

ESV 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)

Alle Rechte vorbehalten

© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021

www.ESV.info

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 berichtet? 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

Vorwort der Herausgeberin	5
I. Bedeutung eines IT-Risikomanagementsystems in der Praxis in Zeiten der digitalen Transformation	11
1. Einleitung	11
2. Forschungsstand	14
2.1 Risikomanagement	14
2.2 Cyber-Sicherheit	21
3. Theoretische Grundlagen	22
3.1 Vorstellung relevanter Normen, Gesetze und Verordnungen	22
3.2 Definition Risiko	28
3.3 Darstellung und Beschreibung einer Risikomatrix	31
3.4 Theoretischer Aufbau eines Risikomanagementsystems und das dazugehörige Modell	31
4. Praktische Umsetzung	44
4.1 Arbeitspaket 1: Kick-off-Strategie und Planung	46
4.2 Arbeitspaket 2: Geltungsbereich, ISMS-Organisation und Dokumentation	47
4.3 Arbeitspaket 3: Prozessoptimierung und Erhöhung des Reifegrads des ISMS	53
4.4 Arbeitspaket 4: Werteverzeichnis als Grundlage für die weitere Vorgehensweise	54
4.5 Arbeitspaket 5: Risikomanagement	55
4.6 Arbeitspaket 6: Ableitung der technischen und organisatorischen Maßnahmen	57
4.7 Arbeitspaket 7: Vorbereitung, Planung und Begleitung der ISMS Zertifizierung	59
4.8 Arbeitspaket 8: ISMS Regelbetrieb	59
5. Fazit und Ausblick	60
Literaturverzeichnis	63
II. Identifikation von Cyber-Risiken	67
1. Einführung Cyber-Crime und Cyber-Risiken	67
2. Bewertung und Beurteilung von Cyber-Risiken, Auswirkungen von Cyber-Vorfällen im Unternehmen	72
3. Behandlung von Cyber-Crime-Risiken durch Risiko-Management	76
Literaturverzeichnis	97
III. Unternehmensübergreifende IT-Vernetzung	101
1. Einleitung	101

2. Theoretische Grundlagen	102
2.1 Bezug IT-Risiken	102
2.2 Neue Situation durch unternehmensübergreifende Vernetzung (insbesondere durch IoT und Industrie 4.0)	103
2.3 Anwendungsfelder	104
2.4 Anwendungsbeispiele	106
2.5 Kooperationen mit anderen Unternehmen	108
3. Praktische Bewertung von Chancen und Risiken	110
3.1 Chancen durch unternehmensübergreifende und unterneh- mensinterne Vernetzung	110
3.2 Risiken durch unternehmensübergreifende und unterneh- mensinterne Vernetzung	111
3.3 Maßnahmen zur Minimierung der Risiken	112
3.4 Bewertungsansätze	114
4. Umsetzungsstrategien	116
5. Fazit und Ausblick	117
IV. Relevanz von Cyber Security Controls im Zuge der Risikobe- richterstattung	119
1. Einleitung	119
2. Bedeutung von Cyber Security	120
2.1 Grenzen zwischen IT-Security, Information Security und Cyber Security	120
2.2 Historische Entwicklung und heutige Bedeutung von Cyber Security	123
2.3 Herausforderung der rechtlichen und regulatorischen Anforderungen in der Cyber Security	126
2.4 Wirtschaftsprüfung 2.0	127
3. Einfluss- und Risikofaktoren einer modernen IT-Infrastruktur	128
3.1 Digitalisierung	128
3.2 Risikokultur & Security Awareness	130
3.3 Schatten-IT	131
3.4 Cloud Computing	133
4. Security Audits und Cyber Security Risk Assessments	134
4.1 Einsatz einer Risikomatrix zur Risikobewertung	136
4.2 Risikobeurteilung mit Hilfe von Cyber-Security-Ratings und Indizes	138
4.3 Exkurs: Datenschutzaudits	141
5. Einsatz von Cyber Security Controls	142
5.1 Was sind Cyber Security Controls?	142
5.2 Frameworks und Standards als nützliche Hilfsmittel	145
5.3 Entwicklung und Auswahl von Cyber Security Controls	149
6. Bedeutung und Nutzen von Auditberichten, Zertifikaten und Testaten im Cyber-Security-Umfeld	151
6.1 Auditberichte nach den Prüfungsstandard des IDW	151
6.2 System and Organization Controls Reporting	153

6.3 ISO 27001 Zertifizierung	154
6.4 BSI C5-Testat	154
6.5 Vorteile von Zertifizierungen	154
6.6 Kritische Betrachtung von Zertifizierungen	155
7. Aktuelle Situation und zukünftiger Ausblick auf rechtliche Entwicklungen im Cyber-Security-Bereich	157
7.1 IT-Sicherheitsgesetz	157
7.2 Europäische Datenschutz-Grundverordnung	158
7.3 EU Cybersecurity Act	161
7.4 EU NIS-Richtlinie	163
7.5 Verordnung zur Errichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung	164
7.6 Exkurs: Cyber-Security-Versicherungen	165
8. Empfehlungen zur Verbesserung der Cyber Security	166
8.1 Attack libraries	166
8.2 MITRE	167
8.3 Attack trees	168
8.4 ISIS12	168
8.5 BSI Basis-Sicherheitscheck	170
8.6 Angebot der Allianz für Cyber-Sicherheit vom BSI	171
8.7 Security Awareness (Employee Security Index)	173
8.8 Security Operations Center	175
9. Abschließende Betrachtung	176
Literaturverzeichnis	178
V. Darstellung der Cyber-Risiken im Lagebericht – praktische Umsetzung in den Geschäftsberichten des DAX, MDAX und SDAX	187
1. Einleitung	187
2. Theoretische Grundlagen	188
2.1 Definition Cyber-Risiken	188
2.2 Risikoberichterstattung im Lagebericht	190
3. Praktische Umsetzung in den Lageberichten	192
3.1 Stichprobe	192
3.2 Untersuchungsergebnisse	193
4. Fazit und Ausblick	212
Literaturverzeichnis	213
Geschäftsberichte 2019	214
Anhang 1: Unternehmensstichprobe	214
Anhang 2: Auszug aus den Risikoberichten	218
Autorenverzeichnis	223