IT-Sicherheit: Weniger ist oft mehr.

Risikomanagement – schlank und nachvollziehbar

Von Dr. Dietmar Posseldt*

Risiken, die man kalkulieren kann, lassen der Unsicherheit keinen Raum – auch wo es um die IT-Sicherheit eines Unternehmens geht. Unternehmen, die sich in diesem Sinne den relevanten Sicherheitsaspekten stellen, bekommen ihre Sicherheitskosten unter Kontrolle, können die Risiken aktiv managen und sichern damit ihre Unternehmenswerte. Nur eine quantitative Risikobewertung eröffnet den Weg zu einem unternehmensindividuellen Optimum zwischen Risikoabdeckung einerseits und IT-Sicherheitsinvestitionen andererseits.

Viele Unternehmen – die tägliche Praxis zeigt es – sind in Sachen IT-Sicherheit nicht optimal aufgestellt; mal ist ihre Risikovorsorge unter-, mal überdimensioniert. Oft reagieren Budget-Verantwortliche beim Bekanntwerden neuer Sicherheitsbedrohungen mit der Frage: „Bei uns ist doch nichts passiert. Investieren wir etwa zuviel in die IT-Sicherheit?“ Auch Marktanalysen bestätigen, dass der Bereich IT-Sicherheit ein Krisengebiet ist.

Während TNS Emnid Ende 2003 feststellte, dass IT-Sicherheitsinstrumente wie Passwortschutz, Anti-Viren-Software und Firewalls fast überall üblich sind, räumte trotzdem jeder fünfte Befragte Gefährdungen durch unzureichende IT-Schutzvorkehrungen ein.

Darüber hinaus kam Forrester Research in 50 US-amerikanischen Großunternehmen zu dem Ergebnis, dass die Budgetierung für die IT-Sicherheit wenig Systematik und demzufolge wenig Effizienz aufweist. So konnten 28 Prozent der befragten Unternehmen ihre IT-Sicherheitsausgaben nicht näher beziffern, viele überziehen auf Grund unpräziser Planung ihre IT-Security-Budgets. Die Konsequenz hieraus ist fehlende Ausgewogenheit zwischen erreichtem Sicherheitsniveau und dem hierfür betriebenen Aufwand.

Woher kommen diese Defizite an Systematik und Effizienz? Oft besteht Unklarheit, welche der zahllosen potenziellen Gefahren für das betreffende Unternehmen relevant sind. Vielfach sind die Spezialkenntnisse bezüglich Technik und Organisation nicht vorhanden, um die komplexe Aufgabe der Identifizierung und Sicherung der Unternehmenswerte qualifiziert, zukunftssicher und bezahlbar angehen zu können. Ebenso gravierend ist aber auch der Mangel an schlanken und pragmatischen Vorgehensweisen, die mit angemessenem Kosten- und Zeitaufwand zu nachvollziehbaren Ergebnissen führen.

Grundlagen schaffen

Das Ziel eines ausgewogenen Verhältnisses zwischen den Kosten für die Sicherheitsmaßnahmen und der Reduktion der Risiken wird man nicht im ersten Anlauf und schon gar nicht für immer erreichen. Das IT-Sicherheitsmanagement ist ebenso wie das Risikomanagement ein iterativer Prozess.

Zielführend und effizient ist es, in der ersten Iteration gemäß der 80:20 Regel die wesentlichsten Risiken durch ein Bündel geeigneter IT-Sicherheitsmaßnahmen abzudecken. Empfehlenswert hierfür ist ein verkürztes Verfahren auf der Basis beispielsweise des BSI-Grundschutzhandbuches.
Es werden dabei die individuellen Risiken durch die Betrachtung pauschalierter Bedrohungen ersetzt, für die wiederum ein Standardkatalog von empfohlenen Maßnahmen besteht. So kann man durch einfachen Soll-Ist-Vergleich die grundlegenden Risiken identifizieren und begrenzen (s. Bild: 1). Da die im Grundschutzhandbuch aufgeführten Maßnahmen recht umfänglich sind, empfiehlt sich dringend eine Priorisierung. Hierfür eignen sich konsolidierte Kataloge, die die Redundanzen des Grundschutzhandbuches vermeiden und aus denen eine A-B-C-Klassifizierung hervorgeht.

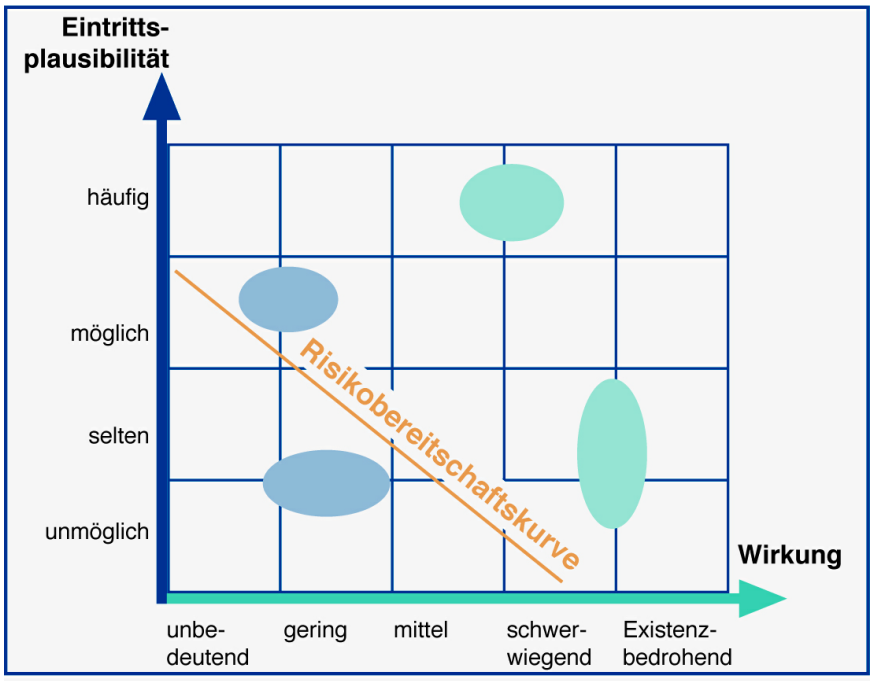

Bild 1: Riskmap

Erst in späteren Iterationen können die Bewertungen verfeinert und entsprechend zukünftiger Bedrohungen aktualisiert werden. Dazu bieten sich dann Verfahren des Risikomanagements an, welche gleichzeitig den Vorteil haben, dass Risk-Manager und IT-Security-Officer nicht nur eine gemeinsame Sprache und Terminologie benutzen. Die inhaltliche Koordination der beiden Prozesse führt zu weiteren Einsparungen. Die verwendeten Begriffe entsprechen ohnehin denen, die für die Behandlung operationeller Risiken nach den gesetzlich vorgegebenen Regularien üblich sind. Zu diesen Regularien gehören Basel II, KonTraG, Sarbanes Oxley, HGB (§289, §317), AO/GDPdU und KWG §25a.

IT-Sicherheits-Entscheidungen objektivieren und quantifizieren

Wer ein Optimum anstrebt muss immer zwischen verschiedenen Handlungsoptionen auswählen können. Entsprechende Methoden und Verfahren ergänzen deshalb das traditionelle Repertoire des IT-Sicherheitsmanagements.

Um Risikopotenziale und Handlungsoptionen zu identifizieren und zu bewerten, kommen Methoden aus der Strategieplanung und des IT-Controlling zum Einsatz. Erfahrungen im Umgang mit beispielsweise der Szenariotechnik und mit betriebswirtschaftlichen Bewertungsverfahren gehören deshalb zum methodischen Rüstzeug. Natürlich ist für die realistische Bewertung der Kosten der Handlungsoptionen und der Risiken auch die Qualität der vom Controlling bereitzustellenden Datenbasis entscheidend.

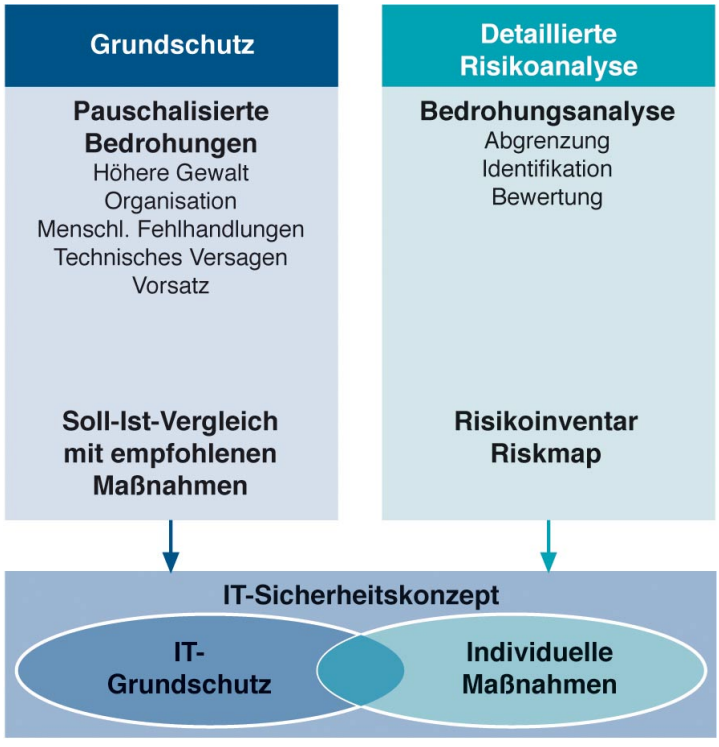

Bild 2: Vorgehen nach BSI

Bei einem gegebenen Bedrohungspotential bestimmt die Risikobereitschaft die Höhe der IT-Sicherheitsinvestitionen. Je nach Lage der unternehmensindividuellen Risikobereitschaft kommen unterschiedliche Maßnahmen in Frage. Zur Visualisierung dieses Zusammenhanges hat sich die Methode der Aufstellung einer Riskmap (s. Bild: 2) bewährt. Sie verdeutlicht neben der Beurteilung von Wirkung und Eintrittsplausibilität des gefährdenden Ereignisses auch sehr gut die Priorität für Gegenmaßnahmen in Abhängigkeit von der Risikobereitschaft.

Für eine detailliertere Betrachtung aller Risiken, die jenseits der Risikobereitschaft liegen (s. Bild: 2) wird ein so genanntes Risikoinventar herangezogen. Es strukturiert die Risiko- und Maßnahmenbewertung, und priorisiert diejenigen Maßnahmen, die die höchste Wirkung haben. Das Risikoinventar liefert auch den Ansatzpunkt, die finanziellen Auswirkungen möglicher Sicherheitsvorfälle quantitativ zu bewerten und daraus fundierte Return-on-Investment-Betrachtungen für die IT-Sicherheitsmaßnahmen anzustellen. Dafür werden die Drohverluste vor und nach der Maßnahmenergreifung für das jeweilige Risiko bestimmt und direkt den Aufwänden der Schutzmaßnahme gegenüber gestellt (s. Bild: 3).

Maßnahmen	Drohverlust	Material-Kosten		Kosten Bedienung und Betrieb		Summe Kosten		Interne Weiterver-rechnung
		Fix	Variabel	Fix	Variabel	Fix	Variabel	

Bild 3: Wertmäßige Gegenüberstellung von Maßnahmen und Risiken als Drohverlust

Damit sind die Voraussetzungen für das Erreichen des „Optimum-Sektors“ (s. Bild: 4) geschaffen. Solange die monetär bewertete Risikominderung größer als die Kosten der zugehörigen Maßnahmen ist, der Return on Security Investment (ROSI) also positiv ist, bewegt sich das Unternehmen noch auf die Zone eines ausgewogenen Kosten-Nutzen-Verhältnisses (Optimum) zu.

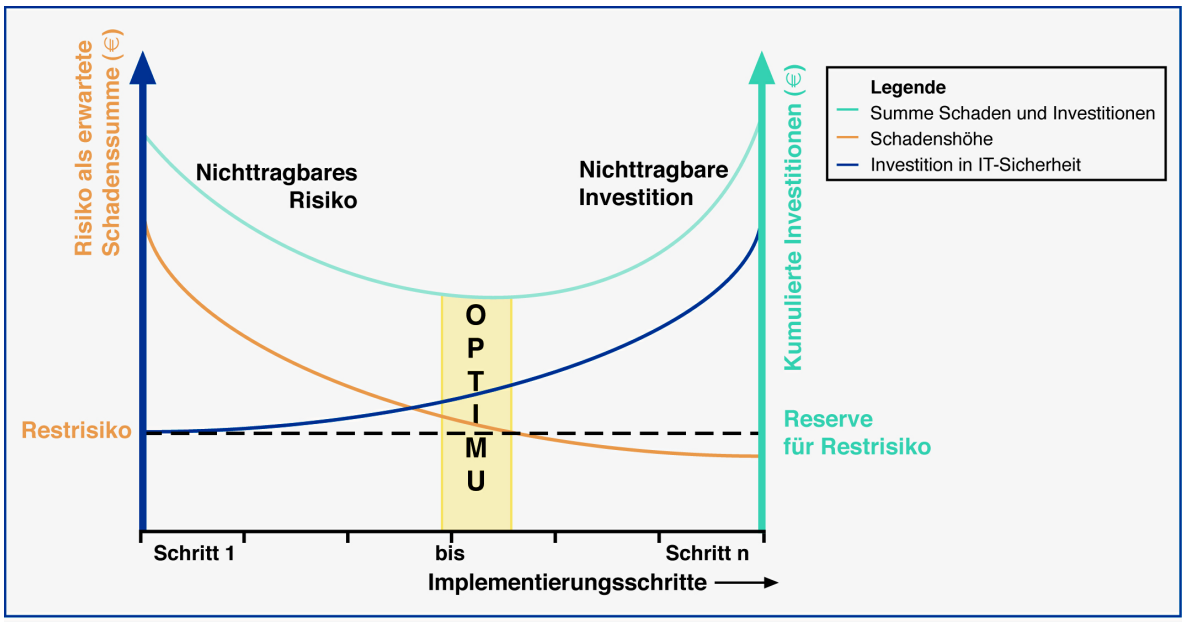

Bild 4: Optimum bei den Investitionen in die IT-Sicherheit
Vgl.: N. Pohlmann: „Wirtschaftlichkeitsbetrachtung von IT-Sicherheitsmechanismen“

Sicherheit als integraler Bestandteil des Managementprozesses

IT-Sicherheit liegt in der Verantwortung der Geschäftsführung, ist aber nur dann dauerhaft, wenn jeder Mitarbeiter den dafür notwendigen Prozess als integralen Bestandteil seines Arbeitsalltages „lebt“. Dieser Prozess findet seine Nachhaltigkeit in einer klar beschriebenen Leitlinie, die Ziele, Verantwortlichkeiten und grundsätzliche Maßnahmen der IT-Sicherheit für das Unternehmen zusammenfasst. Zum anderen lebt er von einem Sicherheitsmanagement, das die Phasen Analyse, Umsetzung und Überwachung (s. Bild: 5) als Regelkreis versteht und gewährleistet.

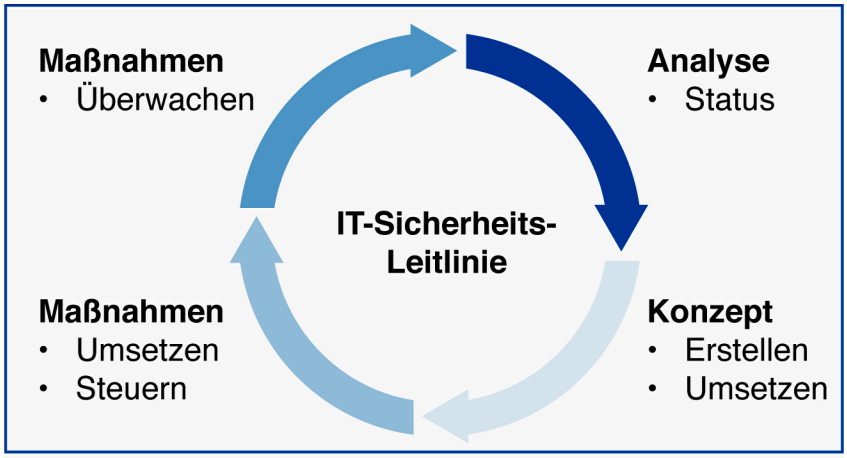

Bild 5: IT-Sicherheitsmanagement

Dieser quantitative Ansatz zur fundierten Etablierung des passenden Sicherheitslevels ist für jedes Unternehmen erreichbar. Voraussetzung ist, dass es sich die eigenen Daten und Erfahrungen nutzbar macht und darüber hinaus den externen Austausch mit anderen Fachleuten pflegt.

Die INSENTIS Managementberatung hat mit der skizzierten Vorgehensweise einen pragmatischen Ansatz entwickelt, der es Unternehmen ermöglicht, den Investitionen in die IT-Sicherheit die monetär bewertete Reduktion der Risiken gegenüber zu stellen und so die Wirtschaftlichkeit der Maßnahmen zu beurteilen. Grundlage dafür ist eine Kombination und Straffung erprobter Vorgehensmodelle des BSI-Grundschutz, des Risikomanagements und neuerer Konzepte wie ROSI (Return on Security Investment). Damit haben die Unternehmen die Möglichkeit, auf der Basis einer definierten Risikobereitschaft, zielgerichtet einen robusten Schutz gegen die wesentlichen Risiken zu erreichen, zu managen, nachzuweisen und immer mit Blick auf die Kosten anforderungsgerecht auszubauen.

* Dr. Dietmar Posseldt ist Management Consultant der Insentis GmbH, Geisenheim.