

Methodik von Renditeanalysen bei Experten umstritten IT-Leiter rechnen bei Sicherheit selten nach

Die Zeiten sind hart, die Kassen leer. Kennzahlen erleichtern da die Entscheidung für oder gegen Investitionen im Schutzbereich. Für mehr Sicherheit sprechen neben abgewendeten Schäden auch neue Prozesse und Einsparungen.

Der Return on Investment kommt aus der Rentabilitätsrechnung. In Zeiten knapper Budgets liegt es nahe, mit einem Return on Security Investments (Rosis) eine Security-spezifische Kennzahl für die Rendite von Investitionen in Sicherheit zu schaffen. „Niemand will mehr Geld in seinen Schutz investieren, als dieser an Nutzen für ihn kreiert“, beschreibt Wolfram Funk, Consultant bei der Meta Group, die Philosophie des Konzepts. Es gelte also, die Kosten für den Schutz mit dem potenziellen Schaden zu vergleichen.

IT-Profis scheuen die Kennziffer

Dirk Fox, Geschäftsführer von Secorvo Consulting, beobachtet allerdings in der Praxis: „Die kaufmännische Leitung fordert die Berechnung von Renditekennziffern ein – die IT-Verantwortlichen jedoch scheuen zurück.“ Er vermutet Unkenntnis über die Ermittlung des Rosis und methodische Schwierigkeiten als Grund für die Verweigerungshaltung.

„Beim Rosis werden zwar die expliziten Kosten problemlos in die Rechnung einbezogen – der implizite Aufwand allerdings wird gerne übersehen“, erklärt Fox. So würden Posten wie Hardware- oder Softwarekosten angesetzt. Die Ausgaben für Personal hingegen würden die Verantwortlichen jedoch meist vergessen, berichtet er weiter. Dabei bilden die bei Alarmen oder zur Pflege von Systemen einen wesentlichen Punkt.

Weiteres schwer zu kalkulierendes Problem: „IT-Sicherheitslösungen ermöglichen oft erst Geschäftsprozesse“, erklärt Fox. „Da ist es schwierig, den Nutzen vorab monetär zu bewerten.“ Als Beispiel nennt er sichere Kommunikation mit Kunden, die Online-Banking erst möglich macht.

Einen Präzedenzfall für den Vorteil einer solchen Renditerechnung liefert die Einführung eines Smartcard-Systems für das Single-Sign-on bei der Schweizer Großbank UBS. Projektleiter Frank Stoll stellte den hohen Kosten für die Smartcard-Einführung die Einsparungen durch die geringere Auslastung des Helpdesk wegen fehlender Passwortanfragen entgegen. Das überzeugte.

Stefan Strobel, Chef von Cirosec, hingegen steht der Berechnung eines Rosis kritisch gegenüber. Nach seiner Erfahrung führen nur wenige Kunden solche Berechnungen aus. „Rosis ist ein Thema für Theoretiker, die lieber Geld für Risikobewertungen als für offensichtlich notwendige Grundschutzmaßnahmen ausgeben“, keult er. Von der Notwendigkeit einer Sicherheitsmaßnahme würde er Firmenentscheider mit einer Demonstration der Einbruchsmöglichkeiten überzeugen. tr