

# Security Corner

[Zurück zur Übersicht](#)  
[Zum Portal](#)

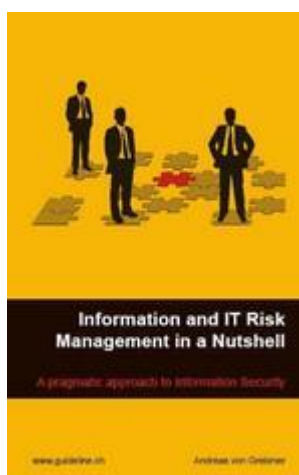
## Security Corner: Man sieht nur, was man weiß

### Buchbesprechung: „Stets pragmatische, nutzenorientierte Betrachtung für IT-Manager“

Von Peter Berlich (CISA, CISM, CISSP-ISSMP), Gründer Birchtree Consulting und Mitglied des ISC<sup>2</sup> Board of Directors

15. August 2008

Eine gute Darstellung des komplexen Themas Risikomanagement findet sich selten. Andreas von Grebmer hat in seinem Buch „Information and IT Risk Management in a Nutshell: A pragmatic approach to Information Security“ jedoch einen Weg gefunden, das Thema lesefreundlich aufzubereiten – und dies nicht mit detaillierten Darstellung der Theorie, sondern konsequent aus Praxissicht.



Nützliche Übersicht, geht aber aufgrund des knappen Umfangs nicht tiefer in

einzelne Themen  
ein: Das Buch  
Information and  
IT Risk  
Management in a  
Nutshell: A  
pragmatic  
approach to  
Information  
Security. Foto:  
Guideline

Ohne Zweifel ist Risikomanagement ein Thema, das nicht in drei Sätzen abgehandelt werden kann. Eine leserfreundliche und einfache Darstellung dieses Themas wird oft versprochen, aber selten gehalten. Die Komplexität – oder die scheinbare Einfachheit – des Themas scheint dem generell entgegen zu stehen, so dass anscheinend ausschließlich diejenigen, die mit dem Thema bereits vertraut sind, einen schnellen und einfachen Zugang finden.

Andreas von Grebmer hat in seinem Buch „Information and IT Risk Management in a Nutshell: A pragmatic approach to Information Security“ dennoch einen Weg gefunden, das Thema einer breiteren Leserschaft zugänglich zu machen. Der Autor versucht sich dabei nicht an einer detaillierten Darstellung der Theorie, sondern nähert sich dem Thema konsequent aus einem praxisorientierten Blickwinkel.

Der knapp 180 Seiten schmale Band ist in sieben Hauptabschnitte unterteilt, die durch ein umfangreiches Abkürzungs- und Begriffsverzeichnis, Verweise und eine Sammlung von gebrauchsfertigen Formularen ergänzt werden. Der erste Teil, gleichzeitig der ausführlichste, erklärt auf über sechzig Seiten die Grundlagen des IT-Risikomanagements. Darauf folgend werden die Ziele des IT-Risikomanagements aus Geschäftssicht erläutert, und die Verbindung zwischen Risikomanagement und Informationssicherheit aufgezeigt.

Der anschließende Teil beschäftigt sich mit dem Aufbau eines Sicherheitsprogramms und dem in diesem Zusammenhang bedeutende (und meist unterschätzte) Management von Zulieferern. Er beinhaltet daneben eine Sammlung von Faustregeln. Behandelt werden Themen wie Risikoarten, Risikostrategie, Rollendefinitionen, der Aufbau einer Organisation sowie Disaster Recovery, Projekt- und Change Management. Ein grundlegendes Verständnis der verwendeten Begriffe kann im Laufe der Lektüre erlangt werden, was den Band auch für Nicht-Experten geeignet macht.

Hervorzuheben ist die Konzentration auf das Wesentliche, aber auch die stets pragmatische, nutzenorientierte Betrachtung. Dem Leser wird eine schrittweise Anleitung an die Hand gegeben, anhand derer er die eigene Vorgehensweise

planen kann. Die zahlreichen Checklisten, Formulare und Pläne helfen dabei. Das Buch enthält darüber hinaus viele hilfreiche Grafiken und Tabellen, die in einem ausgewogenen Verhältnis eine Einheit mit dem Textteil bilden. Diese Darstellungsweise macht Abläufe und Zusammenhänge unmittelbar verständlich und kann auf das eigene Unternehmen zugeschnitten werden.

Trotz der vielen anschaulichen Beispiele sind angesichts des knappen Fließtextes Verständnislücken nicht immer ausgeschlossen. Eine summarische Beschreibung der verschiedenen Risk-Management-Methodologien wäre dem Thema angemessen gewesen. Dem Büchlein hätte ein genaueres Lektorat an einigen Stellen gut getan, was freilich dem Inhalt keinen Abbruch tut.

„Information and IT Risk Management in a Nutshell“ ist eine Handreichung, die sich vor allem an den Praktiker richtet, der eine übersichtliche Zusammenfassung sucht. Das Aufgreifen von unternehmenspraktischen Fragen, wie Stakeholder Management, Supplier Management oder allgemeine unternehmensinterne Politik, schafft unmittelbaren, praktischen Nutzen für den Leser.

Das Buch stellt dabei nicht den Anspruch, in sich abgeschlossen zu sein, was im Rahmen des gegebenen Umfangs auch nicht machbar gewesen wäre. „Man sieht nur, was man weiß“, ist die eindeutige Botschaft des Autors. Somit ist dieses Handbuch eine nützliche Hilfe für den IT-Manager, der sein Vorgehen zusammen mit Experten planen und koordinieren muss.

Als einführende Übersicht und praktisches Nachschlagewerk verdient „Information and IT Risk Management in a Nutshell“ einen Platz in Griffweite. Für eine tiefere Betrachtung der einzelnen Themen wird man sich dann der reichlich verfügbaren Spezialliteratur bedienen.

Der Autor, Andreas von Grebmer, ist Manager bei einem Schweizer Pharmaunternehmen und bereits mit Bänden zum Thema Projektmanagement („The project is dead... Long live the project“) und Qualitätssicherung („Der Software-Testprozess für IT-Manager“) hervorgetreten, die einen ähnlich pragmatischen und zielorientierten Fokus haben.

Buch: Andreas von Grebmer: Information and IT Risk Management in a Nutshell: A pragmatic approach to Information Security,  
<http://www.guideline.ch/>, ISBN 978-3-8334-9658-5 ; 179 Seiten; 24,90 Euro.

**Zurück zur Übersicht**