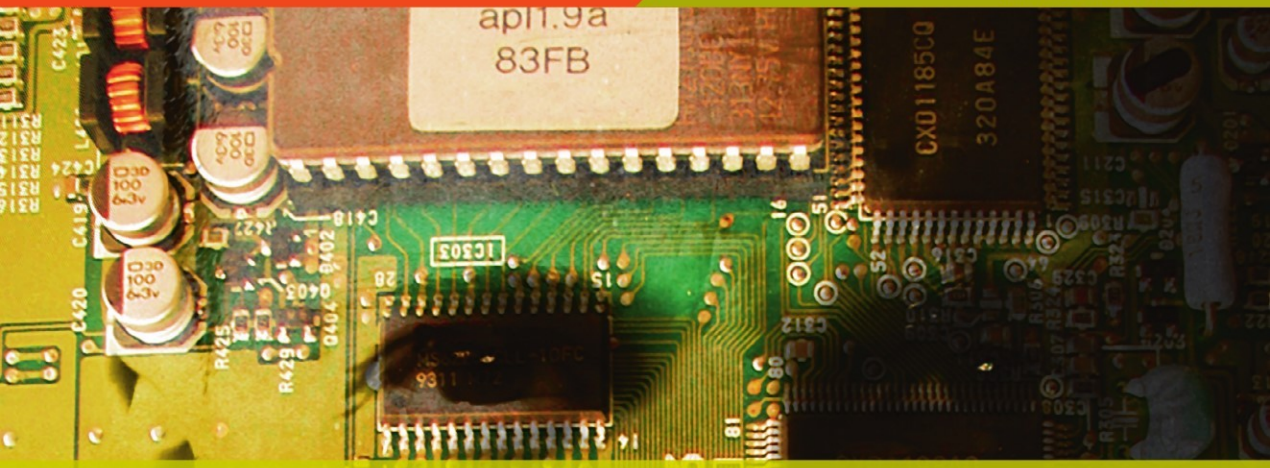
Sebastian Klipper

Information Security Risk Management

Risikomanagement mit ISO/IEC 27001, 27005 und 31010

PRAXIS



VIEWEG+ TEUBNER

‹kes›

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

1. Kapitel

1 Einführung

"Es ist unmöglich, ein unnötiges Risiko einzugehen. Denn ob das Risiko unnötig war, findet man erst heraus, wenn man es längst eingegangen ist."
Giovanni Agnelli

1.1 Wie wir uns entscheiden

Sie halten das Buch *„Information Security Risk Management mit ISO/IEC 27005"* in den Händen und stehen möglicherweise vor der Frage: *„Direkt kaufen, erst mal ein wenig durchblättern oder sofort wieder weg legen?"* Für manchen Zeitgenossen ist diese Frage der einzige Grund weiterhin in Buchhandlungen zu gehen, statt in Online-Shops einzukaufen: Es geht darum, erst einmal ins Buch zu schauen, es einer ersten Vor-Ort-Prüfung zu unterziehen und erst dann zu entscheiden, ob sich der Kauf wohl lohnen könnte. Letztlich geht es darum, das Risiko zu verringern, mit dem Kauf vollständigen Schiffbruch zu erleiden.

S. Klipper, *Information Security Risk Management,* DOI 10.1007/978-3-8348-9870-8_1,

„drive-by"-Risikoanalyse

In meinem Buch „Konfliktmanagement für Sicherheitsprofis" [1] habe ich diese Art von Schnellprüfung *„drive-by"*-Risikoanalyse genannt. Die Frage, wie wir Menschen Risikoentscheidungen treffen, ist nämlich wirklich spannend. Warum gibt es Menschen, die auf der einen Seite Brücken über hunderte Meter tiefe Schluchten bauen und sich auf der anderen Seite mit einer halb in Russisch geschriebenen Phishing-Mail die Zugangsdaten zu ihrer Bank stehlen lassen? Warum sind Menschen gleichzeitig so schlau und doch so dumm? Das liegt daran, dass wir uns bei unseren Entscheidungen auf zwei Systeme des Denkens stützen: ein automatisches und ein reflektierendes [2].

Automatisches System

Das automatische System kommt z.B. zum Zuge, wenn Menschen sich jeden Tag durch einen Berg von E-Mails klicken. Hier kann es schnell passieren, dass das automatische System die Oberhand gewinnt. Das Logo der eigenen Bank und deren Corporate Design legen den Risiko-Schalter um und schon werden die Zeilen mit dem russischen Akzent vom automatischen System ins Unterbewusste verbannt. Ohne Scheu kramen jeden Tag tausende Menschen, wie schon hunderte Male zuvor, die Zettel mit den PINs und TANs heraus und geben drei davon in das Eingabefeld einer dubiosen Web-Seite ein. Auf diese Weise klickt das automatische System die Menschen Tag für Tag durch die E-Mail-Fluten.

Bauchgefühl

Würden die Opfer die Gefahr erkennen, würde das reflektierende System sie dazu veranlassen, die Phishing-Mail genau zu prüfen und ihnen würden die Rechtschreibfehler auffallen. Sie würden merken, dass in der Adresszeile des Browserfensters nicht die Adresse der Bank steht, sondern eine ganz andere und sie würden merken, dass die Seite auch kein Sicherheitszertifikat zur Verfügung stellt. Viele zu viele Menschen verlassen sich auf ihr Bauchgefühl und das automatische System übernimmt die Entscheidungen. Bei einer Umfrage, die ich 2009 in der Zeitschrift <kes> veröffentlicht habe [3], hatten immerhin 36% der befragten IT-Sicherheitsfachleute gesagt, dass Sie sich bei der Planung ihrer IT-Sicherheitsprojekte auf ihr Bauchgefühl verlassen. Die *„drive-by"*-Risikoanalysen spielen also nicht nur bei der individuellen Entscheidungsfindung eine Rolle, sondern auch im Security Management.

Gerade wenn es um Sicherheit geht, sollte man sich jedoch nicht auf das Bauchgefühl verlassen. Die Komplexität heutiger Informationssysteme ist ohnehin schwer verdaulich. Das damit verbunde-

ne Bauchgefühl muss also zwangsläufig unangenehm sein und es verursacht schon seit vielen Jahren den Ruf nach Unterstützung bei der schwierigen Aufgabe des Managements von Informationssicherheit. In komplexen Informationssystemen, wie wir sie heute kennen, lässt sich die Flut an Informationen unmöglich mit dem fehlerbehafteten automatischen System abarbeiten.

Reflektierendes System

Das reflektierende System hingegen tritt in Erscheinung, wenn sich ein Mensch schwierigen Entscheidungen stellt. Diese Entscheidung trifft er bewusst und kontrolliert.

Auf dem Weg zu einer Zertifizierung nach ISO/IEC 27001 [4] muss jedes Unternehmen ein Risikomanagementsystem einführen. Auf welchen Standard man sich abstützt, und welchen Anforderungen er genügen muss, ist dabei nicht festgelegt und hängt nicht zuletzt von den Wünschen des Unternehmens oder der Behörde und der Person des Auditors ab.

Zu einem solchen Risikomanagementsystem gehört es, Risiken festzustellen und dann festzulegen, wie mit ihnen umgegangen werden soll. Nicht zuletzt geht es darum, eine leistungsfähige Risikokommunikation zu etablieren. Während sich ISO 27001 nur am Rande mit dieser für die ISO-Zertifizierung wichtigen Frage auseinandersetzt, ist ISO/IEC 27005 [5] genau dafür ausgelegt. Dieses Buch erläutert den Standard, ordnet ihn in die ISO/IEC 27000 [6] Familie ein und gibt Ihnen Tools und Frameworks an die Hand, mit denen Sie ein Risikomanagementsystem aufbauen können.

1.2 ISMS – Managementsysteme für Informationssicherheit

ISMS

Bevor man jedoch mit dem Management von Risiken für die Informationssicherheit beginnen kann, müssen gewisse Voraussetzungen geschaffen werden. Information Security Risk Management besteht also nicht losgelöst von anderen Sicherheitsbemühungen. Im Gegenteil: es ist integraler Bestandteil eines Managementsystems für Informationssicherheit (ISMS) und nicht etwa eine beliebige Erweiterung.

Auswahl von Maßnahmen

Die Auswahl von Sicherheitsmaßnahmen basiert in einem ISMS auf Entscheidungen, die auf Grundlage von Kriterien zur Risikobehandlung oder gar zur Risikoakzeptanz getroffen werden. Wie sie zustande kommen, damit befasst sich das Risikomanage-

ment. Nicht zuletzt spielen dabei nationale und internationale Gesetze eine Rolle, was üblicherweise unter dem Begriff Compliance zusammengefasst wird.

Risikomanagementprozess

An dieser Stelle wollen wir einen ersten Blick auf eine Grafik werfen, die uns im Verlauf des Buches noch einige Male begegnen wird. Sie ist noch nicht vollständig, aber wir werden sie im Laufe des Buchs mit Inhalt füllen:

Abbildung 1: Der erste Grundriss des Risikomanagementprozesses (nach [5])

Black-Box Risikomanagement

Es ist wichtig zu erkennen, dass die zwei ersten Felder, die in der Grafik zum Risikomanagementprozess gefüllt wurden, ganz unten stehen. Die Felder Risikobehandlung und Risikoakzeptanz sind die entscheidenden Schnittstellen zum ISMS, mit dem der Risikomanagementprozess in Verbindung steht. Die weiteren Felder bilden

für das ISMS quasi eine Black-Box, denn Risiken werden immer irgendwie behandelt oder akzeptiert. Wie diese Entscheidung zustande kommt variiert unter Umständen beträchtlich. Wenn Sie allerdings nicht auf soliden Füßen steht, ist die Wirksamkeit des ganzen ISMS in Frage gestellt.

Daher gehört Risikomanagement auch zu jedem ISMS. Die Standards ISO/IEC 27001 und 27002 sind jedoch recht zurückhaltend, wenn es darum geht zu klären, wie Risikomanagement aussehen soll. ISO/IEC 27005 ist daher in gewisser Weise der Inhalt für die Black-Box. Führen Sie sich jedoch vor Augen, dass Risikomanagement nicht etwa ein kleines Add-On ist, sondern eine beachtliche Aufgabe. Allein der Blick auf die Seitenzahl der Standards macht diesen Trend deutlich:

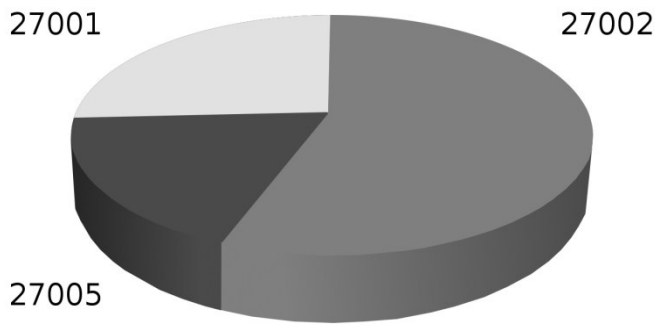


Abbildung 2: Gewichtung der Standards anhand ihrer Seitenzahl

Nun ist es natürlich nicht statthaft, die Wichtigkeit eines Standards beziehungsweise den Aufwand bei dessen Umsetzung anhand der Seitenzahl zu bestimmen. Sie sollten jedoch bedenken, dass Sie sich etwas Eigenes einfallen lassen müssen, wenn Sie sich dagegen entscheiden, die Risikomanagement-Black-Box mit ISO 27005 zu füllen.

Hand in Hand

Am Ende kann es eigentlich nur einen Schluss geben: Wer ein ISMS etabliert, kommt nicht mit ISO/IEC 27001 aus und wird daher auf den Code of Practice aus ISO/IEC 27002 zurückgreifen. Und wer den Code of Practice einsetzt muss sich etwas zum Risikomanagement einfallen lassen. Was liegt da näher, als den passenden Standard aus der ISO/IEC 27000 Familie zu verwenden. Dabei können die Standards jeweils nur schwer voneinander losgelöst betrachtet werden.

ISO/IEC 27003 und 27004

Wenn Sie jetzt nach den dazwischenliegenden Nummern 27003 und 27004 fragen, stellen Sie keine ganz unberechtigte Frage. Die

Standards befassen sich mit Implementierung und Design eines ISMS beziehungsweise mit dessen Bewertung. Das sind natürlich durchaus wichtige Themen, wenn es um ein ISMS geht. Sie bilden jedoch beide kein neues Stück vom Kuchen, sondern eher Zuckerguss und Sahne. Beides natürlich auch wichtig, aber nicht unverzichtbar. Sie sollten nicht vergessen, dass es für den ISO/IEC 27000 Kuchen noch jede Menge Schokoraspel, Candy und Marzipan-Figürchen gibt:

https://psi2.de/RM-Liste-des-SC27
(Liste der Security-Standards des ISO/IEC Subcommittee 27)[2]

1.3 Schritt für Schritt

Lassen Sie uns nun einen Blick darauf werfen, was Sie in diesem Buch inhaltlich erwartet. Wenn Sie bereits einige Erfahrung mit der ISO/IEC 27000 Familie haben, finden Sie hier eine Orientierung, welche Abschnitte für Sie besonders interessant sind und wo Sie welchen Stoff schneller finden können.

Kapitel 1

Das erste Kapitel (Sie vermuten richtig: das ist das Kapitel, das Sie gerade lesen) soll Ihnen helfen, sich zum Thema Risikomanagement zu orientieren und einen gedanklichen **Einstieg** zu finden. Darüber hinaus enthält es im Abschnitt 1.4 einige technische Hinweise und Tipps, wie Sie mit dem Buch am effektivsten arbeiten können, ohne viel Zeit mit Blättern zu verbringen.

Kapitel 2

Im zweiten Kapitel sollen die **Grundlagen** vermittelt werden, die benötigt werden, um mit der ISO/IEC 27000 Familie arbeiten zu können. Dafür müssen wir uns zunächst auf die verwendeten Begriffe einigen und die Standards in einen Zusammenhang setzen. Um das zu erreichen ist es unumgänglich, sich damit auseinanderzusetzen, wie ISO-Standards entstehen, und wie sie aufeinander aufbauen. Am Ende dieses Grundlagenkapitels sollten Sie auf dem ISO-Terrain ein gewisses Maß an Trittsicherheit

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

gesammelt haben. Es sollte klar sein, dass ISO/IEC 27005 nicht im luftleeren Raum schwebt, sondern großflächige Schnittstellen mit der ISO/IEC 27000 Familie und den Standards der 31000er Reihe hat. Am Ende des Kapitels stehen die ersten kleineren Fallbeispiele, die den Praxisbezug herstellen.

Kapitel 3

Bezogen auf den Titel des Buches ist Kapitel 3 das Herzkreislaufsystem des Risikomanagements. Der **Risikomanagementprozess** hält die Aktivitäten in gelenkten Bahnen und sorgt für eine gleichmäßige Verteilung von Informationen. Die Bruchstücke dieses Prozesses werden wir bereits in den ersten beiden Kapiteln zusammentragen und sie danach zu einem vollwertigen Gesamtkonzept zusammenfügen. Die nachfolgenden Kapitel bauen darauf auf und ergänzen dieses Herzkreislaufsystem um wichtige Organe und Körperteile. Denn das, was Sie in Ihrem Unternehmen oder Ihrer Behörde zu einem funktionierenden System führt, ist in ISO/IEC 27005 allein nicht enthalten.

Kapitel 4

Die Verwendung von ISO/IEC 27005 im **BSI IT-Grundschutz** ist eine Möglichkeit, die Grundschutz Vorgehensweise zu ergänzen. Hier können aber beide Welten voneinander lernen und sich gegenseitig ergänzen. Insbesondere die Grundschutzkataloge sind ein wertvoller Ideenpool, auf den es sich lohnt, einen genaueren Blick zu werfen, was wir in diesem Kapitel auch tun werden.

Kapitel 5

Kapitel 5 befasst sich mit den Inhalten des Standards **ISO/IEC 31010** und gibt Ihnen für eine Auswahl der dort vorgestellten Methoden jeweils einen Steckbrief an die Hand, der Ihnen die Auswahl der für Sie passenden Methode erleichtern soll. Hier gibt es kein falsch oder richtig. Eine Assessment-Methode, die in einen Unternehmen ein voller Erfolg war, kann im anderen Unternehmen in einem Fiasko enden. Die Chance, dass Sie sich für die richtige Methode entscheiden, steigt mit jeder Methode, die Sie kennen.

Kapitel 6

Ein oft vernachlässigtes Thema ist die **Risikokommunikation**. Man kann fast den gesamten Risikomanagementprozess im stillen Kämmerlein durchziehen, ohne darüber mit jemandem zu sprechen. So kommt man schnell zu Ergebnissen, deren Wert aber anzuzweifeln ist und sich sicher kaum an der Realität messen lassen kann. Wäre es anders müsste man Managementsysteme für Informationssicherheit nicht vor Ort auditieren. Eine Dokumentenprüfung würde dann völlig ausreichen. Wir wissen, dass das nicht so ist. Im Gegenteil können die Abweichungen zwischen der

Theorie der Konzepte und der Realität vor Ort erheblich sein. Will man diese Lücke verkleinern muss man in die Rolle des Verkäufers schlüpfen, und lernen, sich und das Produkt Risikomanagement besser zu verkaufen. Kapitel 6 setzt sich daher von der menschlichen Seite mit dem Thema Risikokommunikation auseinander und verzichtet bewusst auf eine weitere Verkomplizierung des Status quo.

Kapitel 7

Das Thema, das in Kapitel 7 beschrieben wird, ist eines der am schlechtesten erforschten im Security-Umfeld. Welche Kosten verursachen **Sicherheitsinvestitionen** und welchen Nutzen bringen sie. Statistische Daten gibt es wenig und wenn, dann beziehen sie sich naturgemäß auf die Vergangenheit – in einem Umfeld, in dem sich Angriffsvarianten, Schwachstellen und Möglichkeiten von Verteidigern und Angreifern rasend schnell verändern ist das keine gute Basis für eine aussagekräftige Entscheidungsgrundlage.

Was hilft es, Ende des Jahres 2010 zu wissen, wie hoch der Schaden durch Botnets im Jahre 2009 war, wenn man einen Return on Security Invest (ROSI) für die nächsten drei Jahre berechnen will. Wer weiß, ob Botnets in drei Jahren überhaupt noch eine Rolle spielen?

Kapitel 8

In diesem Kapitel werfen wir einen Blick auf einige Software-**Tools**, die den Risikomanagement-Prozess erleichtern sollen. Dabei soll der Blick für die Möglichkeiten der Softwareunterstützung geöffnet werden. Ein abschließender Überblick ist weder sinnvoll noch möglich. Kapitel 8 wird daher nur einige Produkte exemplarisch herausgreifen und sie ähnlich wie in Kapitel 5 als Steckbrief mit den wichtigsten Eckdaten vorstellen.

Kapitel 9

Am Ende des Buchs stehen schließlich **die 10 wichtigsten Tipps** zum Management von Informationssicherheitsrisiken. Sie bilden den Extrakt der bis dahin behandelten Themen und gehen dabei über die rein fachliche Ebene hinaus. Auch wenn sich Standards und Methoden über die Jahre ändern, einige Punkte sind gleich geblieben, seit sich Menschen in den unterschiedlichsten Kulturen mit Risiken auseinandersetzen müssen.

1.4 Hinweise zum Buch

Notizen, Notizen!

Die meisten von uns haben in der Schule gelernt, nichts in Bücher zu schreiben. Das halte ich für einen großen Fehler. Wahrschein-

lich könnte man den Notenschnitt an deutschen Schulen deutlich heben, wenn Schüler in ihre Bücher schreiben dürften. Ich möchte Sie daher einladen, sich im Buch Notizen zu machen. Sie werden das Buch dann wahrscheinlich nicht mehr gebraucht verkaufen können, aber Sie erhöhen den Wert für sich dadurch um ein Vielfaches.

Lesen Sie dieses Buch am besten immer mit einem Stift in der Hand. Streichen Sie an, was immer Ihnen gefällt, und streichen Sie durch, was für Ihre konkrete Situation uninteressant ist. Wenn die Stelle in einem Jahr für Sie wichtig wird, werden Sie sie schnell wiederfinden. Streichen Sie nicht nur an und durch; kommentieren Sie und nummerieren Sie sich Denkschritte am Rand mit. So werden auch eher theoretische Abschnitte zum ganz praktischen Arbeitsabschnitt. Welchen Vorteil sollte man sonst haben, ein Buch zu kaufen? Nutzen Sie diese Möglichkeiten.

Stichworte

Am Rand des Buchs finden Sie regelmäßig Stichworte, die es Ihnen erleichtern sollen, wichtige Stellen wiederzufinden und das Buch als Nachschlagewerk zu nutzen. So können Sie die Kapitel nach den Stichworten am Rand überfliegen. Wichtige Stichworte, die als Wegweiser am Rand auftauchen, können Sie auch über das Stichwortverzeichnis nachschlagen. So finden Sie schnell, wonach Sie suchen.

Icons

Zusätzlich zu den Stichworten werden Icons verwendet, um auf besondere Dinge hinzuweisen. Eines dieser Icons haben Sie bereits auf der ersten Seite dieses Kapitels kennen gelernt. Die Sprechblase verweist auf ein Zitat einer bestimmten Person. Neben der Orientierungshilfe durch die Icons sind diese Hinweise auch immer vom sonstigen Text freigestellt und grau hinterlegt. Im Folgenden sehen Sie die verwendeten Icons und die zugehörige Bedeutung:

http://psi2.de/Risikomanagement-das-Buch
(Hinweis auf eine Webseite)

Zitat oder Hinweis auf einen Standard, ein Buch o.Ä.

Beachten Sie, dass die Original-Zitate aus den Standards in Englisch verfasst sind. In diesem Buch wurden sie durch den Autor selbst ins Deutsche übertragen. Diese Übersetzungen dienen ausschließlich der besseren Lesbarkeit dieses Buchs und ersetzen keinesfalls den Original-Text. Insbesondere können Übersetzungsfehler – auch bei größter Sorgfalt – nicht ganz ausgeschlossen werden. Das Problem der richtigen Übersetzung ist nämlich nicht nur ein rein theoretisches, sondern von ganz praktischer Bedeutung. Daher widmet sich das Buch in einem eigenen Abschnitt dem Themenfeld *„Sprachgebrauch,* Begriffe und Besonderheiten der Übersetzung*"*.

Quellenangaben

Das Buch enthält zahlreiche Quellenangaben und Literaturhinweise. Sie erscheinen im Text in [eckigen Klammern] und verweisen auf das Literaturverzeichnis ab Seite 227.

Online-Quellen und QR-Codes

Bei Online-Quellen und Verweisen ins Internet wurde jeweils eine URL angegeben. Die Links des Buches verweisen so ausnahmslos auf die Domain der Webseite zum Buch, von wo aus direkt auf die entsprechende Internetadresse weitergeleitet wird. Dadurch können die Links des Buches nicht veralten und regelmäßig aktualisiert werden. Das ist insbesondere bei den zahlreichen Web-Tipps von Vorteil. Auch wenn das Buch nicht mehr ganz so neu ist, werden Sie so stets den neuesten Tipp zur Vertiefung des Themas im Internet bekommen.

Alle Links des Buchs können darüber hinaus auf der Webseite zum Buch oder mit einem QR-Code-Reader in Ihrem Smart-Phone als Linkliste aufgerufen werden:

https://psi2.de/RM-Liste-der-Links
(Linkliste auf der Webseite zum Buch)

Auf diese Weise habe ich versucht, das Papier-Medium Buch mit den Möglichkeiten des Internets zu verbinden. Die Leser dieses Buchs sind dafür also in gewisser Weise die *„Versuchskaninchen"* und ich würde mich sehr über Ihr Feedback freuen, ob der Versuch gelungen ist. Diese Rückmeldung ist mir besonders wichtig, da ich den Ansatz gerne weiterentwickeln möchte. Im Frühjahr 2011 wird dann ebenfalls im Vieweg+Teubner Verlag das Buch *„Soft-Skills für Freelancer"* erscheinen, das diese Linie noch konsequenter

verfolgen wird. Vielleicht sind dann ja sogar ein paar Ideen von Ihnen mit dabei.

Webseite zum Buch

Die Webseite zum Buch wurde mit einer Foren-Software erstellt und bietet daher die Möglichkeit, mit dem Autor, anderen Lesern und den sonstigen Nutzern des Portals in Verbindung zu treten. Sie wurde bereits vor dem Schreiben des Buchs erstellt und sollte bis zum Erscheinungstermin bereits eine Reihe zusätzlicher Informationen für Sie bereithalten. Die Webseite wurde so ausgelegt, dass Sie sie auch mit modernen Smartphones nutzen können.