ERICH
SCHMIDT
VERLAG

Cyber Security in der Risikoberichterstattung

Praxisleitfaden für optimiertes IT-Risikomanagement

Von

Dr. Carola Rinker

Mit Beiträgen von

Helmut Brechtken
Manuel Dinis
Dr. Dominique Hoffmann
Patrick Król
Chris Lichtenthäler
Dr. Carola Rinker
Thomas Zimmerer

ERICH SCHMIDT VERLAG

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.

Weitere Informationen zu diesem Titel finden Sie im Internet unter
http://ESV.info/978-3-503-19924-2

Zitiervorschlag:
Rinker, Carola (Hrsg.), Cyber Security in der Risikoberichterstattung

ISBN 978-3-503-19924-2 (gedrucktes Werk)
ISBN 978-3-503-19925-9 (eBook)

Druck: docupoint, Barleben

Vorwort der Herausgeberin

Auch wenn zu Beginn des neuen Jahrzehnts das Corona-Virus massive Auswirkungen auf die Konjunktur und die Unternehmen hatte: Die Risiken eines Hackerangriffs und anderer Cyber-Attacken auf Unternehmen gewinnen zunehmend an Bedeutung. Sie erinnern sich vielleicht an den Mai 2017: Damals legte ein Hackerangriff die Wirtschaft lahm. Ich war zu der Zeit mit dem Zug unterwegs. Anstelle der Informationen über die Abfahrten der Züge auf den Bildschirmen stand damals lediglich der Hinweis „Bitte Aushänge beachten".

Am Stuttgarter Bahnhof standen sogar von Hand geschriebene Aufsteller mit den Abfahrtszeiten der Züge. Ich fühle mich wie in Havanna, wo immer noch Fahrpläne von Hand an den Bahnhöfen hängen. Als sowohl an den Bahnhöfen in Karlsruhe und Freiburg die digitalen Anzeigen nur auf „Bitte Aushänge beachten" anzeigen, wird mir das Ausmaß etwas bewusster. Ich fühle mich wie in „You are wanted", einer Serie von Matthias Schweighöfer, in der die Geschichte eines Mannes erzählt wird, der gehackt wird. Der Film war also teilweise Wirklichkeit geworden.

Die Risiken unserer vernetzten und digitalisierten Welt liegen also bei Hackerangriffen und Daten. Daten – das sind die Vermögenswerte der Zukunft. Ein Hackerangriff könnte unsere ganze Wirtschaft lahmlegen. Wird darüber seitens der Unternehmen in den Geschäftsberichten ausreichend berichten? Wurde das Risiko als eher gering eingestuft? Waren die Kosten zu hoch? Wie kann es sein, dass große Unternehmen nicht regelmäßig ihre Programme updaten? Fragen über Fragen. Dieses Ereignis gab den Anlass für meine erste Studie zur Berichterstattung über Cyber-Risiken im DAX.

Meine Studie zu Cyber-Risiken fand regen Anklang. So wurde ich seitens des Erich Schmidt Verlags angefragt, daraus ein Praxis-Handbuch zu verfassen. Wie ich bereits nach einigen Recherchen und Gesprächen feststellte, ist dieser Themenkomplex sehr breit gefächert. So entstand die Idee, die Thematik in einem Sammelband zu veröffentlichen.

Mit Unterstützung des Erich Schmidt Verlags und meinem Netzwerk ist es mir gelungen, einige Experten für das Buchprojekt zu gewinnen. Im ersten Beitrag beleuchtet Manuel Dinis die Bedeutung eines IT-Risikomanagementsystems in der Praxis. Helmut Brechtken, Chris Lichtenthäler und Dr. Dominique Hoffmann beschäftigen sich in dem folgenden Beitrag sowohl mit den Auswirkungen als auch der Bedeutung von Cyber-Risiken in der externen Berichterstattung. Erläuterungen zur unternehmensübergreifende IT-Vernetzung finden sich im Beitrag von Thomas Zimmerer. Patrick Król stellt die Relevanz von Cyber Security Controls im Zuge der Risikoberichterstattung dar, bevor mein Beitrag den Sammelband mit einer empirischen Studie der Risikoberichterstattung von Cyber-Risiken börsennotierter Unternehmen abschließt.

Mein Dank gilt Wolfhart Fabarius für die gute Zusammenarbeit bei der Erstellung des Werkes. Ebenso möchte ich mich bei den Autoren bedanken, die stets offen für meine Vorschläge waren und mit Eifer die Beiträge verfassten.

Wir wünschen Ihnen viel Spaß bei der Lektüre.

Carola Rinker
Freiburg, April 2021

Inhaltsverzeichnis