

Sebastian Klipper

Information Security Risk Management

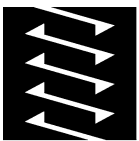
Sebastian Klipper

Information Security Risk Management

Risikomanagement mit ISO/IEC 27001, 27005
und 31010

Mit 31 Abbildungen, 10 Tabellen und 14 Fallbeispielen

PRAXIS



VIEWEG+
TEUBNER

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

Das in diesem Werk enthaltene Programm-Material ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor übernimmt infolgedessen keine Verantwortung und wird keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programm-Materials oder Teilen davon entsteht.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage 2011

Alle Rechte vorbehalten

© Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011

Lektorat: Christel Roß | Maren Mithöfer

Vieweg+Teubner Verlag ist eine Marke von Springer Fachmedien.

Springer Fachmedien ist Teil der Fachverlagsgruppe Springer Science+Business Media.

www.viewegteubner.de



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

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.

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Printed in Germany

ISBN 978-3-8348-1360-2

Dank

Dank

„Begegnet uns jemand, der uns Dank schuldig ist, gleich fällt es uns ein. Wie oft können wir jemandem begegnen, dem wir Dank schuldig sind, ohne daran zu denken!“

Johann Wolfgang von Goethe



Zunächst gilt natürlich allen mein Dank, die mich bei der Arbeit an diesem Buch unterstützt haben.

Dr. Michael Pietsch danke ich für die Unterstützung bei der Ideensammlung zur Verknüpfung von Buch und Internet und deren Umsetzung.

Dr. Jörg Kümmerlen danke ich für die moralische und fachliche Unterstützung beim Abschnitt zu den Risikomanagement-Tools.

Besonderer Dank gilt meinen Kunden und Lesern, die mich mit Projektaufträgen und dem Kauf meiner Bücher bei der Arbeit am Thema Security Management unterstützen.

Vorwort

„Nichts geschieht ohne Risiko, aber ohne Risiko geschieht auch nichts.“

Walter Scheel



Die Geschichte dieses Buchs begann vor etwa einem Jahr, als ich es selbst kaufen wollte. Sie haben ganz Recht, da war es noch gar nicht geschrieben. Ich war auf der Suche nach einem Buch, das sich explizit mit dem Management von Sicherheitsrisiken auf Basis des ISO/IEC-Standards 27005 beschäftigt. Meine Vorstellung war es, ein Buch zu finden, in dem das Thema Risikomanagement als integraler Bestandteil der ISO/IEC Normenreihe 27000 verstanden und beschrieben wird. Ich musste feststellen, dass es so ein Buch noch nicht gibt und beschloss daher, es selbst zu schreiben.

Motivation

Hierzu gehörte insbesondere die Frage, welche Standards der ISO/IEC-Normenreihen für die Implementierung eines Risikomanagementsystems wichtig sind und welche nicht. Will man dieser Frage auf den Grund gehen, indem man die Standards selbst zu Rate zieht, belaufen sich die Investitionskosten schnell auf einige

Welche Norm ist die passende?

tausend Euro. Das Buch will diese Standards natürlich keinesfalls ersetzen. In der Regel sollten Sie einige davon trotzdem erwerben. Besonders die Standards 27001, 27002 und 27005 dürfen in keiner Grundausstattung fehlen, wenn Sie sich ernsthaft mit ISO/IEC 27000 auseinandersetzen wollen.

Von der Theorie
zur Praxis

Der reine Kauf von Standards und deren Lektüre führt jedoch auch nicht zwangsläufig zum Erfolg. Daher war eine weitere wichtige Frage, die ich mir stellte, wie sich die generischen Formeln eines Standards in die Praxis übertragen lassen und welche Möglichkeiten es gibt, auf der ISO-Klavatur zu improvisieren. Niemandem ist geholfen, wenn man Standards vom Blatt abliest. Die eigentliche Kunst ist es, sie im eigenen Unternehmen oder dem Unternehmen des Kunden umzusetzen.

Der Mensch
steht im
Mittelpunkt ...

Ich werde mich daher nicht nur der Frage widmen, was die Standards vorschlagen, sondern ebenso erörtern, wie sich die Anforderungen und Vorschläge eines Standards mit den anderen Zwängen, Zielen, Prioritäten und Risiken eines Unternehmens oder einer Behörde in Einklang bringen lassen. Wie schon in meinem ersten Buch „*Konfliktmanagement für Sicherheitsprofis*“ [1] steht dabei der Mensch im Mittelpunkt. Spitze Zungen fügen diesem geflügelten Wort gerne folgenden Halbsatz hinzu: „...und damit allen im Weg“. Richtig muss es heißen:

Der Mensch steht im Mittelpunkt ... jeder Sicherheitsbetrachtung!

Wie schwierig es ist, die Frage nach der praktischen Umsetzung ausschließlich anhand des Standards zu beantworten, zeigt sich bei einem kleinen Test: Der gesamte Risikomanagementprozess soll laut Standard durch die Kommunikation von Informationssicherheitsrisiken überspannt werden.



ISO/IEC 27005

11. Kommunikation von Informationssicherheitsrisiken:

Tätigkeit: Informationen zu Risiken sollen zwischen den Entscheidungsträgern und anderen Prozessbeteiligten ausgetauscht und/oder geteilt werden.

Erläutert wird diese Tätigkeit im Standard auf nur einer Seite. Das reicht natürlich in der Praxis kaum aus, um vor einer Bruchlandung bewahrt zu werden.

Daher wird das Buch regelmäßig die durch die Standards eingetretenen Pfade verlassen und nach weiteren Wegen suchen, auf denen Sie ihre Ziele erreichen können. Ein eigenes Kapitel beschäftigt sich so zum Beispiel mit der Frage, ob man ISO/IEC 27005 in einem IT-Grundsicherungsprojekt einsetzen kann, in dem eine erweiterte Risikoanalyse notwendig ist.

Eingetretene
Pfade verlassen

Im Grunde ging es bei der Arbeit an diesem Buch also darum, die Fragen zu beantworten, die sich mir selbst bei meinen Projekten als Security-Consultant gestellt hatten. Sie erinnern sich, dass ich das Buch ursprünglich kaufen und nicht selbst schreiben wollte. Ergänzt wurden sie durch Fragen, die sich in zahlreichen Gesprächen ergeben haben, die ich während der Recherche mit Anwendern der ISO/IEC 27000 Familie geführt habe.

Meine Hoffnung ist es, dass die Schnittmenge mit Ihren Fragen dadurch besonders groß ist und Sie in dem Buch die Antworten finden, die Sie in Ihrem täglichen Schaffen weiterbringen. Sollten trotzdem Fragen offen geblieben sein, möchte ich Sie einladen, auf der Webseite zum Buch mit mir und anderen Anwendern in Kontakt zu treten:

Möglichst große
Schnittmenge

<http://psi2.de/Risikomanagement-das-Buch>
(Webseite mit Anwenderforum zum Buch)¹



Ich wünsche Ihnen viel Spaß beim Lesen und viel Erfolg bei der Anwendung in der Praxis.

Sebastian Klipper

Oktober 2010

¹ Zur Bedeutung des grafischen Codes rechts neben dem Hinweis auf die Webseite zum Buch beachten Sie bitte Erklärung zu QR-Codes auf Seite 9.

Inhaltsverzeichnis

1	Einführung	1
1.1	Wie wir uns entscheiden	1
1.2	ISMS – Managementsysteme für Informationssicherheit	3
1.3	Schritt für Schritt	6
1.4	Hinweise zum Buch	8
2	Grundlagen	13
2.1	Sprachgebrauch, Begriffe und Besonderheiten der Übersetzung	14
2.1.1	Begriffe aus ISO/IEC 27001	16
2.1.2	Begriffe aus ISO/IEC 27002	18
2.1.3	Begriffe aus ISO/IEC 27005	19
2.1.4	Übersicht der explizit definierten Begriffe	21
2.2	Entscheidend ist die Methodik	23

2.3	Der Ansatz der ISO	25
2.3.1	Die Entwicklung der ISO-Standards	26
2.3.2	Der PDCA-Zyklus	29
2.4	Die ISO 31000 Familie	31
2.4.1	Risikomanagement mit ISO 31000	31
2.4.2	Von der Theorie zur Praxis: ISO/IEC 31010	35
2.5	Die ISO/IEC 27000 Familie	39
2.5.1	Familienübersicht	39
2.5.2	Weitere Security-Standards	43
2.6	Abgrenzung zum BSI IT-Grundschutz	43
2.7	Was ist Risikomanagement?	46
2.7.1	Typische Bedrohungen der Informationssicherheit	47
2.7.2	Typische Schwachstellen der Informationssicherheit	50
2.7.3	Ursache und Wirkung	51
2.7.4	SANS Risikoliste	53
2.8	ExAmpLe AG - Die Firma für die Fallbeispiele	55
2.9	Die ISO/IEC 27000 Familie in kleinen Organisationen	59
2.10	Zusammenfassung	60
3	ISO/IEC 27005	63
3.1	Überblick über den Risikomanagement-Prozess	64
3.2	Festlegung des Kontexts	66
3.3	Risiko-Assessment	70
3.3.1	Risikoidentifikation	72
3.3.2	Risikoabschätzung	76
3.3.3	Risikobewertung/ Priorisierung	78
3.4	Risikobehandlung	81
3.5	Risikoakzeptanz	89
3.6	Risikokommunikation	90

3.7	Risikoüberwachung/ -überprüfung.....	93
3.8	Zusammenfassung.....	96
4	ISO 27005 und BSI IT-Grundschutz.....	99
4.1	Die Vorgehensweise nach IT-Grundschutz.....	100
4.2	BSI-Standard 100-3.....	102
4.3	Die IT-Grundschutz-Kataloge.....	105
4.4	Zusammenfassung.....	107
5	Risiko-Assessment.....	109
5.1	Methodensteckbriefe.....	110
5.2	Merkmale.....	111
5.3	Gruppierungen.....	112
5.4	Brainstorming.....	114
5.5	Strukturierte und semistrukturierte Interviews.....	116
5.6	Die Delphi-Methode.....	118
5.7	Checklisten.....	120
5.8	Vorläufige Sicherheitsanalyse (Preliminary Hazard Analysis PHA).....	122
5.9	HAZOP-Studie (HAZard and OPerability).....	124
5.10	HACCP-Konzept (Hazard Analysis and Critical Control Points).....	128
5.11	SWIFT-Technik (Structured "What if").....	130
5.12	Szenario-Analysen.....	132
5.13	Business Impact Analysen (BIA).....	134
5.14	Ursachenanalyse (Root Cause Analysis RCA).....	136
5.15	Auswirkungsanalysen (FMEA und FMECA).....	138
5.16	Fehler- und Ereignisbaumanalyse (FTA und ETA).....	140
5.17	Ursache-Wirkungsanalysen.....	142
5.18	Bow Tie Methode.....	144
5.19	Zuverlässigkeitsanalyse (Human Reliability Assessment HRA).....	146

5.20	Risikoindizes.....	148
5.21	Auswirkungs-Wahrscheinlichkeits-Matrix	150
5.22	Entscheidungsmatrizen.....	152
5.23	Zusammenfassung.....	154
6	Risikokommunikation	155
6.1	Theoretische Grundlagen.....	156
6.2	Das besondere an Risiken	161
6.3	Konfliktpotential	163
6.4	Kommunikationsmatrix	165
6.5	Zusammenfassung.....	169
7	Wirtschaftlichkeitsbetrachtung	171
7.1	Pacta sunt servanda	173
7.2	Wirtschaftlichkeitsprinzipien	174
7.3	Kosten-Nutzen-Analysen.....	176
7.4	Pareto-Prinzip.....	177
7.5	Total Cost/ Benefit of Ownership (TCO/ TBO)	179
7.6	Return on Security Investment (ROSI).....	182
7.7	Stochastischer ROSI	183
7.8	Return on Information Security Invest (ROISI)	186
7.9	Zusammenfassung.....	189
8	Die 10 wichtigsten Tipps	191
8.1	Hören Sie aufmerksam zu.....	192
8.2	Achten Sie auf die Usability.....	192
8.3	Reden Sie nicht nur von Risiken	192
8.4	Denken Sie wirtschaftlich	193
8.5	Der Weg ist das Ziel.....	193
8.6	Schauen Sie über den Tellerrand	194
8.7	Übernehmen Sie Verantwortung	194
8.8	Geben Sie Verantwortung ab.....	194

8.9	Der Empfänger macht die Nachricht	195
8.10	Verbeißen Sie sich nicht ;-)).....	195
Interessante Tools und Frameworks		197
Steckbriefe		198
Übersicht		199
Security Risk Management Guide (SRMG)		200
Security Assessment Tool (MSAT)		202
Common Vulnerability Scoring System (CVSS)		204
Risk Management Framework chaRMe.....		206
Weitere Tools		208
Secricon Risk Management Software.....		208
Lumension Risk Manager		209
Proteus		209
Modulo Risk Manager (NG)		210
STEAM.....		210
risk2value		211
BPSResolver ERM.....		211
Risk Watch.....		212
Risk Management Studio		212
RA2 Art of Risk.....		213
OCTAVE.....		213
Zusammenfassung.....		214
Sachwortverzeichnis		215
Abkürzungsverzeichnis		223
Literaturverzeichnis		227
GNU General Public License		231