Vorwort

„Nichts geschieht ohne Risiko, aber ohne Risiko geschieht auch nichts."
-- Walter Scheel

Motivation

Die Geschichte dieses Buchs begann vor etwa fünf Jahren, 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!*
> *Oder noch besser:*
> *Menschliches Handeln und Unterlassen 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 in der Praxis kaum aus, um vor einer Bruchlandung bewahrt zu werden. Mit jedem Beteiligten wachsen die unterschiedlichen Interessen und damit auch die unterschiedlichen Sichtweisen auf die Risiken. Mit jeder Kommunikation leitet man eine Quasi-Evaluierung der kommunizierten Risiken ein und bringt den mühsam etablierten Risikomanagementprozess wieder ein wenig ins Wanken.

Unsicherheit

Selbst hervorragend analysierte Risiken sind nicht unerheblich von geschätzten Größen abhängig. Potentielle Schadenshöhen oder Eintrittswahrscheinlichkeiten stehen nicht in irgend einer international anerkannten Tabelle, aus der man nur abzulesen bräuchte. Es handelt sich hierbei um interne oder externe Schätzgrößen oder Erfahrungen der Vergangenheit, zu deren Festlegung man unterschiedlichster Meinung sein kann.

Eingetretene Pfade verlassen

Das Buch wird regelmäßig versuchen die durch die Standards eingetretenen Pfade zu 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.

Fragen über Fragen

Im Grunde ging es bei der Arbeit an diesem Buch darum, die Fragen zu beantworten, die sich mir selbst bei meinen Projekten als Security-Consultant gestellt hatten. Ich hatte bereits erwähnt, dass ich das Buch ursprünglich kaufen und nicht selbst schreiben wollte. Ergänzt wurden meine Fragen durch weitere, die sich in zahlreichen Gesprächen ergeben haben, die ich während der Recherche zu diesem Buch 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, direkt mit mir Kontakt aufzunehmen. Eventuell habe ich einen Tipp, der in diesem Buch noch nicht berücksichtigt wurde, oder ich kann Ihnen auf anderem Weg weiterhelfen. Besuchen Sie doch einfach meine Webseite:

http://psi2.de
(Webseite des Autors)[1]

2. Auflage kompakter im Inhalt

Die Neuauflage dieses Buches wurde deutlich verschlankt. Viele der bisherigen Inhalte, wie z.B. die Softwaretipps waren recht schnell veraltet und haben mit der Zeit ihren Wert verloren. Aber auch einige der prozessualen Bestandteile haben das Thema weiter ausgedehnt, als es in der Praxis erforderlich ist. Diese Abschnitte wurden meist entfernt oder entsprechend gekürzt und überarbeitet, was das Buch um einiges kompakter und damit nicht zuletzt für Sie kostengünstiger gemacht hat.

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

Sebastian Klipper
Januar 2015

[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.

http://www.springer.com/978-3-658-08773-9

Information Security Risk Management
Risikomanagement mit ISO/IEC 27001, 27005 und 31010
Klipper, S.
2015, XIV, 198 S. 28 Abb., Softcover
ISBN: 978-3-658-08773-9