Sandy Eggert

Das aktuelle Stichwort: Security management

first published in:
ERP-Management 4 (2008), 4, S. 10

Postprint published at the Institutional Repository of the Potsdam University:
In: Postprints der Universität Potsdam
Wirtschafts- und Sozialwissenschaftliche Reihe ; 022
http://opus.kobv.de/ubp/volltexte/2010/4446/
http://nbn-resolving.de/urn:nbn:de:kobv:517-opus-44467

Postprints der Universität Potsdam
Wirtschafts- und Sozialwissenschaftliche Reihe ; 022

Das aktuelle Stichwort

Security Management

Sandy Eggert, Universität Potsdam

ERP-Systeme zeichnen sich zunehmend durch eine höhere Integrationstiefe aus. Zudem steigt auch die Abhängigkeit von der Informationstechnologie insgesamt. Damit einher geht auch der steigende Bedarf an Sicherheit der eingesetzten Systeme. Das IT-Security Management stellt ein Teilgebiet des IT-Managements dar, welches die IT-Sicherheit im Fokus hat. Ziel ist es, die Sicherheit von Anwendungssystemen in Bezug auf die Integrität, Authentizität, Vertraulichkeit, Verfügbarkeit und Verbindlichkeit zu gewährleisten. Im Rahmen eines Sicherheitskonzeptes werden konzeptionelle Sicherheitsanforderungen festgehalten und daraus resultierende Maßnahmen festgelegt. Im Zusammenhang mit dem Security Management stehen die Aufdeckung und Minderung von Gefahrenpotenzialen sowie das Risikomanagement.

Gefahrenpotenziale

Allgemeine Gefahrenpotenziale, bezogen auf Angriffe auf Anwendungssysteme, wie ERP-Systeme richten sie generell gegen die Infrastruktur, Benutzer, Netze und Schnittestellen. Diese Angriffspunkte umfassen eine Vielzahl von Angriffsszenarien, welche wiederum die Gefahren ableiten lassen. Eine Klassifizierung dieser Gefahren erlaubt weiterhin eine Ableitung und Einstufung in Bezug auf einen abgegrenzten Bereich. Darunter befinden sich bspw. Gefahren höherer Gewalt (z.B. Naturkatastrophen) oder auch Gefahren aus organisatorischen Mängeln (z.B. Umgang mit Passwörtern) [1]. Ziel ist die Gefahrenpotenziale zur erkennen und geeignete Maßnahmen zu treffen, diesen Gefahren entgegen zu wirken.

Risikomanagement

Die Risiken im IT-Bereich sind vielfältig und gehen von der Datensicherheit und Sicherstellung der Infrastruktur bis hin zur Formulierung und Implementierung einer IT-Strategie [2]. Das Ziel bei der Entwicklung und Etablierung eines Risikomanagements ist nach Rauschen und Disterer eine Organisation zur Identifikation und Beeinflussung aller Risiken, die die Vermögens-, Finanz-, und Ertragslage des Unternehmens gefährden [2]. Die dabei zu unterscheidenden Risikofelder sind in Bild 1 dargestellt.

Um eine Risikobewertung durchführen zu können, sollen zunächst die wesentlichen Phasen des IT-Risikomanagements unterschieden werden. Dazu gehören die Risikoidentifikation, -analyse, -steuerung und –überwachung.

Risikoidentifikation: Um eine strukturierte Risikoidentifikation durchführen zu können, sollten zunächst gegenwärtige und zukünftige Risikobereiche erfasst werden. Dieses frühzeitige Erkennen und Erfassen aller Risiken bildet die Grundlage zur Risikoanalyse [2].

Risikoanalyse: Hier werden identifizierte Risiken analysiert und bewertet, um eine Einordnung in einem Risikoportfolio vornehmen zu können. Die Risikobewertung kann unter qualitativen und quantitativen Aspekten erfolgen [2].

Risikosteuerung: Die identifizierten und analysierten Risiken sollen in dieser Phase durch geeignete Maßnahmen gezielt beeinflusst werden. Hierbei werden vorbeugende Maßnahmen getroffen, die die Eintrittswahrscheinlichkeit des Risikos verringern.

Risikoüberwachung: Die Überwachungsphase beinhaltet geeignete Steuerungsmaßnahmen, die der Beeinflussung der Risikolage dienen. Damit einher geht auch die Überprüfung der Wirksamkeit der Steuerungsmaßnahmen.

Bild 1: Risikokategorien [2]

Risiken aus dem Management der IT	Organisatorische Risiken	Technische Risiken	Sicherheitsrisiken
Projektbezogene Risiken	Kosten- und leistungsbezogene Risiken	Infrastrukturelle Risiken	Anwendungs- und prozessbezogene Risiken

Fazit

Insgesamt darf das IT-Sicherheitsmanagement nicht als einmalige, zeitpunktbezogene Durchführung von bestimmten Maßnahmen angesehen werden Vielmehr sollte es als kontinuierlicher Prozess im Unternehmen etabliert werden.

Literatur:

[1] Humpert, F.: IT-Sicherheit. In: IT-Sicherheit, Mörike, M. (Hrsg.) 2004. S.7-18
[2] Rauschen, T.; Disterer, G.: Identifikation und Analyse von Risiken im IT-Bereich. In: IT-Sicherheit, Mörike, M. (Hrsg.) 2004. S.19-32