Technik

Marc Laszlo

Security Risk Management

Kostenbetrachtung bei der Untersuchung von IT-Risiken

Diplomarbeit

Diplom.de

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlages. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 2004 Diplom.de
ISBN: 9783832480059

https://www.diplom.de/document/223210

Marc Laszlo

Security Risk Management

Kostenbetrachtung bei der Untersuchung von IT-Risiken

Diplom.de

Marc Laszlo

Security Risk Management

Kostenbetrachtung bei der Untersuchung von IT-Risiken

Diplomarbeit
Fachhochschule Darmstadt
Fachbereich Informatik
Abgabe Februar 2004

Diplom.de

Diplomica GmbH
Hermannstal 119k
22119 Hamburg

Fon: 040 / 655 99 20
Fax: 040 / 655 99 222

agentur@diplom.de
www.diplom.de

ID 8005

ID 8005
Laszlo, Marc: Security Risk Management –
Kostenbetrachtung bei der Untersuchung von IT-Risiken
Hamburg: Diplomica GmbH, 2004
Zugl.: Fachhochschule Darmstadt, Diplomarbeit, 2004

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden, und die Diplomarbeiten Agentur, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Diplomica GmbH
http://www.diplom.de, Hamburg 2004
Printed in Germany

Inhaltsverzeichnis

Vorwort 5

1 Einführung 7

1.1 Motivation 7

1.2 Abgrenzung 8

1.3 Begriffsdefinition 9

2 Grundlegendes zu Kosten und IT-Sicherheit 11

2.1 Das „Firewall-Paradoxon" in der IT-Sicherheit 11

2.2 IT-Sicherheitsprobleme bei Netzwerkstrukturen 14

2.3 IT-Sicherheit als wichtiger Unternehmensprozess 17

2.4 IT-Sicherheit bei E-Business-Anwendungen 19

3 Das IT-Risikomanagement 22

3.1 Überblick IT-Risikomanagement 22

3.2 Die Elemente des IT-Risikomanagement-Systems 24

3.3 Der IT-Risikomanagement-Prozess 27

3.3.1 Risikoidentifikation 30

3.3.2 Risikoanalyse 30

3.3.3 Risikosteuerung 31

3.3.4 Risikoüberwachung 32

4 Strategien und Probleme der IT-Risikobehandlung ... 33

4.1 Mögliche Risikotypen im Unternehmen 33

4.2 Darstellung des Lösungsansatzes “Total Cost of Risk” ... 34

4.3 Die Problematik der Kostenreduktion 36

4.4 Strategien der IT-Risikobehandlung 38

5 Untersuchung der Kosten von IT-Risiken 40
5.1 Darstellung relevanter Kostenarten bei IT-Risiken 40
5.1.1 Einmalige / kontinuierliche Kosten 42
5.1.2 Offene / verdeckte Kosten 43
5.1.3 Wiederherstellungskosten 44
5.1.4 Vorsorgekosten..... 44
5.2 Prozesskosten und IT-Komponenten.....45
5.3 Kostenstruktur komplexer IT-Bedrohungen 49
5.4 Neue Geschäftsfelder durch Kontrolle von IT-Risiken 51
5.5 Grenzen bei der Kostenbewertung von IT-Risiken.....52

6 Methode zur detaillierten Analyse von IT-Risiken 53
6.1 Kategorisierung von IT-Risiken 53
6.1.1 BS 7799 / ISO 17799 55
6.1.2 IT-Grundschutzhandbuch des BSI..... 58
6.2 Die Problematik der Eintrittswahrscheinlichkeit 59
6.3 Potenzielle Schäden durch IT-Risiken.....60
6.3.1 Schadensarten..... 60
6.3.2 Schadensmesspunkte 61
6.4 Gegenmaßnahmen bei IT-Risiken.....62
6.4.1 Arten von Maßnahmen..... 62
6.4.2 Maßnahmenmesspunkte..... 63
6.5 Ein Lösungsmodell für das „IT-Risiko Audit”.....64
6.5.1 IT-Schadensklassen..... 65
6.5.2 IT-Risikoklassen..... 65
6.5.3 Der „Security Risk Factor” 66
6.5.4 Das “Corporate Risk Rating” 67
6.5.5 Der IT-Risikobewertungsprozess 68

6.6 Vorschläge für Arbeitsmaterialien zum "IT-Risiko Audit" 70
6.6.1 Die SRM-Risikotabelle 70
6.6.2 Beispiel 72
6.6.3 Der SRM-Fragebogen 73
6.6.4 Beispiel 75
6.6.5 Der SRM-Bewertungsbogen 76
6.6.6 Beispiel 79
6.6.7 Die SRM-Auswertungsmatrix 81
6.6.8 Beispiel 83

7 Zusammenfassung und Ausblick 84

A Glossar 87

B Abbildungsverzeichnis 90

C Tabellenverzeichnis 90

D Literaturverzeichnis 91

E Anhang 93
E.1 Digitale Version der Arbeit 93
E.2 Die SRM-Risikotabelle 93
E.3 Der SRM-Fragebogen 93
E.4 Die SRM-Auswertungsmatrix 93
E.5 Projektplan 93
E.6 Mögliche Risikotypen in Unternehmen 93

Vorwort

Durch meine Arbeit bei einem der weltweit führenden System-integratoren und in der IT-Consulting Firma meines Vaters wurde ich schnell mit der Problematik von Wirtschaftlichkeit, Investitions-sicherheit und technisch sinnvollen Strukturen im Bereich der IT-Sicherheit konfrontiert. Es war für mich immer sehr unbefriedigend, nur hypothetische Aussagen über die Kosten treffen zu können, die dem Kunden durch das Auftreten von IT-Risiken in seinem Unternehmen entstehen können. Da sich diese Kosten aus vielen unterschiedlichen Teilkostenarten zusammensetzen und die mögliche Eintrittswahrscheinlichkeit des IT-Risikos, ein nur schwer exakt berechenbarer Kernfaktor für die Gesamtkostenermittlung, von zentraler Bedeutung ist, gestaltet sich eine solche Risikokosten-berechnung sehr schwierig und zeitaufwändig. Diese wird aber zwingend benötigt, um bei Investitionsvorhaben in diesem Bereich betriebswirtschaftlich fundiert gegenüber Kunden oder den betrieblichen Budgetverantwortlichen argumentieren zu können.

Der Reiz, meine Bachelorarbeit über dieses Thema zu schreiben, bestand für mich darin, dass ich mein technisches Wissen über IT-Sicherheit und meine praktischen Erfahrungen mit einer betriebswirtschaftlichen Fragestellung aus meinem Studien-schwerpunkt verbinden konnte, ohne dabei die darunter liegenden technischen Aspekte gänzlich vernachlässigen zu müssen.

Diese Arbeit verfolgt den Ansatz, die etablierten und bekannten Bereiche IT-Sicherheit und IT-Risikomanagement über eine neue Schnittmenge zu verbinden, um dadurch eine Möglichkeit zu entwickeln, Schadenspotenziale in der Informationstechnologie für Firmen kostenmäßig erfassbar und somit bewertbar zu machen.

Es wird in Zukunft von zentraler Bedeutung für jeden IT-Budget-Verantwortlichen sein, die finanziellen Auswirkungen von Risiken der IT-Sicherheit auf seine IT-Komponenten möglichst genau zu kennen und damit bewertbar zu machen. Durch die Identifikation und Bewertung der IT-Risiken lassen sich entsprechende Strategien für jedes Risiko entwickeln, um dessen geschäftsschädigende Wirkung möglichst zu minimieren. Zu betrachten sind dabei die direkten Kosten des Schadens sowie die daraus resultierenden Folgekosten bei Unternehmensprozessen und die Kosten, die durch Wiederherstellung

des Zustandes vor Schadenseintritt verursacht werden. Eventuelle Kosten zur Risikovorsorge werden dabei gesondert behandelt.

Des Weiteren entstehen aus den Bereichen Corporate Governance[1][2] und Unternehmenscontrolling Fragestellungen mit IT-Sicherheits-relevanz. Durch neue und verschärfte Vorgaben des Gesetzgebers[3] und Anforderungen des Kapitalmarktes[4] entstehen zusätzliche Anforderungen an das IT-Sicherheits- sowie das IT-Risiko-management.

Die Einführung setzt sich mit allgemeinen und übergeordneten Fragestellungen zur IT-Sicherheit in Unternehmensnetzwerken auseinander. Diese werden wie in diesem Zusammenhang nur so detailliert dargestellt wie notwendig, um dem Leser die benötigten Grundlagen vermitteln zu können, die er für das Verständnis dieser Arbeit benötigt. Die folgenden Kapitel beschäftigen sich mit wichtigen Aspekten des klassischen IT-Risikomanagements und stellen einen bereits existierenden Lösungsansatz zur IT-Risikobewertung vor.

Im Kern der vorliegenden Arbeit werden die durch IT-Risiken potenziell entstehenden Kosten und deren Abhänigkeiten im Unternehmens-kontext betrachtet. Des Weiteren werden die entscheidenden Kernelemente und Funktionen des entwickelten Modells für ein „Security Risk Audit" anhand von speziell dafür erarbeiteten Arbeitsmaterialien konkretisiert und erläutert.

Mein Dank geht an dieser Stelle an meinen fachlichen Betreuer, Herrn Dr. Gerald Spiegel, der sich bei der SerCon GmbH seit einigen Jahren mit dieser Problemstellung und verwandten Themen beschäftigt, dazu diverse Vorträge gehalten sowie mehrere Publikationen verfasst hat.

Marc Laszlo im Winter 2003/2004

---

[1] Vgl. Macharzina (2003) S.140 ff

[2] Siehe Glossar unter „C"

[3] Durch Gesetze zur Risikokontrolle in der Unternehmensführung (z.B. KonTraG)

[4] z.B. durch Basel II (Eigenkapitalvorsorge zur Risikominimierung bei der Kreditvergabe im Bankgewerbe)