



Den nutzbringenden Mitteleinsatz ermitteln

ROSI: Ein Konzept zur Bewertung von Sicherheitsmaßnahmen

Auch für IT-Sicherheitsmaßnahmen ist der nutzbringende Mitteleinsatz essenziell. ROSI (Return on Security Invest) bewertet hierzu Sicherheitsinvestitionen analog zum klassischen ROI (Return on Investment). Die Bestimmung des Nutzens in Geldeinheiten ist selten sinnvoll möglich. Eine qualitative Bewertung, inwieweit das Risiko reduziert werden konnte, ist meist praktikabler.

Als Alanson Crane 1863 den ersten Feuerlöscher patentierte, hielten die meisten Menschen den Kauf eines solchen für eine zweifelhafte Investition, denn der Nutzwert war völlig unklar. Analog stehen IT-Leiter und Sicherheitsverantwortliche vor der Herausforderung, das Management vom Nutzwert einer Investition in die Informationssicherheit zu überzeugen. Die Geschichte belegt für die Feuerlöscher einen ROI von 300 Prozent – bei Investi-

tionen in die Informationssicherheit ist es jedoch keine Option, auf historisch belegte ROI zu warten. Andererseits ist es in Zeiten knapper Budgets besonders schädlich, Mittel falsch einzusetzen.

Nutzen von Sicherheitsmaßnahmen

Der Nutzwert von Sicherheitsinvestitionen steigt nachhaltig, wenn er analysiert wird. Außerdem ist es wichtig, dem Management den Nutzen der IT-Sicherheit

in einer ihm verständlichen Sprache zu verdeutlichen. Die Kommunikation über Kennzahlen transportiert messbare Erfolge in verdichteter Form und erlaubt einen schnellen Überblick.

Zudem sollten für den kontinuierlichen Betrieb die IT-Sicherheitsleistungen als Services definiert, detailliert beschrieben und die entstehenden Kosten kalkuliert werden. Dadurch ist es möglich, die Kosten verursachungsgerecht den Leistungsempfängern im Unternehmen zuzuordnen. Dies erfolgt über Verrechnungseinheiten, die für die einzelnen IT-Sicherheitsservices zu definieren sind.

Ebenso kann jederzeit der Nutzen der IT-Sicherheit den aktuellen Kosten gegenübergestellt werden, um sie transparenter darzustellen. Darauf aufbauend können über den Einsatz von Benchmarking oder das Zielkostenmanagement Kostenersparnisse bei gleichbleibender Qualität der IT-Sicherheitsservices erreicht werden.

Risiken sind schwer zu messen

Zur Bewertung von Investitionen in die Informationssicherheit wird häufig ROSI (Return on Security Invest) vorgeschlagen und meist als Nutzwert in Geldeinheiten minus die Betriebskosten, im Verhältnis zu den Investitionen, definiert.

Nur wenige Maßnahmen ergeben aber einen unmittelbaren Nutzwert im klassischen Sinn, messbar in Geldeinheiten. Beispiele sind der Virenschutz, bei dem sich die Verringerung der Schadensfälle und des damit verbundenen Aufwands zur Bereinigung der Systeme einfach messen lässt, oder die Filterung von unerwünschten Mails (Spam). Die meisten Maßnahmen zielen aber auf Risiken, die vor der geplanten Investition noch nicht eingetreten sind und die unter Umständen auch danach nicht eintreten werden.

Daher sind Kostenersparnisse nicht unmittelbar messbar, sondern nur über



Foto: Octave Alex / Fotolia

Nicht immer sichtbar: Der Nutzen von Sicherheitsmaßnahmen ist in der IT nicht immer so offensichtlich wie im „richtigen Leben“.

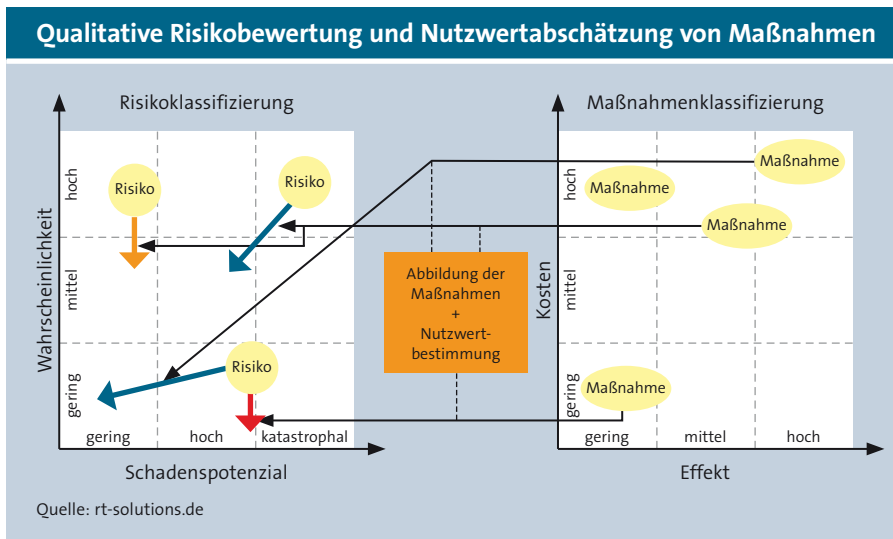


Abbildung konkreter Maßnahmen auf bestehende Risiken: Der Nutzwert jeder Maßnahme wird bestimmt und als Grad der Risikominimierung im Risikoportfolio visualisiert.

die potenzielle Schadenshöhe. Die Maßnahmen reduzieren aber die Eintrittswahrscheinlichkeit oder begrenzen das Schadenspotenzial. Ein Risiko ist eben besonders dann schwerwiegend, wenn das Unternehmen kein Aktionspotenzial – also Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit oder der potenziellen Schadenshöhe – erarbeitet hat.

Relative Risikominderung

Die Anwendung von ROSI setzt voraus, dass die Risiken eines Unternehmens im Rahmen des Risiko-Managements geeignet erfasst und bewertet werden. Für die Bestimmung des Nutzwertes sind dabei auch eine finanzielle Bewertung erwarteter Schäden sowie die Festlegung von Eintrittswahrscheinlichkeiten notwendig. Analog müssen auch die Auswirkungen möglicher Maßnahmen bewertet werden. In der Praxis ist beides nicht immer sinnvoll und mit angemessenem Aufwand durchführbar.

Eine qualitative Bewertung der Eintrittswahrscheinlichkeiten, Schadensausmaße und Risiken ist meist realistischer und weniger aufwendig, aber dennoch hinreichend, um dringenden Handlungsbedarf aufzuzeigen und einen optimierten Einsatz des Sicherheitsbudgets zu unterstützen. Die ROSI-Betrachtung wird hierbei ersetzt durch die relative Risiko-

minderung (Risk Reduction), bezogen auf die entstehenden Kosten.

Diese qualitative Betrachtung ermöglicht es, Maßnahmen angemessen zu bewerten, um mit einem gegebenen Sicherheits-Budget einen möglichst großen Nutzen zu erreichen beziehungsweise für hohe Risiken die günstigsten Maßnahmen auszuwählen.

Bei der Kalkulation des Nutzwertes sind nicht nur die reinen Investitionen, sondern auch die Folgekosten des Betriebs zu beachten. Die Kontrolle und Pflege einer Maßnahme verursachen Kosten, die auf den ersten Blick den Nutzwert schmälern – ohne sie verliert die Risikoreduktion aber schnell an Wirkung. Eine Betrachtung von Kosten und Nutzwert über mehrere Jahre hinweg ist deshalb ratsam.

ROSI im Risikomanagement

Die Anwendung der ROSI-Betrachtungen erfolgt sinnvollerweise eingebettet in einen bestehenden Risikomanagementprozess. Für das IT-Risikomanagement ergibt sich das folgende Vorgehensmodell:

- Ein Risikomanagementprozess wird etabliert und ein Inventar der IT-Risiken erstellt. Die Risiken werden qualitativ auf einer mit dem Management abgestimmten Skala bewertet.

- Risiken (klassifiziert nach Wahrscheinlichkeit und Schadenspotenzial) sowie mögliche Maßnahmen (klassifiziert nach Kosten und Stärke des Effektes) werden qualitativ bewertet und in einem Portfolio angeordnet. Die Maßnahmen werden auf die konkreten Risiken abgebildet und die dadurch erwartete Risikoreduktion qualitativ bewertet.
- Auf Grundlage des Verhältnisses zwischen Risikoreduktion und Kosten werden im Rahmen des gegebenen Budgets oder für spezielle Risiken die effektivsten Maßnahmen ausgewählt.
- Für ausgewählte Maßnahmen wird die qualitative Bewertung durch eine detaillierte ROSI-Betrachtung in Geldeinheiten ergänzt. Dies kann unter Einsatz des Fixpunkt-Konzepts erfolgen. Wenn einzelne Risiken in Geldeinheiten quantifizierbar sind, können die im ersten Schritt nicht quantifizierbaren Risiken durch ordinale Vergleiche mit den bereits quantifizierten Risiken monetär bewertet werden.

Nicht für alle Risiken und Maßnahmen ist die beschriebene Vorgehensweise sinnvoll. Bei Maßnahmen, die für den Geschäftsbetrieb grundlegend sind beziehungsweise der Einhaltung gesetzlicher Vorgaben gelten, stellt sich nur die Frage nach der kostengünstigsten Umsetzung. Auf eine Bewertung des Risikos oder der Risikoreduktion kann verzichtet werden. Für die meisten anderen Maßnahmen ist eine qualitative Bewertung hinreichend.

Werden existenzbedrohende Risiken identifiziert oder Maßnahmen im Zuge der Einführung gesetzlicher Bestimmungen (wie Euro-SOX) notwendig, die sich nicht im Rahmen des bestehenden Budgets durchführen lassen, unterstützt eine Budgetierung auf Basis einer detaillierten ROSI-Betrachtung in Geldeinheiten die Argumentation gegenüber dem Management. > Bp-71

Autor:

Dr. Daniel Mahrenholz
Senior Consultant bei rt-solutions.de GmbH, Köln