Vorwort zur zweiten Auflage

Seit der ersten Auflage sind etwa fünf Jahre vergangen. In der IT ist das eine sehr lange Zeit. Entsprechend viel ist passiert. Mittlerweile gilt es als allgemein akzeptiert, dass sich durch die damals bereits beginnende digitale Transformation alle Unternehmen, aber auch unser Alltag »deutlich« verändern. Es ist notwendig, diese Veränderungen exakter zu beschreiben und zu klassifizieren, um ihre tatsächlichen Auswirkungen besser verstehen zu können. Fragen der Informations-, IT- und nicht zuletzt speziell der Cybersicherheit rücken dabei angesichts unterschiedlichster Ereignisse im Kontext des IT-Einsatzes mehr und mehr ins Bewusstsein der Öffentlichkeit.

Entsprechend hat die Bedeutung des IT-Risikomanagements als ein wichtiges Werkzeug innerhalb eines unternehmensweiten Risikomanagements erheblich zugenommen. Mehr und mehr stellt sich heraus, dass die deutliche Zunahme der technischen Komplexität eingesetzter Lösungen und die damit verbundene steigende fachliche Komplexität in Planung und Betrieb dazu führt, dass eine intensive Diskussion grundsätzlicher Fragen in den Vordergrund tritt. IT-Risikomanagement muss, wie das Risikomanagement in anderen Bereichen auch, institutionalisiert und die Verantwortung dafür ganzheitlich auf Unternehmensleitungsebene gesehen werden. Die Verantwortung für Risiken wandert zunehmend »nach vorne« bzw. »nach oben«. Es ist heute nicht zuletzt vor dem Hintergrund von Compliance- und Haftungsfragen für die Unternehmensleitung entscheidend, hinsichtlich zentraler Prozesse im Internen Kontrollsystem sowie in Bezug auf Sicherheit, Risiko und Business Continuity die Weichen richtig zu stellen und dafür zu sorgen, dass im Falle von eintretenden Risiken »richtig« im Sinne der Compliance-Anforderungen reagiert wird. Geschieht dies nicht, steht schnell der Vorwurf des Organisationsversagens mit allen Konsequenzen im Raum.

Zahlreiche Gespräche, Beobachtungen und Projektbegleitungen in den letzten fünf Jahren zeigen, dass große, insbesondere kapitalmarktorientierte und publizitätspflichtige Unternehmen diese Fragen bereits

adressiert und vielfach (weitgehend) gelöst haben. Doch noch immer gibt es insbesondere im Mittelstand Lücken, deren Ursachen häufig in fehlender Personalkapazität und mangelnder Qualifikation liegen. Selbstverständlichkeiten aus dem IT-Risikomanagement sind dann nicht oder nur unvollständig umgesetzt. Sätze wie »Wer interessiert sich schon für uns« oder »Bei uns ist nichts zu holen« fallen immer noch. Gleichzeitig schließen mittelständische Unternehmen mit innovativen digitalen Lösungen zum internationalen Wettbewerb auf oder führen ihn sogar an. Der umfassende Einsatz neuester Informationstechnologie (die früher vielfach »den Großen« vorbehalten war) lässt dabei die Entwicklung für diese Unternehmen besonders gefährlich werden. Denn beispielsweise eine Beurteilung, ob aus neuartigen Angriffsformen, wie den sogenannten »RAMBleed-Attacken«, tatsächlich Risiken für das Unternehmen entstehen können (»Was hat das mit meiner Cloud-Lösung zu tun?«), erfordert Awareness und methodisches Vorgehen. Gleiches gilt ggf. für die zu ergreifenden Gegenmaßnahmen.

Die vorliegende zweite Auflage trägt diesem Umstand auf unterschiedliche Weise Rechnung. Zum einen sind einzelne Aspekte, etwa der Einsatz von Geräten für das Internet der Dinge, oder neue Paradigmen, wie DevOps, ergänzt, andere, wie etwa Normen und Standards, aktualisiert sowie Zusammenhänge in der Theorie präzisiert worden. Zum anderen sind neue Aspekte aufgenommen worden, die mit Blick auf kritische Infrastrukturen oder Fragen der IT-Strategie, IT-Governance und IT-Architektur eine bisher bestehende Lücke schließen.

Zielgruppe

Dieses Buch richtet sich an alle Neu- und Quereinsteiger in das Themengebiet sowie an Studierende, die sich mit der vielschichtigen und vielseitigen Materie näher befassen wollen oder im Rahmen von Veranstaltungen müssen.

Praxisbeispiele und Handlungsempfehlungen sollen eine Orientierung und Vorschläge für eigene Gedanken ermöglichen. Naturgemäß können solche allgemein gehaltenen Hinweise niemals so speziell sein, dass erfahrene Risikomanager sie als Vorbild (Blaupause) direkt nutzen könnten. Für ein solches Vorbild wäre meines Erachtens sowohl Kenntnis über die jeweilige Branche als auch – in besonderem Maße – möglichst detailliertes Wissen über die unternehmensinternen Prozesse und Rahmenbedingungen notwendig.

Dennoch hoffe ich, dass auch Experten von diesem Buch profitieren können – einerseits durch Übersichten zu den aktuellen Normen und Standards, andererseits durch Bündelung von Themen und Hinweisen auf weiterführende Informationsquellen. Ein Abgleich mit dem

eigenen Wissen ist auf diesem Weg ebenso möglich wie weiter gehende Überlegungen zum Einsatz von Methoden und Werkzeugen für das Risikomanagement anhand der im Buch enthaltenen Übersichten und Hinweise.

Das Buch berücksichtigt neben wissenschaftlichen Quellen auch Beiträge aus der Praxis. Es ist, wie der Titel sagt, praxisorientiert und will nicht den Anspruch einer forschungsorientierten, wissenschaftlichen Auseinandersetzung mit dem Thema erheben. Ziel ist es, dabei zu helfen, das Risikomanagement in der Praxis einzuführen, wo dies noch nicht geschehen ist, und dabei zu unterstützen, es zu verbessern, wo es bereits etabliert ist.

Dabei ist eine Trennung zwischen IT-Risikomanagement und IT-Sicherheit nicht immer einfach. Viele Fragen aus der IT- und speziell der Cybersicherheit haben große Schnittmengen mit dem IT-Risikomanagement. Auch wenn es verlockend ist und interessant wäre, auf Einzelheiten näher einzugehen, etwa bei den speziellen Risiken, aber auch bei den Maßnahmen zur Behandlung dieser Risiken, verzichtet der Text bewusst darauf, verweist jedoch an zahlreichen Stellen auf bestehende Schnittmengen, Normen, Standards und Informationsquellen.

Dank

Auch an der zweiten Auflage dieses Buches haben viele Hände mitgewirkt.

Besonders danken möchte ich meinem Kollegen Daniel Burda, der das Manuskript bereits vorab kritisch durchgesehen und zahlreiche wichtige Impulse zur Verbesserung eingebracht hat, und ebenso den Gutachtern, die viele weitere wertvolle Hinweise im Rahmen des sich anschließenden Reviewprozesses beigesteuert haben und so ebenfalls ihren Beitrag dazu geleistet haben, den Text weiter zu verbessern.

Mein Dank gilt auch meinem Kollegen Urs Andelfinger und Frau Nadin Ebel, die mich mit Informationen zu Standards versorgt und dadurch mitgeholfen haben, Sachverhalte zu präzisieren und Darstellungsfehler zu vermeiden. Irrtümer, die nun noch im Text zurückgeblieben sind, habe ich daher vollständig selbst zu verantworten.

Beim Lektorat und Copy Editing, insbesondere bei Christa Preisendanz und Ursula Zimpfer, sowie bei allen Mitarbeiterinnen und Mitarbeitern des dpunkt.verlags, die in den Herstellungsprozess eingebunden waren, möchte ich mich für die motivierende Betreuung und sehr geduldige Begleitung und die gewohnt höchste Qualität von Satz und Druck ganz herzlich bedanken. Es freut mich sehr, dass das Buch auch in zweiter Auflage im dpunkt.verlag erscheinen darf.

Ich hoffe, dass auch diese zweite Auflage viele interessante und vor allem neue Impulse für Ihre tägliche Arbeit enthält und natürlich wie bereits vor fünf Jahren, dass Sie darin Bewährtes bestätigt finden. Ich freue mich über Ihr Lob ebenso wie über Ihre Anregungen und Kritik, denn nichts ist perfekt und manches regt sicherlich zu Diskussionen an.

Matthias Knoll
Darmstadt im Juni 2019