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.

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

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

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier
Printed in Germany

ISBN 978-3-8348-1360-2

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

Motivation

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.

Welche Norm ist die passende?

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

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-Klaviatur 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.

Eingetretene Pfade verlassen

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-Grundschutzprojekt einsetzen kann, in dem eine erweiterte Risikoanalyse notwendig ist.

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.

Möglichst große Schnittmenge

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:

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.

Inhalt

Inhaltsverzeichnis