Investitionen in IT-Sicherheit mit Augenmaß

Von Dr. Dietmar Posseldt*

In einem Großteil der Unternehmen sind Sicherheitsmaßnahmen bereits ergriffen und orientieren sich an bewährten Vorgehensmodellen und Methoden wie zum Beispiel dem BSI-Grundschutzhandbuch. Trotzdem besteht Unsicherheit, ob damit die für das Unternehmen wichtigen Risiken abgedeckt sind und ob sich der zu betreibende Aufwand im Rahmen eines angemessenen Kosten-Nutzen-Verhältnisses bewegt.

Diese Unsicherheit zu beseitigen und zugleich den Gesamtaufwand im IT-Sicherheitsmanagement zu reduzieren, hat sich die INSENTIS-Managementberatung zum Ziel gesetzt.

Die Lösung besteht in einem methodischen Ansatz, der das Risikomanagement und das IT-Sicherheitsmanagement integriert, der die Redundanzen bisheriger Ansätze vermeidet und der über eine Quantifizierung von Kosten und Nutzen die Rentabilität jeder einzelnen Sicherheitsmaßnahme gewährleistet.

Aufwand reduzierend wirkt insbesondere die Möglichkeit, die Betrachtungstiefe an die Situation des jeweiligen Unternehmens anzupassen und unter Wiederverwendung bereits gewonnener Erkenntnisse die Sicherheitsstrategie und das Verhältnis zwischen Aufwand und Nutzen iterativ zu verfeinern und zu optimieren.

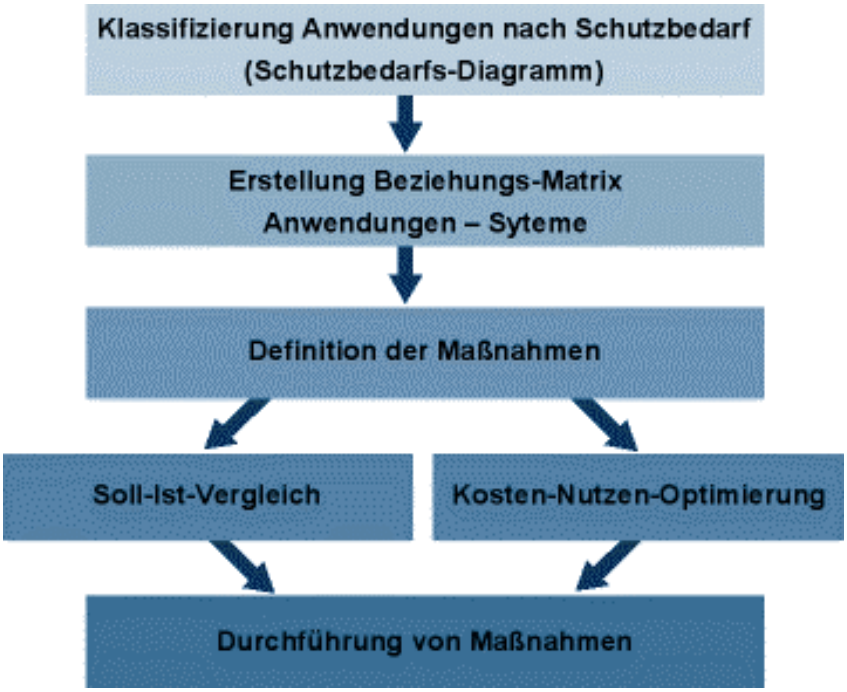

Bild 1: INSENTIS-IT-Sicherheitsmanagement

Wie dem Ablaufdiagramm (Abb. 1) zu entnehmen ist, stehen am Anfang der Analyse die Geschäftsprozesse, die mit IT-Anwendungen unterstützt werden. Die Anwendungen werden in einem Schutzbedarfs-Diagramm erfasst und nach ihrem Schutzbedarf klassifiziert. Maßstab hierfür ist der Schutzbedarf des Geschäftsprozesses (Prozessansatz) und nicht der des IT-Systems. Dabei werden zur quantitativen Bewertung der Risiken die Drohverluste bestimmt, die für die denkbaren Schadensszenarien eintreten.

Als nächstes wird die Beziehungsmatrix erstellt, die den Anwendungen die IT-Systeme und –Funktionen zuordnet, die die Anwendungen betreiben. Diesen Systemen und Funktionen ist damit der Schutzbedarf der Anwendungen zugeordnet.

Die zu definierenden Schutzmaßnahmen werden im nächsten Schritt aus dem Spektrum der verfügbaren Möglichkeiten zur Risikoreduktion (Vermeiden, Vermindern, Überwälzen und Selbsttragen), beim höchsten Schutzbedarf beginnend, ausgewählt. Vorhandene (objektorientierte) Standards, wie z.B. BSI-Grundschutz, werden dabei genutzt. Da viele Maßnahmen nicht nur für ein IT-System oder eine IT-Funktion wirksam sind, vermeidet die INSENTIS-Methodik unnötige Redundanzen, indem sie die Maßnahmen jeweils nur einmal für verschiedene Objekte betrachtet

Mit den definierten Maßnahmen können nun zwei verschiedene Ziele bedient werden:

1. Die marginale Betrachtung hat die Aufgabe, die Differenz zwischen Soll und Ist abzuleiten und erforderliche Projektschritte zur Schließung eventueller Sicherheitslücken zu identifizieren.

2. Die ganzheitliche Betrachtung verschiedener Handlungsoptionen dient der Identifikation eines Optimums zwischen Kosten und Nutzen durch die quantitative Gegenüberstellung der Drohverlust-Reduktion und der dafür erforderlichen investiven Maßnahmen.

Zum Schluss sind im Rahmen eines Change-Management-Prozesses die identifizierten Maßnahmen umzusetzen.

Diese Vorgehensweise kann auch für weitere Verfeinerungen oder aus Anlass veränderter Situationen wiederholt werden und dabei auf den bereits gefundenen Ergebnissen aufbauen. Sie sichert die Ausgewogenheit zwischen reduziertem Schadenspotenzial und investivem Aufwand. Durch Vermeidung von Redundanzen, durch die Betrachtung mit reduziertem Detaillierungsgrad und durch die konsequente Prozesssicht liefert sie schneller quantitativ bewertete Ergebnisse. Außerdem erfüllt sie die Anforderungen an die Transparenz bezüglich der Risiken und der Effektivität der Schutzmaßnahmen, die das heutige Risikomanagement und die Unternehmensführung fordern. Die Ergebnistypen sind vollständig kompatibel zu denen des Risikomanagements auf Unternehmensebene. Diese Durchgängigkeit liefert weitere Aufwands- und Kosteneinsparungen.

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