Security Corner

Zurück zur Übersicht
Zum Portal

Security Corner: Wie sich die Wirksamkeit der Informationssicherheit messen lässt

Gastbeitrag: Wege aus der Sackgasse des Return of Security Investment (ROSI)

Von Wolfgang Böhmer, CISSP, Auditor der ISO 27001 auf Basis von IT-Grundschutz, Lead Auditor der ISO 27001 registriert bei der UKAS

28. Januar 2008

Was nicht gemessen wird, kann nicht bewertet werden. Was nicht bewertet wird, kann nicht verbessert werden. Das gilt auch für ein Sicherheitsmanagement-System (ISMS). Aber leider fokussieren viele Unternehmen nach wie vor auf eine einseitige Return of Security Investment (ROSI) Betrachtung, die in vielen Fällen in eine Sackgasse führt. Für ein Messsystem, das die Wirksamkeit eines ISMS offen legt, muss eine Kennzahl für die Wirksamkeit (Effektivität) und eine Kennzahl für die Kosten (Effizienz) entworfen werden.

_Wolfgang Böhmer
Foto: Privat

Aufgrund des Kostendrucks reicht es heute nicht mehr aus, nur die Wirksamkeit einer Sicherheitsmaßnahme zu betrachten. Es wird vielmehr gefordert, auch die jeweiligen Kosten in Bezug zu den Gegenmaßnahmen zu kalkulieren. Die Bezifferung des Gegenwertes für Sicherheitsmaßnahmen (Return on Security Investment) ist daher ein Dauerthema in vielen

IT-Sicherheitsabteilungen.

Derzeit orientiert sich diese Diskussion stark an der Verlusterwartung, die durch einen Angriff hervorgerufen wird. Dabei wird die Frage, wie ein geeignetes Messsystems für die Wirksamkeit der Maßnahmen aussieht, meist nicht gestellt.

Für ein Messsystem, das die Wirksamkeit eines Informationssicherheitsmanagementsystems (ISMS) offen legt, muss eine Kennzahl für die Wirksamkeit (Effektivität) und eine Kennzahl für die Kosten (Effizienz) entworfen werden – wie im Management von Prozessen üblich.

Dabei stehen die Kennzahlen der Effektivität und Effizienz in einem funktionalen Zusammenhang. Als Kennzahl der Effektivität kann die Bewertung der Wirksamkeit der Maßnahmen, die zur Abwehr der Risiken entworfen wurden, betrachtet werden. Die Maßnahmen können zum Beispiel entsprechende Policies (Richtlinien), Prozeduren und firmeninternen Standards sein.

Kennzahl der Effektivität: Es sind drei Kennzahlen zweckmäßig, die zu einer Gesamtkennzahl der Effektivität verdichtet werden können. Dabei wird die Verdichtung so vorgenommen, dass die Effektivität zwischen 0 und 1 rangiert:

Mittels Assessment kann geprüft werden, ob die vorhandenen Policies geeignete und ausreichende Prüfpunkte hinsichtlich der Prozeduren, Protokolle, (firmeninterne) Standards etc. aufweisen (Kennzahl der Prüfbarkeit/Messbarkeit).

Mittels Assessment kann geprüft werden, ob die Policies zur Umsetzung der Gegenmaßnahmen bezüglich der Risiken mittels Prozeduren, (firmeninternen) Standards und so weiter vorgenommen wurden und entsprechende Nachweise (Aufzeichnungen) existieren (Kennzahl der Umsetzung).

Mittels Assessment kann geprüft werden, ob für alle kritischen Geschäftsprozesse und den dazugehörigen Assets ausreichend Policies vorliegen (Kennzahl der Vollständigkeit).

Kennzahl der Effizienz: Hierfür bieten sich die Kosten der Gegenmaßnahmen bezogen auf ein Fiskaljahr an, die zur Risikobehandlung aufgewendet werden. Dabei müssen sowohl die indirekten als auch die direkten Kosten zusätzlich zu den Betriebskosten in die Gesamtrechnung zur Vermeidung, Verminderung, Überwälzung und Eliminierung der Risiken einfließen. Diese Kosten werden als infrastrukturelle Kosten bezeichnet.

Anschließend kann die Gesamtkostenentwicklung im nächsten Fiskaljahr mit dem Fiskaljahr zuvor ins Verhältnis gesetzt werden. Somit kann je nach Kostenentwicklung das Verhältnis positiv als auch negativ ausfallen. Negativ dann, wenn im zweiten Fiskaljahr nach einer jahresbedingten Bereinigung mehr Kosten zur Risikoabwehr entstehen als im Fiskaljahr zuvor.

Damit wird ein völlig anderer Ansatz gewählt, als die typische Betrachtung des Return of Security Investment (ROSI) . Denn eine ROSI Betrachtung unterliegt der hypothetischen Kostenbetrachtung einer Verlusterwartung und ist somit für ein Unternehmen nicht sinnvoll.

Betrachtet werden in diesem Kennzahlensystem daher die realen Kosten zweier Fiskaljahre bezogen auf die Aufschlüsselung der Gesamtkosten zur Risikoabwehr. Es entstehen drei Kennzahlen, die wiederum zu einer Gesamtkennzahl der Effizienz verdichtet werden können. Dabei wird die Verdichtung so vorgenommen, dass die Effizienz zwischen 0 und 1 rangiert.

Mittels Assessment können die Kosten zur Risikovermeidung in einem Fiskaljahr ermittelt werden (Kennzahl zur Risikovermeidung).

Mittels Assessment können die Kosten zur Risikoverminderung in einem Fiskaljahr ermittelt werden (Kennzahl der Risikoverminderung).

Mittels Assessment können die Kosten zur Risikoübertragung (Überwälzung) in einem Fiskaljahr ermittelt werden. Hier fallen dann jedoch keine Infrastrukturkosten an. (Kennzahl des Risikotransfers).

Aufgrund von äußeren und inneren Einflüssen können durchaus von einem Fiskaljahr zum nächsten die Kosten schwanken. Es können zum Beispiel Prozesse verbessert werden oder auch die Kosten des Risikotransfers können sich ändern.

Abschließend ist es zur Einschätzung hilfreich, die beiden verdichteten Kennzahlen (Effektivität, Effizienz) in einem Quadrat bestehend aus vier Feldern (Quadranten) darzustellen. Die Quadranten entstehen aus den vier möglichen Kombinationen von Effektivität und Effizienz, wenn diese jeweils die Bewertung zwischen 0 und 1 annehmen können.

Dabei ist in einer ersten Approximation die Effektivität gegeben, wenn der Wert von 0,5 überschritten wird. Gleiches gilt für die Effizienz. Wird für die Effektivität und Effizienz jeweils ein Wert größer als 0,5 ermittelt, unterstützt das ISMS-Leistungspotenzial wirkungsvoll und wirtschaftlich die zweckmäßigen Absicherungsmaßnahmen der kritischen Geschäftsprozesse.

Neben diesem strategischen Gleichgewicht existieren drei Arten des Ungleichgewichts. Im Extremfall des strategischen Dilemmas, wenn die Kennzahlen unter 0,5 liegen, wird das ISMS-Leistungspotenzial nicht ausgeschöpft und die durchgeführten Investitionen verpuffen und sind darüber hinaus kaum beziehungsweise gar nicht wirksam. Feldversuche zeigen bedauerlicherweise, dass sich viele Firmen in diesem ungünstigen Quadranten bewegen.

Die Security-Corner erscheint regelmäßig auf der Homepage der Computer Zeitung in Zusammenarbeit mit (ISC)². In der Kolumne geben IT-Sicherheitsexperten (Certified Information Systems Security Professional, CISSP) Tipps aus der Praxis und kommentieren aktuelle Entwicklungen.

Meinungen bitte an: securitycorner@konradin.de

Zurück zur Übersicht