publikationen

calpana

8. Mai 2006

Das Paradoxon der Eintrittswahrscheinlichkeit in der Informationstechnologie

Ein innovativer Ansatz zur Lösung des Problems

Ein Fachbeitrag von
DI Dr. Manfred Stallinger, MBA

Impressum:

calpana business consulting gmbh
Bockgasse 2a
4020 Linz
Tel: +43.732.601216-0
Fax: +43.732.601216-209
email: office@calpana.com

Für den Inhalt verantwortlich:
DI Dr. Manfred Stallinger, MBA

Das Paradoxon
der Eintrittswahrscheinlichkeit in der IT.

DI Dr. Manfred Stallinger Geschäftsführender Gesellschafter der calpana business consulting gmbh, Lektor an der Donauuniversität Krems und geistiger Vater von der CRISAM® Methode.

Wie wahrscheinlich ist es, dass der neu installierte Server ausfällt, dass Unbefugte in den Serverraum eindringen können, oder dass vertrauliche Informationen in unerwünschte Hände gelangen? Diese und ähnliche Fragen im Kontext mit der Informationstechnologie sind unter seriösen Gesichtspunkten erst oft nach mehrjähriger Erfahrung zu beantworten. Um jedoch ein zeitnahes IT-Risikomanagement zu führen, werden diese Informationen heute und nicht erst in 3 Jahren benötigt. Rund um dieses Paradoxon drehten sich zahlreiche spontane Diskussionen während des IT-Riskmanagement Forums 2006 in Köln.

DI Dr. Manfred Stallinger, MBA

Garbage In – Garbage Out

Wirft man einen Blick hinter die Kulissen, so herrschen in der Praxis bei namhaften Unternehmen grundsätzlich zwei Methoden vor. Einerseits das Einschätzen auf „Gering – Mittel – Hoch“ oder anderseits das Festlegen einer fiktiven Zahl aufgrund eines Bauchgefühls. Werte, die zumeist in Systeme (Softwaretools, die der Unterstützung dienen) eingepflegt werden und die Risikowahrheit ungenügend abbilden. „Garbage in - Garbage out“, könnte man nach einem bekannten IT-Grundsatz etwas forsch die Methoden auf den Punkt bringen.

Die Lösung mit der Methode CRISAM®

Die Grundlage der CRISAM®-Methode stellt der so genannte „Stand der Technik“(siehe Exkurs) dar, welcher als Referenzmaß verwendet wird und in Form des Standard & Poors Ratingmodells ausgedrückt wird. Mittels Audits während der Risikoanalyse werden die Abweichungen (Über- bzw. Untererfüllung) zum Stand der Technik bewertet. Der damit ermittelte Qualitätsgrad (Abweichung zum Stand der Technik) wird zur Berechnung der Eintrittswahrscheinlichkeit herangezogen. Somit bestimmt die Qualität des Risikoobjektes direkt die Eintrittswahrscheinlichkeit einer möglichen Bedrohung.

Die Methode CRISAM® ist ein Best Practice Ansatz und ist wissenschaftlich anerkannt.

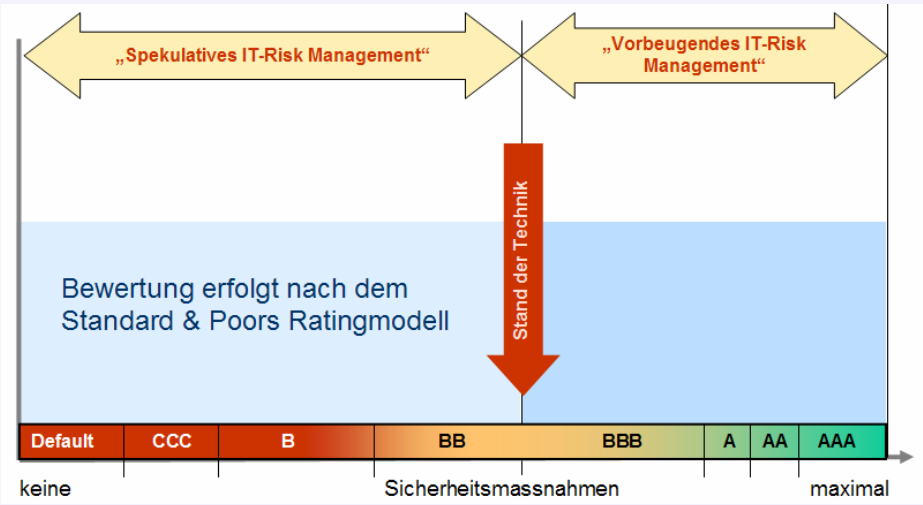

Abbildung 1: Positionierung des „Stand der Technik“ im Standard & Poors Rating Modell

*EXKURS: Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Gesundheit der Beschäftigten gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere vergleichbare Verfahren, Einrichtungen und Betriebsweisen heranzuziehen, die mit Erfolg in der Praxis erprobt worden sind.

Was sagt Wikipedia zum „Stand der Technik“?

Der Stand der Technik ist eine Technikklausel und stellt die technische Möglichkeiten zu einem bestimmten Zeitpunkt, basierend auf gesicherten Erkenntnissen von Wissenschaft und Technik dar. Er findet sich in vielen Vorschriften und Verträgen und wird durch die Regelungen zur Rechtsförmlichkeit präzise definiert.

Der Stand der Technik beinhaltet auch, dass er wirtschaftlich durchführbar ist. Dies heißt nicht, dass jedes Unternehmen sich den Stand der Technik leisten kann, aber die Mehrheit in dem betreffenden industriellen Sektor. Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung der Maßnahme im Hinblick auf die angestrebten Ziele (z.B. der Ziele des Arbeitsschutzes, des Umweltschutzes, der Sicherheit für Dritte, der Wirtschaftlichkeit: Also allgemein zur Erreichung eines allgemein hohen Niveaus bezogen auf die zu beachtenden Aspekte) insgesamt gesichert erscheinen lässt. Für das IT-Risikomanagement bezieht CRISAM die Informationen aus dem deutschen Grundschutzhandbuch des BSI, der ISO27000 Normenreihe, ITIL, Cobit und dem österr. Sicherheitshandbuch.