig auf zahlreiche Einzelrisiken, umgekehrt treten in einem Schadensfall erfahrungsgemäß meist Folgen aus kumulierten Risiken ein.

Nicht zuletzt sorgt die hohe Entwicklungsgeschwindigkeit in der Informationstechnik dafür, dass für die Amortisation einer Sicherheitsinvestition in der Regel nur kurze Zeit bleibt, da die ständige Veränderung der IT-Infrastrukturen die Wirksamkeit einer Schutzmaßnahme erheblich beeinträchtigen können. Werden beispielsweise mobile Geräte (Laptops, PDAs) mit direktem Internet-Zugang eingeführt, benötigen sie Personal Firewalls, um das durch die Firewallinfrastruktur erreichte Sicherheitsniveau nicht zu gefährden – eine zusätzliche Investition, die die ROSI-Erfolgsrechnung der Firewall verschlechtern kann.

Auf einen wichtigen, allerdings ebenfalls schwer kalkulierbaren, in den Modellen von Hoo und Wei unberücksichtigten Kostenfaktor bei Sicherheitsinvestitionen weisen Sonnenreich et. al. [8] hin: den Produktivitätsverlust, der mit einigen Schutzmaßnahmen einhergeht. In Einzelfällen kann eine Sicherheitsmaßnahme zudem durch Seiteneffekte produktivitätsfördernd wirken, so beispielsweise, wenn eine systematische Vergabe von Benutzerrechten und die Etablierung von Prozessen den Aufwand für die Administration (bspw. durch Gruppenbildung) verringert

oder *Single Sign On* (SSO) die Authentisierungsprozesse beschleunigt.

3 Weitere quantitative Modelle

In den vergangenen Jahren wurden zahlreiche Erweiterungen oder Anpassungen des ROSI-Modells vorgestellt, die einige der Nachteile des ursprünglichen Modells abschwächen. Zwei dieser Modelle sind besonders viel versprechend und werden im Folgenden vorgestellt: ein Ansatz, der eine statistische Verteilung von Eintrittswahrscheinlichkeit und Schadenshöhe berücksichtigt, und ein zweiter, der die betriebswirtschaftliche Sicht eines Angreifers modelliert.

3.1 Der Lockstep-Ansatz

Dem Problem der „Unschärfe" widmet sich ein Ansatz der Australischen Bundesbehörden, der von Lockstep Consulting entwickelt wurde [2]. Er basiert auf dem Australischen Risiko-Management-Standard AS 4360, der eine Klassifikation von Eintrittswahrscheinlichkeiten für IT-Sicherheitsvorfälle sowie die Schadenshöhe bietet (Threat & Risk Assessment, TRA). Anstatt nun feste Werte für die Eintrittswahrscheinlichkeit und die Kosten eines Schadensereignisses zu verwenden, wird für jede Klasse ein Bereich definiert (minimale/maximale Häufigkeit/Kosten). Mit einem Zufallsgenerator werden dann über mehrere Iterationen unterschiedliche Werte nach einer vorgegebenen statistischen Verteilung gewählt und die Erwartungswerte für den jährlichen Verlust mit und ohne Schutzmaßnahmen berechnet.

Ergebnis dieser Kalkulation sind Histogramm-Darstellungen, die die Häufigkeitsverteilung der erwarteten Schadenshöhen und der Einsparungen durch Schutzmaßnahmen angeben. Die Genauigkeit des Ergebnisses steigt dabei mit der Zahl der berechneten Iterationen. Über die Summierung der Häufigkeiten lässt sich aus den Histogrammen beispielsweise ablesen, wie hoch die Schadenssumme in 90% der Fälle maximal ist, und dass man mit einer 50%igen Wahrscheinlichkeit eine bestimmte Mindesteinsparung durch Schutzmaßnahmen erzielt.

Auch dieses Modell beruht auf einer vereinfachenden Annahme: Für die Eintrittswahrscheinlichkeit wurde eine uniforme Verteilung angenommen, für die Kosten eine Dreiecksverteilung zwischen Minimum, Maximum und wahrscheinlichstem Wert. Diese Einschränkung, die den als Excel-Erweiterung genutzten Freeware-Tools geschuldet ist, kann durch entsprechende Anpassungen jedoch leicht aufgehoben werden.

Das Modell schwächt einen erheblichen Nachteil des ursprünglichen ROSI-Modells ab. Allerdings sind auch hier bestimmte Annahmen wie die Definition des Wertebereichs und der statistischen Verteilung der Ausgangswerte (Eintrittswahrscheinlichkeit und Schadenshöhe) entscheidend für die Qualität des Resultats – und für diese Zahlen gibt es auch keine belastbaren Erfahrungswerte.

3.2 Das Mizzi-Modell

Von Adrian Mizzi [4] stammt ein Berechnungsmodell, das die ROSI-Kalkulation um eine interessante Perspektive ergänzt: Die betriebswirtschaftliche Rechnung des Unternehmens wird in Relation gesetzt zu betriebswirtschaftlichen Betrachtungen aus der Perspektive eines potentiellen Angreifers. Denn auch dem Angreifer entstehen Kosten – nämlich der Aufwand zur Konzeption des Angriffs (Identifikation einer Schwachstelle, C_a; abhängig von der Kompetenz des Angreifers können die dafür erforderlichen Kosten erheblich differieren) und für deren Umsetzung (also der konkreten Ausnutzung einer gefundenen Schwachstelle, C_b), für die er Zeit und Investitionen in Hardware und Software tätigen muss.

Diesen Kosten muss aus Sicht des Angreifers ein Wert gegenüber stehen, der die Kosten deutlich übersteigt und ihn zur Durchführung des Angriffs motiviert. Betriebswirtschaftlich gesehen kann dies entweder der Wert einer durch den Angriff gewonnenen Information (I) sein, oder aber die Höhe des Schadens, den er dem angegriffenen Unternehmen zufügen kann (L_{tot}). Bei einem betriebswirtschaftlich rechnenden Angreifer ist ein Angriff dann zu erwarten, wenn gilt:

$$I+L_{tot} >> C_a+C_b$$

Eine große Stärke dieses Ansatzes ist die Unabhängigkeit von wenig verlässlichen Wahrscheinlichkeitsannahmen, die die Aussagekraft der Ergebnisse beim ROSI-Modell erheblich einschränken. Auch ermöglicht der Ansatz, aktuelle Entwicklungen zu berücksichtigen, wie z. B. die Veröffentlichung einer kritischen Schwachstelle einer Standard-Anwendung und die Verbreitung von darauf adaptierter Exploit-Software.

Gewichtig sind aber auch die Nachteile des Modells: Die Risikoberechnung basiert auf erheblich vereinfachenden Annahmen über die Angreifermotivation. Denn viele Hacker denken keineswegs betriebswirtschaftlich – zwar versuchen sie möglicherweise, eine (vor allem in der Szene) beeindruckende Wirkung mit einem Hack zu erzielen; viele zielen aber keineswegs auf Schadensmaximierung oder Informationsgewinnung. Dennoch ist der Ansatz wertvoll, denn er dient dazu, die Kosten-/Nutzen-Situation des Angreifers zu prüfen. Daraus kann folgen, dass einem theoretisch denkbaren Angriffsszenario nur eine geringe praktische Bedeutung zuzumessen ist.

Fazit

Bei der Entscheidung über die Einführung von Schutzmaßnahmen spielen betriebswirtschaftliche Fragen oft eine erschreckend unbedeutende Rolle. Häufig werden auch die tatsächlichen Kosten nicht korrekt bestimmt; manchmal ist dies allerdings auch budgetpolitischen Rahmenbedingungen geschuldet.

Auch zur Bewertung der praktischen Bedeutung von Angriffsszenarien werden betriebswirtschaftliche Bewertungen erstaunlich selten herangezogen, mit z. T. skurrilen Ergebnissen in Bedrohungsanalysen.

Allerdings hat die Berücksichtigung wirtschaftlicher Aspekte bei Investitionsentscheidungen in der IT-Sicherheit auch Grenzen. Denn nicht erst seit dem „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich" (KonTraG, 1998) sind Geschäftsführer und Vorstände von Kapitalgesellschaften zur Reduktion unternehmenskritischer Risiken verpflichtet. Einen planvollen Umgang mit operationellen Risken gebietet allein schon die allgemeine Sorgfaltspflicht.[2]

Darüber hinaus gibt es gesetzliche Einzelbestimmungen wie das Bundesdatenschutzgesetz (BDSG), das Telekommunikationsgesetz (TKG) oder das Kreditwesengesetz (KWG), die z. T. sehr konkrete Anforderungen an den Informationsschutz und die IT-Sicherheit stellen.

2 „Sorgfalt des ordentlichen und gewissenhaften Geschäftsleiters", § 93 Aktiengesetz und § 43 GmbH-Gesetz.

Diese gesetzlichen Anforderungen sind damit einer generellen betriebswirtschaftlichen Bewertung als Entscheidungsgrundlage entzogen, da ihre Umsetzung gesetzlich geboten ist.

Neben gesetzlichen Erfordernissen (Compliance) gibt es einen zweiten Bereich, in dem die Investition in Sicherheitsmaßnahmen außer Frage steht: Online-Angebote, seien es eCommerce-Lösungen oder Kunden-Services, sind ohne ein Minimum an geeigneten Sicherheitsmaßnahmen undenkbar – man stelle sich Online-Banking ohne PIN, TAN und andere Sicherheitsmechanismen vor.

Literatur

[1] Berinato, Scott: *Finally, a Real Return on security Spending*. CIO Magazine, 08.04.2002.

[2] Government Chief Information Office: *A Guide for Government Agencies Calculation Return on Security Investment*. New South Wales Government, Department of Commerce; Version 2.0, 13.06.2006. http://www.gcio.nsw.gov.au/publications/Lockstep_ROSI_Guideline_SGW_282_2_29.pdf

[3] Hoo, Kevin J. Soo: *How Much Is Enough? A Risk-Management Approach to Computer Security*. Working Paper, CRISP, Stanford University, June 2000. http://iis-db.stanford.edu/pubs/11900/soohoo.pdf

[4] Mizzi, Adrian: *Return on Information Security Investment – Are you spending enough? Are you spending too much?* Januar 2005.

[5] Möricke, Michael; Teufel, Stephanie (Hrsg.): *Kosten & Nutzen von IT-Sicher¬heit*. Praxis der Wirtschaftsinformatik, HMD Heft 248, April 2006, dpunkt.verlag 2006.

[6] Nowey, Thomas; Federrath, Hannes; Klein, Christian; Plößl, Klaus: *Ansätze zur Evaluierung von Sicherheitsinvestitionen*. In: Sicherheit 2005. Lecture Notes in Informatics, P-62, Köllen-Verlag, Bonn 2005, S. 15-26. http://www-sec.uni-regensburg.de/publ/2005/Si2005NFKP2005Sicherheitsinvestitionen.pdf

[7] National Institute of Standards and Technology (NIST): *Guideline for Automatic Data Processing Risk Analysis*. FIPS PUB 65, 01.08.1979 (zurückgezogen am 25.08.1995).

[8] Sonnenreich, Wes; Albanese, Jason; Stout, Bruce: *Return On Security Investment (ROSI) – A Practical Quantitative Model*. Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006, S. 55-66.

[9] Wei, Huaqiang; Frinke, Deborah et.al.: *Cost-Benefit Analysis for Network Intrusion Detection Systems*. In: Proceedings of the 28th Annaul Computer Security Conference October 2001.