

GUNDEL (Hrsg.)



Unternehmenssicherheit

Handbuch für Wirtschaft und Behörden

 | BOORBERG

Unternehmenssicherheit

Handbuch für Wirtschaft und Behörden

herausgegeben von
Dr. Stephan Gundel
Chefexperte Sicherheit,
Gruner AG, Basel

mit Beiträgen von
Heinz-Werner Aping
Dr. Claudia Brandkamp
Prof. Dr. Martin Grothe
Dr. Stephan Gundel
Prof. Oliver Hirschi
Richard Huber
Damian In-Albon
Thomas Jehmlich
Manfred Jilg
Lars Mülli
Dan Pruschy
Matthias Rössler
Prof. Dr. Meike Schröder
Silvester Siegmann
Patrick Sonntag
Kai Ullwer
Christian Willi
Wolfgang Zier

Bibliografische Information der Deutschen Nationalbibliothek |
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind
im Internet über www.dnb.de abrufbar.

Print-ISBN 978-3-415-07635-8

E-ISBN 978-3-415-07636-5

© 2024 Richard Boorberg Verlag

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt.
Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zu-
gelassen ist, bedarf der vorherigen Zustimmung des Verlages. Dies gilt
insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen,
Mikroverfilmungen und die Einspeicherung und Verarbeitung in
elektronischen Systemen.

Titelfoto: © Monster Ztudio – stock.adobe.com | Satz: abavo GmbH,
Nebelhornstraße 8, 86807 Buchloe | E-Book-Umsetzer: abavo GmbH,
Nebelhornstraße 8, 86807 Buchloe

Richard Boorberg Verlag GmbH & Co KG | Scharrstraße 2 | 70563 Stuttgart
Stuttgart | München | Hannover | Berlin | Weimar | Dresden
www.boorberg.de

Vorwort

Spätestens mit Beginn des russischen Angriffskriegs auf die Ukraine im Februar 2022 rückte das Thema „Sicherheit“ wieder mit aller Deutlichkeit ins breite Bewusstsein von Politik, Wirtschaft und Öffentlichkeit. Ähnlich wie die Terroranschläge des 11. September 2001 kann dieses Ereignis als Zäsur oder, um den mittlerweile in den gängigen Wortschatz eingegangenen Begriff aus der Regierungserklärung des deutschen Bundeskanzlers Olaf Scholz vom 27. Februar 2022 zu gebrauchen, sogar als „Zeitenwende“ aufgefasst werden.

Bereits etwa 20 Jahre zuvor hatte die mit einem Mal offensichtlich gewordene Gefahr islamistischen Terrors auch Auswirkungen auf die Unternehmenssicherheit. Das noch heute als Grundlagenwerk häufig zitierte Buch „Rethinking Corporate Security in the Post 9/11-Era“ des US-amerikanischen Beraters Dennis R. Dalton aus dem Jahr 2003 formulierte seinerzeit das Leitbild einer Unternehmenssicherheit als „business enabler“, die unternehmerische Tätigkeiten in einem zunehmend unübersichtlichen und gefährlichen Umfeld sicher ermöglicht. Daraus folgten in vielen Unternehmen der Auf- und Ausbau von Sicherheitsfunktionen, die Sicherheitsrisiken weltweit oder zumindest in den relevanten Regionen analysieren, bewerten und durch geeignete Maßnahmen minimieren sollen.

Mit dem steigenden Sicherheitsbedürfnis der Unternehmen gingen auch verschiedene Professionalisierungsbemühungen einher. Aus der Erkenntnis, dass für Erfolg und Akzeptanz der Unternehmenssicherheit eine solide akademische Ausbildung, die nationale bzw. internationale Vernetzung von Fachpersonen sowie belastbare Grundlagen notwendig sind, wurden unter anderem Studienangebote geschaffen, Verbände und Austauschgremien etabliert oder ausgebaut sowie verschiedenste Fachpublikationen veröffentlicht. Die „Corporate Security“ sollte dadurch zu einer anerkannten und gleichwertigen Funktion im oberen Management von Unternehmen werden, die selbstverständlich an Entscheidungen beteiligt wird sowie Einfluss und Ressourcenbedarf geltend machen kann.

Die Ergebnisse dieser Bemühungen können zum aktuellen Zeitpunkt als gemischt bezeichnet werden. Tatsächlich wird die Notwendigkeit von Sicherheitsfunktionen in Unternehmen heutzutage kaum mehr grundsätzlich in Abrede gestellt, ihre Wahrnehmung und Etablierung variiert aber immer noch. Gemäß dem „Corporate Security Survey 2022“ der Unternehmensberatung PwC waren zwar 80 % der 150 befragten Führungs-

kräfte bzw. Sicherheitsverantwortlichen tatsächlich der Ansicht, dass die Unternehmenssicherheit die Rolle des „business enablers“ erfülle, gleichzeitig wurde die Funktion aber nur durch etwa die Hälfte der Befragten als im Unternehmen etabliert eingeschätzt.¹ Hinsichtlich Aufgaben und Ausrichtung der Unternehmenssicherheit bestehen zudem teilweise deutliche Wahrnehmungsdifferenzen zwischen Führungskräften und Sicherheitsverantwortlichen in Unternehmen.² Auch nach der persönlichen Erfahrung des Herausgebers sind Einheiten der Konzern- oder Unternehmenssicherheit häufig Gegenstand wiederkehrender Diskussionen über grundsätzliche Ausrichtung, organisatorische Verankerung oder notwendige Ressourcen, die eine effektive Aufgabenerfüllung oftmals lähmen. Schließlich wird, auch im besagten „Corporate Security Survey 2022“, immer wieder der Mangel an ausreichend qualifiziertem Personal für Aufgaben der Unternehmenssicherheit als Entwicklungshindernis hervorgehoben.³

Das vorliegende Buch soll vor dem Hintergrund dieser Ausgangslage sowie der für Unternehmen im deutschsprachigen Raum absehbar immer herausfordernder werdenden Sicherheitslage eine zusätzliche und aktuelle Hilfestellung sein. Es richtet sich primär an Praktiker in Unternehmen, Behörden, Versicherungen und Verbänden, die mit Aufgaben im Umfeld der Unternehmenssicherheit betraut sind oder zumindest Berührungspunkte haben. Ergänzend soll es auch für Aus- und Weiterbildungszwecke dienlich sein, indem es einen umfassenden Überblick über die verschiedenen Bestandteile einer modernen Unternehmenssicherheit ermöglicht. Bereits 2009 hatte ich mit meinem damaligen Kollegen Lars Mülli im Oldenbourg-Verlag ein erstes Buch über Unternehmenssicherheit verfasst, welches einen – wenn auch teilweise recht rudimentären – grundlegenden Einstieg in das Thema ermöglichen sollte. Drei Jahre später durfte ich dann als Mitherausgeber für den Teil „Unternehmenssicherheit (Corporate Security)“ am „Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit“ des Richard Boorberg Verlags mitwirken, welches als sehr umfassendes Kompendium zu allen Fragen des Sicherheitsmanagements auf die Initiative von Prof. Dr. Dr. h. c. mult. Rolf Stober und Dr. Harald Olschok zurückging.

1 Vgl. PwC (2022): Corporate Security – Today’s Business Enabler. Corporate Security Benchmarking Survey 2022, S. 5.

2 Vgl. ebenda, S. 15.

3 Vgl. ebenda, S. 13.

Im Laufe des Jahres 2023 übertrug mir der Richard Boorberg Verlag schließlich die Aufgabe, ein neues Werk mit ausschließlichen Fokus auf die Kernthemen der Unternehmenssicherheit zu konzipieren und herauszugeben. Für das damit verbundene Vertrauen sowie die während dem gesamten Erstellungsprozess gewährte Unterstützung möchte ich dem Verlag sowie insbesondere dem Leitenden Lektor Hanno Thielen ausdrücklich danken. Auch mein Arbeitgeber, die Gruner AG in Basel, hat meine zeitaufwendige Nebentätigkeit als Herausgeber und Autor ein weiteres Mal genehmigt und durch meinen Vorgesetzten Stephan Gürtler (Mitglied der Geschäftsleitung) wohlwollend unterstützt, wofür ich mich ebenfalls bedanken möchte.

Trotz des immer deutlicher werdenden Fachkräftemangels und vielfältiger anderweitiger Verpflichtungen haben sich schließlich diverse Autorinnen und Autoren, allesamt ausgewiesene Fachpersonen in ihren Gebieten, zur Mitwirkung bereit erklärt, die nachfolgenden Beiträge erarbeitet, geduldig Rückfragen oder Änderungswünsche berücksichtigt und mich auch in vielerlei anderer Hinsicht bei der Erstellung des vorliegenden Werkes unterstützt. Hierfür bin ich sehr dankbar und hoffe, dass sie und alle anderen Leser mit dem vorliegenden Ergebnis zufrieden sind.

Abschließend noch ein Hinweis: Wo im vorliegenden Werk geschlechtsneutrale Formulierungen aus Gründen der Lesbarkeit unterbleiben, sind ausdrücklich stets alle Geschlechter angesprochen.

Basel, im Frühjahr 2024

Dr. Stephan Gundel

Inhaltsverzeichnis

Vorwort	5
Gliederung „Unternehmenssicherheit“	9
Herausgeber und Autoren	11
Teil A. Einführung und Überblick über die Unternehmenssicherheit	17
I. Ausgangslage	17
II. Die Rolle der Unternehmenssicherheit in einer volatilen Welt	19
III. Unternehmenssicherheit als Bestandteil des unternehmerischen Risikomanagements	29
IV. Unternehmenssicherheit im Kontext der öffentlichen Sicherheit	37
V. Rechts- und Regelungsrahmen der Unternehmenssicherheit	42
VI. Die Rolle von Versicherungen	54
Teil B. Physische Sicherheit als Bestandteil der Unternehmenssicherheit	60
I. Schutz vor Naturgefahren	60
II. Sicherheit, Gesundheit und Wohlbefinden bei der Arbeit ...	77
III. Brand- und Explosionsschutz/Gefahrstoffe und Gefahrgüter	92
IV. Standortsicherheit (Site Security)	111
V. Schutz von Personen	128
VI. Bedrohungsmanagement: Schutz vor Gewalt am Arbeitsplatz	148
Teil C. Informationssicherheit als Bestandteil der Unternehmenssicherheit	158
I. Integrale Betrachtung der Informationssicherheit	158
II. IT-Sicherheit (Cybersecurity)	170
III. Digital Listening: Digitale Lageverfolgung	189
IV. Schutz vor Wirtschafts- und Industriespionage	205

Teil D. Schutz der unternehmerischen Aktivitäten als Bestandteil der Unternehmenssicherheit	221
I. Supply Chain Security Management	221
II. Schutz vor Produkt- und Markenpiraterie	235
III. Schutz vor Wirtschaftskriminalität	254
IV. Sicherheit bei Auslandsreisen/Auslandssicherheit	271
Teil E. Bewältigung sicherheitskritischer Ereignisse als Bestandteil der Unternehmenssicherheit	289
I. Operational Resilience und Business Continuity Management	289
II. Notfall- und Krisenmanagement	307
III. Interne Untersuchungen durch Unternehmen	325
IV. Zusammenarbeit mit Dritten	344
Stichwortverzeichnis	361

Herausgeber und Autoren

Herausgeber

Dr. Stephan Gundel, Dr. rer. pol., Diplom-Volkswirt, Chefexperte Sicherheit bei Gruner am Hauptsitz Basel. Seit 2006 internationale Beratungstätigkeiten im Bereich Sicherheits- und Risikomanagement bzw. Gefahrenabwehr für Unternehmen, Betreiber kritischer Infrastrukturen, Groß-Veranstalter sowie Behörden und Organisationen mit Sicherheitsaufgaben. Zuvor wissenschaftlicher Mitarbeiter am Betriebswirtschaftlichen Seminar der Albert-Ludwigs-Universität Freiburg im Breisgau mit Forschungsschwerpunkt Risiko- und Sicherheitsmanagement. Forschungs- und Lehrtätigkeiten zur Entstehung sicherheitskritischer Ereignisse und ihrer Bewältigung, Sicherheit und Risikomanagement an verschiedenen Hochschulen und Bildungseinrichtungen. Buchautor und Herausgeber, diverse Publikationen in internationalen Fachzeitschriften.

Autoren

Heinz-Werner Aping, selbstständiger Consultant im Bereich öffentliche und private Sicherheit, zuvor bis zur Pensionierung 2014 Direktor beim Bundeskriminalamt und Leiter der Abteilung Sicherungsgruppe, anschließend Senior Expert für das BKA. 1975 Studium an der heutigen Hochschule für Wirtschaft und Recht Berlin zum Diplom-Verwaltungswirt, von 1975–1999 Laufbahn vom Kommissar bis zum Kriminaldirektor bei der Berliner Polizei, ab 1999 beim Bundeskriminalamt vom Leitenden Kriminaldirektor bis zum Direktor beim BKA. Von 2001 bis zur Pensionierung mit mehrmaliger Wiederwahl Chairman der Association of Personal Protection Services (APPS), des internationalen Netzwerkes von 50 staatlichen Personenschutzdienststellen von China bis zu den USA einschließlich Europol, Interpol, EU und UN mit Konferenzen weltweit.

Dr. Claudia Brandkamp, Dr. rer. pol., Dipl.-Kauffrau, Senior Expertin Personelle Sicherheit bei der Deutschen Telekom AG, Telekom Security. In dieser Funktion seit 2013 verantwortlich für das Thema Prävention gegen Gewalt am Arbeitsplatz sowie Aufbau und Implementierung des Bedrohungsmanagements innerhalb des Konzerns. Vom Europäischen Fachverband AETAP zertifizierte Bedrohungsmanagerin sowie Mitbegründerin des bundesweiten Forums Bedrohungsmanagement. Seit 2021 berufsbeleitend Studium der forensischen Psychologie an der Universität Konstanz. Vor dem Wechsel zur Deutschen Telekom Tätigkeiten in Unternehmensberatungen.

Prof. Dr. Martin Grothe, Dr. rer. pol., Geschäftsführer der complexium GmbH, Berlin. Studium und Promotion an der WHU. Nach Stationen in der freien Wirtschaft 2004 Gründung der complexium GmbH in Berlin: Mission ist die passgenaue und zeitnahe Bereitstellung von Security Intelligence durch Digital Listening. Das complexium-Analyseteam unterstützt die Unternehmenssicherheit von Klienten durch Früherkennung und Aufklärung von aktivistischen u. a. Bedrohungen, Sichtbarkeitsanalysen für den Personenschutz sowie einen übergreifenden Aktivismus-Monitor. Die Weiterentwicklung gelingt durch praxisgerichtete Forschung, etwa mit BMBF-Förderung im Bereich Desinformation (Hybrid). Neben dem Analyse-Lagezentrum wurde in den letzten Jahren die complexium.academy aufgebaut, um bewährte Fähigkeiten mit digitaler Kompetenz zu verbinden.

Prof. Oliver Hirschi, MSc. Business Information Technology, Dipl.-Ing. Informatik FH. Nach verschiedenen Tätigkeiten in der freien Wirtschaft als Projektleiter, Software-Architect und -Engineer Wechsel in Forschung und Lehre im Bereich Information Security an der Hochschule Luzern. Aktuell Dozent für Informationssicherheit und Leiter „eBanking – aber sicher“ an der Hochschule Luzern, zudem Inhaber und Geschäftsführer der SecAware GmbH sowie als Freier Lead Auditor ISO/IEC 27001 für die SQS tätig. Mitautor des Informationssicherheitshandbuchs für die Praxis, Autor diverser Publikationen, Vertreter der Hochschule Luzern in div. Gremien, Bearbeitung von Forschungs- und Dienstleistungsprojekten.

Richard Huber, Dipl.-Ing. (FH) für Technische Informatik. Studium Maschinenbau und dann Technische Informatik in Berlin mit Spezialisierung auf Systemanalyse, IT-Sicherheit, Medieneinsatz, Datenschutz. Seit Februar 2017 als Sicherheitsforscher am Fraunhofer FOKUS in der strategischen Entwicklung im Geschäftsbereich Vernetzte und zivile Sicherheit tätig. Von 2011 bis 2017 CIO der Europa-Universität Viadrina mit Verantwortung für die komplette Neugestaltung der Hochschul-IT-Landschaft. Zuvor von 1999 bis 2011 am FIZ CHEMIE Berlin beschäftigt. In früheren Tätigkeiten Spieleprogrammierer in Kanada und Oberflächenprogrammierer in der IT-Industrie.

Damian In-Albon, MSc. Security and Safety Management, Executive DAS HSG. Head of Corporate Resilience Management bei Die Mobiliar, die älteste private Versicherungsgesellschaft der Schweiz, am Hauptsitz in Bern. Davor Leiter Risikomanagement (Division Personenverkehr) bzw. Head of Corporate Security bei den Schweizerischen Bundesbahnen SBB sowie Ermittler/Inspektor sowie Einsatzleiter Spezialeinsätze beim Bun-

desamt für Polizei, fedpol. Vertretung der Mobiliar in diversen nationalen Gremien, Betreuung von internen und externen Forschungsprojekten.

Thomas Jehmlich, Studium an der Hochschule München, Abteilungsleiter Sicherheitsmanagement Ausland bei der KfW-Bankengruppe. Zuvor Leiter Sicherheit und Zentrale Dienste bei Cemex Deutschland sowie Senior Expert International Security bei der Daimler AG. Vor dem Wechsel in die private Wirtschaft Offizier beim Kommando Spezialkräfte (KSK) der Bundeswehr.

Manfred Jilg, Dipl.-Pädagoge, freiberuflicher Berater für Sicherheitsmanagement. Zuvor über 20 Jahre Direktor Security in der BASF-Gruppe am Standort Ludwigshafen, davor Leiter Security-Bereich Terminals bei der Fraport AG sowie Leiter Sicherheitsdienst der Verkehrsgesellschaft Frankfurt am Main. Vor dem Wechsel in die Privatwirtschaft Offizier der Bundeswehr mit unterschiedlichen Verwendungen im In- und Ausland.

Lars Mülli, Dipl. Ing. ETH Zürich, Executive MBA HSG, Direktor der Gebäudeversicherung des Kantons Zürich. Zuvor Leiter der Abteilung Brandschutz der Gebäudeversicherung des Kantons Zürich, Leiter der Abteilung Brandschutz, Entrauchung bei der Gruner AG sowie Projektleiter Risiko und Sicherheit bei EBP Zürich. Präsident der Vereinigung der Kantonalen Feuerversicherungen (VKF) sowie der Technischen Kommission Brandschutz (TKB) der VKF, Gesamtverantwortlicher für die Brandschutzvorschriften 2026 in der Schweiz. Buchautor, Referent und Dozent.

Dan Pruschy, Rechtsanwalt und Master of Laws (MLaw, Universität Zürich). Associate bei VISCHER Rechtsanwälten in Zürich, zuvor Tätigkeiten in internationalen Rechtsanwaltskanzleien. Zu den aktuellen Tätigkeitsgebieten gehören unter anderem Investigations & eDiscovery sowie Wirtschaftsstrafrecht, mit einem speziellen Fokus auf regulierte Unternehmen.

Matthias Rössler, Dipl.-Ing. Maschinenbau (RWTH Aachen), LL.M., Patentanwalt. Seit 1999 im Gewerblichen Rechtsschutz tätig, 2003 Zulassung als Patentanwalt und European Patent Attorney. Seit 2004 Partner in Patentanwaltskanzleien, seit 2018 in der Kanzlei karo IP Patentanwälte. Seit 2007 Dozent für Patent-, Gebrauchsmuster-, Marken- und Designrecht sowie für Arbeitnehmererfinder- und Lizenzvertragsrecht an der RWTH Aachen. Betreuung deutscher und internationaler Mandanten auf allen Gebieten des Gewerblichen Rechtsschutzes.

Prof. Dr. Meike Schröder, Dr. rer. pol., Dipl.-Kauffrau, Oberingenieurin am Institut für Logistik und Unternehmensführung der TU Hamburg so-

wie Professorin für Supply Chain Management an der IU Internationale Hochschule. Habilitation zum Thema „Strukturierte Verbesserung des Supply Chain Risikomanagements“ über einen Reifegradmanagement-Ansatz sowie ein Auditierungskonzept für das Supply Chain Risikomanagement. Aktuell Forschung zur Fragestellung, wie sich das Supply Chain Risikomanagement durch den Einsatz neuer Technologien, u.a. Maschinelles Lernen, verändern wird und wie sich Unternehmen darauf vorbereiten können. Umfangreiche Lehr- und Publikationstätigkeiten zum Supply Chain Risk Management.

Silvester Siegmann, Dipl.-Min., M.Sc. Betriebssicherheitsmanagement. Senior Scientist und Projektleiter am Institut für Arbeits-, Sozial- und Umweltmedizin der Heinrich-Heine-Universität in Düsseldorf sowie Leitender Sicherheitsingenieur bei ASS – Arbeitsschutz Siegmann. Vor dem Wechsel an die Heinrich-Heine-Universität Mitarbeiter bei der Deutschen Montan Technologie LB (DMT LB) in Bochum. Zahlreiche Publikationen in internationalen Fachzeitschriften, Dozent und Referent. Mitglied im Geschäftsführenden Vorstand des Verbandes für Sicherheit, Gesundheit und Umweltschutz bei der Arbeit (VDSI e.V.), Mitglied im DIN ISO 31000 ff. Risikomanagement und diversen RL-Ausschüssen des VDI e.V., Autor diverser Schriften zum Arbeitsschutz.

Patrick Sonntag, M.Sc. Sicherheitstechnik (Bergische Universität Wuppertal), staatlich anerkannter Sachverständiger für die Prüfung des Brandschutzes. Geschäftsführender Gesellschafter und Senior Projektleiter Brandschutz bei der Gruner Sachverständigen GmbH in Köln. Langjährige Erfahrung als Brandschutzingenieur, Mitarbeit in diversen Richtlinienausschüssen des VDI sowie Veröffentlichungen in Fachzeitschriften. Ehrenamtliches Mitglied einer Freiwilligen Feuerwehr.

Kai Ullwer, Kommunikationselektroniker, Lehrrettungsassistent, B.A. Emergency Management, Ausbildung zum gehobenen feuerwehrtechnischen Dienst an der Landesfeuerwehrschule Bruchsal. Kommandomitglied und Ressortleiter Betrieb & Projekte bei der Berufsfeuerwehr Basel, zuvor u.a. Mitglied der Geschäftsleitung DRK-Kreisverband Müllheim e.V. (Leiter Rettungsdienst und Bevölkerungsschutz). Langjähriges Mitglied des Führungsstabes des Landkreises Breisgau-Hochschwarzwald, Lehrtätigkeiten an der DRK-Landesschule Baden-Württemberg sowie als freiberuflicher Dozent für Führungslehre, Sicherheit und Gefahrenabwehr an diversen Symposien und Einrichtungen im deutschsprachigen Raum. Kommandant der Freiwilligen Feuerwehr Heitersheim und Leiter des kommunalen Krisenstabes der Stadt Heitersheim.

Christian Willi, Dipl. Ing. ETH Zürich. Leiter Geschäftsbereich Sicherheit bei EBP am Hauptsitz in Zürich. Experte im Bereich Risiko und Sicherheit mit Arbeitsschwerpunkten im Bereich integrales Risikomanagement von Naturgefahren, Resilienz-Management von Infrastrukturnetzen und Gesellschaften gegenüber naturbedingten und sozioökonomisch bedingten Einwirkungen und Entwicklungen sowie Fragestellungen im Bereich der Sicherheit im Straßenverkehr. Langjährige internationale Erfahrung als Sicherheitsexperte und Projektleiter.

Wolfgang Zier, Dipl.-Verwaltungsfachwirt, MBA, Head of Corporate Security eines DAX-Konzerns. Zuvor in vergleichbaren Funktionen bei diversen Unternehmen in Deutschland tätig. Vor dem Wechsel in die Privatwirtschaft Kriminalbeamter beim Bundeskriminalamt mit verschiedenen Verwendungen im In- und Ausland. Veröffentlichungen in internationalen Fachpublikationen, Referent und Diskutant an internationalen Fachtagungen.

Teil A. Einführung und Überblick über die Unternehmenssicherheit

Stephan Gundel, Gruner AG, Basel

Lars Mülli, GVZ Gebäudeversicherung Kanton Zürich, Zürich

I. Ausgangslage

Die Funktion der Unternehmenssicherheit ist im Kontext der Unternehmensführung eine immer noch **junge, stark interdisziplinäre Aufgabe**. Aufgrund ihrer verhältnismäßig kurzen Entwicklung und des nicht immer unmittelbar sichtbaren Beitrags zur unternehmerischen Wertschöpfung fehlt ihr bis heute vielfach an breiter Akzeptanz sowie Verankerung in den Unternehmen, deren Schutz sie eigentlich gewährleisten soll.

Dieser Umstand ist bis zu einem Teil zunächst dadurch erklärbar, dass es bis heute im deutschsprachigen Raum an **konkreten Rechtsnormen fehlt**, welche die umfassenden Sicherheitspflichten eines Unternehmens vollständig kodifizieren. Ergänzend trägt vermutlich auch der immer noch geringe Akademisierungsgrad, heterogene Ausbildungsstand sowie stark variierende Erfahrungshintergrund der in den Unternehmen tätigen Sicherheitsverantwortlichen dazu bei, dass ihre Rolle – ungeachtet ihrer realen Arbeitsqualität und Erfolge – **nicht immer mit dem notwendigen „Standing“ in den Konzernen und Unternehmen** verbunden ist. So ist es kaum verwunderlich, dass ihre Positionierung – viel zu selten direkt auf oder bei der Ebene der Geschäftsleitung –, das definierte Aufgabengebiet und die zur Verfügung stehenden Ressourcen auch zwischen vergleichbaren Unternehmen stark variieren. Nur selten lassen sie eine wirklich umfassende, strategische und operative Interpretation einer modernen **„Corporate Security“** zu. Dass sich diese überdies in unterschiedlichsten Themenfeldern und hierarchischen Ebenen bewegen und an rasch wandelnde Rahmenbedingungen anpassen muss, erschwert ihre Rolle zusätzlich. Schließlich ist auch der als **„Präventionsparadox“** bekannte Mechanismus zu beachten, nachdem risikominimierende Maßnahmen für ein Unternehmen trotz ihrer generellen Effektivität für einzelne Mitarbeitende oder Bereiche wenig greifbar oder sogar vordergründig hinderlich sind und zudem – wenn sie zur Risikominimierung beigetragen haben – retro-

spektiv übertrieben wirken.⁴ Die dauerhafte Gewährleistung der Unternehmenssicherheit ist somit eine **schwierige, mit hohen Anforderungen an die Frustrationstoleranz** einhergehende Aufgabe.

Dieser Ausgangslage tragen seit mehreren Jahren **vielfältige Professionalisierungsbemühungen** Rechnung. Einschlägige Lehr- und Nachschlagewerke, Fachzeitschriften, Verbandstätigkeiten, Aus- und Weiterbildungsangebote sowie politische Initiativen können jedoch nicht darüber hinwegtäuschen, dass der Themenkomplex „Unternehmenssicherheit“ immer noch eine, wenn auch wachsende, Nische darstellt. Bis heute ist den Autoren beispielsweise keine Bildungseinrichtung auf universitärem Niveau bekannt, welches Aspekte der Unternehmenssicherheit in anerkannte, betriebswirtschaftliche oder Management-Studiengänge quasi selbstverständlich als Vertiefungsfach integriert. Dies ist umso erstaunlicher, wenn man die immer wieder betonte Wichtigkeit entsprechender Experten einerseits sowie die voranschreitende Akademisierung und Spezialisierung in vielen unternehmerischen Bereichen andererseits bedenkt.

Diese mitunter etwas ernüchternde Ausgangslage in akademischer Ausbildung und Unternehmenspraxis trifft nun auf ein sich rapide wandelndes und **immer anspruchsvoller werdendes, sicherheitspolitisches Umfeld** der Unternehmen und Konzerne sowie damit einhergehend stetig **steigende Ansprüche an ihre Sicherheit und „Resilienz“**. Die Liste der einschlägigen Schlagwörter und Einflussfaktoren – von der viel beschworenen „*Zeitenwende*“ in öffentlicher wie privater, militärischer wie ziviler Hinsicht bis zu den sicherheitsrelevanten Nebenwirkungen der digitalen Transformation – ist lang und wird in den folgenden Beiträgen detailliert untersucht. Generell lässt sich jedoch feststellen, dass diese Entwicklungen zu einer **stetigen Erweiterung der durch die Unternehmenssicherheit zu berücksichtigenden Themen** führen. Der damit verbundene und oft nicht zu deckende Bedarf an qualifizierten personellen Ressourcen, die häufig kritisch hinterfragten finanziellen Aufwände für diese Ressourcen, Programme und Maßnahmen sowie unklare Vorstellungen, Ziele und organisatorische Einbettungen der Unternehmenssicherheit in den Unternehmen selbst führen dann zu einem immer schwierigeren Umfeld für die Sicherheitsverantwortlichen. Das vorliegende Buch hat sich daher zum Ziel gesetzt, in diesem Umfeld eine Hilfestel-

4 Das Präventionsparadox geht auf den britischen Epidemiologen Geoffrey Rose zurück, vgl. Franzkowiak (2022): Präventionsparadox, in: Bundeszentrale für gesundheitliche Aufklärung (Hrsg.): Leitbegriffe der Gesundheitsförderung und Prävention. Glossar zu Konzepten, Strategien und Methoden.

lung für die mit Sicherheit in Unternehmen betrauten Verantwortungsträger, aber auch für ihre Ansprechpartner bei Behörden oder Dienstleistern zu sein.

II. Die Rolle der Unternehmenssicherheit in einer volatilen Welt

1. Anfänge der Unternehmenssicherheit

Wie eingangs bereits erwähnt, ist die Unternehmenssicherheit im deutschsprachigen Raum eine recht neue Disziplin bzw. Funktion. Dieter K. Sack hat in seinem Beitrag zum Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit deren historische Entwicklung dargestellt und dabei festgehalten, dass vor allem **die terroristischen Aktivitäten der 1970er-Jahre** zu einer Professionalisierung des Werkschutzes sowie dem Aufbau von weitergehenden Sicherheitsfunktionen im „**Security**“-**Bereich** geführt hatten.⁵ In der Folge, insbesondere im Zuge der nach dem Fall des Eisernen Vorhangs einsetzenden **Globalisierung**, entwickelten sich Ansprüche an und Aufgaben von unternehmenseigenen Sicherheitsabteilungen nochmals deutlich weiter und es kam zur Etablierung heute noch gebräuchlicher Strukturen sowie einer **vertieften Zusammenarbeit zwischen staatlichen Behörden und der Wirtschaft**.⁶

Zeitgleich stiegen im selben Zeitraum auch die Anforderungen der zum damaligen Zeitpunkt noch häufig getrennt betrachteten „**Safety**“-**Funktionen** deutlich an. Mit zunehmendem Wohlstand, einer stärkeren Rolle der Gewerkschaften bzw. Verbreitung von arbeitnehmerfreundlichen Vorstellungen des Arbeitsplatzes sowie einem steigenden Umweltbewusstsein wurden Vorschriften zu Arbeitssicherheit und Gesundheitsschutz, betrieblichem Brandschutz, Störfallvorsorge und Umweltschutz etc. ausgebaut und stellten **erhöhte Anforderungen an entsprechende Ressourcen und Maßnahmen** in Unternehmen. Im nationalen, zumeist standortbezogenen Kontext, wurden jedoch lange Zeit wenig Synergieeffekte mit den „Security-lastigen“ Abteilungen zur Unternehmenssicherheit im Sinne von Sack genutzt oder überhaupt gesehen. Noch zu Beginn dieses Jahrtausends existierten daher in vielen Unternehmen organisatorisch und personell getrennte Organisationseinheiten, die sich mit Sicherheitsbe-

5 Vgl. Sack (2012): Vom Werkschutz zur Unternehmenssicherheit, in: Stober/Olschok/Gundel/Buhl (2012), Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Stuttgart, S. 847–852.

6 Vgl. ebenda.

langen der Unternehmen weitestgehend autonom befassten. In nicht wenigen Unternehmen ist diese Trennung bis heute stark verankert.

2. Weitere Professionalisierung nach dem Jahrtausendwechsel

Mit den islamistischen Anschlägen auf Ziele in New York und Washington am **11. September 2001** wandelte sich die allgemeine Stimmung und geopolitische Lage in den westlichen Ländern merklich – das vermeintliche „**Ende der Geschichte**“⁷ war auf einschneidende Art und Weise vom „**Ende der Spaßgesellschaft**“⁸ abgelöst worden. Trotz des alsbald startenden „**Kriegs gegen den Terror**“ und seiner bis heute nachwirkenden Verwerfungen im Nahen und Mittleren Osten schritt aber die internationale Verflechtung von Politik, Wirtschaft, Kultur und Umwelt weiter voran und brachte umfangreiche Sicherheitsanforderungen für **die zunehmend international agierenden Unternehmen** mit sich. Dies zeigte sich einmal in den neu aufkommenden Regularien zur Verhinderung terroristischer Anschläge (vor allem in Verkehr- und Logistikbereichen seitens der USA stark vorangetrieben) sehr konkret, generell aber auch in einer **vermeintlich zunehmenden Bedeutung sicherheitsrelevanter Fragestellungen in Gesellschaft und Unternehmen** allgemein. In seinen auch heute noch hochaktuellen Ausführungen schrieb Schmidt jedoch bereits 2012, dass man hieraus „*keinen Automatismus*“ für eine zunehmende Bedeutung der Unternehmenssicherheit ableiten könne – vielmehr hänge der Erfolg entsprechender Personen und Abteilungen im starken Masse davon ab, wie weitblickend, unterstützend und letztendlich auch qualifiziert die eigene Rolle ausgeübt würde.⁹ Er bezog sich dabei, wie viele andere Verantwortungsträger und Beobachter im Umfeld der Unternehmenssicherheit auch, auf das seinerzeit (und bis heute) aufgrund seiner griffigen Aussage **sehr populäre Modell der Unternehmenssicherheit** als „**business enabler**“, welches durch den US-Amerikaner Dennis R. Dalton 2003 geprägt worden war.¹⁰ Demnach wäre die idealtypische Unternehmenssicherheit „*eine etablierte betriebliche Funktion, die die Kernprozesse unterstützt bzw. teilweise sogar erst ermöglicht. Zur Erfüllung dieser Aufgaben hat die*

7 Fukuyama (1992): *The End of History and the last man*, New York.

8 NZZ (2002): *Vom Ende der Spassgesellschaft*, ohne Verfasser, 14.04.2002.

9 Vgl. Schmidt (2012): *Umfang, Bedeutung und Ziele der Unternehmenssicherheit*, in: Stober/Olschok/Gundel/Buhl (2012), *Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit*, Stuttgart, S. 873–874.

10 Vgl. Dalton (2003): *Rethinking Corporate Security in the Post-9/11 Era*, Amsterdam et al.

*Unternehmenssicherheit ausreichende Kompetenzen, Aufgaben und Ressourcen.*¹¹

In eine ähnliche Richtung zielte eine ebenfalls aus den 2000er-Jahren stammende Definition der Unternehmenssicherheit durch die beiden Autoren des vorliegenden Beitrags, wonach sich die Unternehmenssicherheit strukturiert und umfassend mit jenen Gefährdungen bzw. Risiken befassen müsse, „*die den operativen Betrieb des Unternehmens beeinträchtigen oder sogar unterbrechen können und aus den Unternehmenseigenschaften und der Unternehmensumwelt resultieren*“.¹² Demnach ist die **Unternehmenssicherheit als Bestandteil des unternehmerischen Risikomanagements** zu verstehen, welcher sich thematisch integral (d.h. über Safety- und Security-Belange hinweg) mit den sog. **operativen Risiken** (in Abgrenzung zu den strategischen und Finanzrisiken) befasst. Faktisch würde dies eine sehr umfassende Positionierung mit einer Vielzahl an Themen und adressatengerecht zu bedienenden Anspruchsgruppen bedeuten. Hintergrund dieser Überlegung war die nach den verschiedenen Bilanzierungsskandalen und dem Zusammenbruch des sog. „*Neuen Markts*“ aufkommende, verschärfte Regulierung von Unternehmen (d.h. primär Kapitalgesellschaften) hinsichtlich ihres allgemein notwendigen Risikomanagements. Schmidt merkte hierzu allgemein an, dass dieser vorrangig in angelsächsischen Ländern anzutreffende Ansatz bzw. seine organisatorische Umsetzung eher einem **theoretischen, zentralistischen Verständnis** entspreche und in den dezentral geprägten Organisationsstrukturen großer Unternehmen **Reibungsverluste hervorrufen** würden.¹³ Nichtsdestoweniger orientieren sich viele Unternehmen aktuell am sog. „**Three-Lines-Modell**“ des Risikomanagements, in dem auf einer Konzernebene (oder „*Second-line*“) Konzernsicherheitsfunktionen und -aufgaben mehr oder minder gleichberechtigt zu anderen Risikomanagement- und Compliance-Funktionen angeordnet sind.¹⁴

Trotz des vermeintlichen Bedeutungszuwachses von Sicherheitsfunktionen und den damit einhergehenden, eingangs bereits erwähnten Professionalisierungsbemühungen verschiedener Akteure kann retrospektiv

11 Schmidt (2012): Umfang, Bedeutung und Ziele der Unternehmenssicherheit, in: Stober/Olschok/Gundel/Buhl (2012), Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Stuttgart, S. 874.

12 Gundel/Müllli (2009): Unternehmenssicherheit, München, S. 5.

13 Vgl. Schmidt (2012): Umfang, Bedeutung und Ziele der Unternehmenssicherheit, in: Stober/Olschok/Gundel/Buhl (2012), Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Stuttgart, S. 875.

14 Vgl. dazu die Ausführungen im nachfolgenden Kapitel.

nicht das Bild einer deutlichen sowie breit abgestützten positiven Entwicklung von Unternehmenssicherheit (im Sinne von allgemeiner Bedeutung, hierarchischer Verankerung, Sichtbarkeit und Ressourcen) im Zeitraum zwischen den Anschlägen des 11. September 2001 sowie der aktuellen „*Zeitenwende*“ mit dem russischen Überfall auf die Ukraine im Frühjahr 2022 gezeichnet werden. Während einige Unternehmen und ihre Verantwortlichen – oft auch als Autorinnen, Referenten oder „*role model*“ deutlich sichtbar – ein durchaus sehr modernes und zukunftsfähiges Modell der Konzern- oder Unternehmenssicherheit entwickelten, wird derselbe Themenkomplex andernorts immer noch eher nachrangig betrachtet – wobei sich hier erfahrungsgemäß häufig mangelndes Verständnis der Unternehmen einerseits sowie eine mindestens rückwärts-gewandte Rollenvorstellung der Sicherheitsverantwortlichen andererseits im ungünstigen Sinne gegenseitig beeinflussen. Am Vorabend der Corona-Pandemie sowie des russischen Überfalls auf die Ukraine befanden sich viele Unternehmen und ihre Sicherheitsverantwortlichen daher immer noch in einem Rollen- und Sicherheitsverständnis wieder, welche vermutlich schon eine Dekade zuvor modernisierungsbedürftig gewesen wären. Nichtsdestoweniger gibt es auf der anderen Seite eine steigende Zahl von Sicherheitsverantwortlichen, die einen sehr umfassenden Blick auf ihre Herausforderungen und Aufgaben haben und diese integral, vernetzt und nachhaltig angehen.

3. Unternehmenssicherheit im Kontext der „*Zeitenwende*“

Die anfangs 2020 in den europäischen Ländern ihre volle Wucht entfaltende Corona-Pandemie sowie der fast genau 2 Jahre später beginnende Überfall des russischen Militärs auf die Ukraine stellen, möglicherweise auch erst mit dem Abstand von einigen Jahren betrachtet, den **vorläufigen Kulminationspunkt** einer **schleichenden Entwicklung zu einer unsicheren, multipolaren Welt** dar. Beide Ereignisse und ihre Folgen, so unabhängig sie voneinander auch sind, verdeutlichen exemplarisch die **bereits lange zuvor schwelenden Probleme** globaler Umweltveränderungen, wachsender Entfremdung zwischen unterschiedlichen politischen und kulturellen Einflussphären (die sich paradoxerweise gemeinsam mit immer stärker integrierten, internationalen Lieferketten entwickelte), nachteiliger demografischer Entwicklungen und eines zunehmend offen und verdeckt geführten, erbitterten Kampfes um knappe Ressourcen. Ähnlich wie der 11. September 2001 stellen sie in jedem Fall eine **deutliche und umfassende Zäsur für die öffentliche und private Sicherheit** dar, die vor-

dergründig zu einem Bedeutungszuwachs der Unternehmenssicherheit führen sollte – wobei dies auch heute, ganz im Sinne der Überlegungen von Schmidt aus dem Jahr 2012, keinen Automatismus darstellt. Vielmehr wird zumindest entsprechend sensiblen Verantwortungsträgern immer mehr bewusst, was Unternehmenssicherheit eigentlich leisten müsste, häufig aber aufgrund fehlender Kompetenzen und Aufgabengebiete sowie insbesondere mangelnder (qualifizierter) Ressourcen nicht zu leisten im Stande ist. Demgegenüber stehen über die letzte Dekade **stetig gewachsene Anforderungen aus verschiedenen Richtungen**, die es zukünftig zu erfüllen gilt.

Bereits seit mehreren Jahren steigen generell die **Erwartungen an die „Corporate Governance“** von Unternehmen, d. h. eine den gesamten, einschlägigen rechtlichen Regelrahmen berücksichtigende, langfristig orientierte, nachhaltige und Risiken minimierende Unternehmensführung. Anfangs der 2000er-Jahre wurden im deutschsprachigen Raum entsprechende für Kapitalgesellschaften mehr oder weniger verbindliche Regelwerke eingeführt, namentlich der:

- „Deutsche Corporate Governance Kodex“¹⁵,
- „swiss code of best practice for corporate governance“¹⁶,
- „Österreichischer Corporate Governance Kodex“¹⁷.

In allen entsprechenden Regelwerken, die zumeist auf Basis handels- oder aktienrechtlicher Gesetze mindestens für börsennotierte Gesellschaften verbindlich zu berücksichtigen sind, wird die besondere Bedeutung **angemessener Risikomanagement- und Kontrollsysteme** für die gute Unternehmensführung besonders hervorgehoben. Insbesondere international tätige Unternehmen sind überdies mit den **OECD-Leitsätzen für multinationale Unternehmen** und den Grundprinzipien des **UN Global Compact** konfrontiert, die auf freiwilliger Basis zu Verbesserungen der Unternehmen u. a. in den für die Unternehmenssicherheit hochrelevanten Bereichen des Arbeits- und Gesundheitsschutzes, Umweltschutzes sowie Wirtschaftskriminalität und Korruption führen sollen.¹⁸ Daraus ergibt sich fast zwangsläufig, dass Unternehmen ihre Anstrengungen im **Bereich Sicherheit (Safety), Nachhaltigkeit und Integrität** erheblich ausweiten muss(t)en, um zumindest in den westlichen Demokratien den normativen

15 Vgl. Deutscher Corporate Governance Kodex in der Fassung vom 28. April 2022.

16 Vgl. swiss code of Best Practice for corporate governance, Fassung 2016, economiesuisse.

17 Vgl. Österreichischer Corporate Governance Kodex, Fassung Jänner 2023.

18 Vgl. ausführlich Gundel (2020): Global Security – Sicherheit bei Auslands- und Reisetätigkeiten, Stuttgart, S. 119–120.

und gesellschaftlichen Anforderungen zu genügen. In aktuell stark aufgewühlten und zunehmend polarisierten Gesellschaften werden vermeintliche oder tatsächliche Abweichungen häufig aufgegriffen und scharf verurteilt, wobei meinungsstarke Gruppierungen potenzieller Stakeholder sehr kompromisslos **ein über alle Zweifel erhabenes Agieren der Unternehmen verlangen**. Generell ist zudem zu beobachten, dass die Toleranz der Gesellschaft gegenüber Fehlern und Unterlassungen, seien sie auch unabsichtlich, stetig abnimmt. Parallel dazu nehmen jedoch Vorverurteilungen – nicht selten mit bescheidenem Wissen zum effektiv Vorgefallenen – stark zu. Diese sind gerade durch ihre rasche und häufig sehr reißerische Publikation in den (sozialen) Medien kaum mehr aus den Köpfen zu kriegen.

Dieser erhöhten Sensibilität für Sicherheit (im Sinne von „Safety“) und Compliance steht im deutlichen Widerspruch zum **starken, zunehmend polarisierten und oft mit unlauteren Mitteln geführten Wettbewerb im internationalen Kontext**. Konkurrierende Staaten und Wirtschaftsblöcke kämpfen auf der internationalen Bühne rücksichtslos und weit weniger moralorientiert um **geopolitischen sowie wirtschaftlichen Einfluss**, den Zugang zu knappen Ressourcen und Märkten sowie den damit verbundenen Wohlstand.

Die Bedeutung von Innovationen und neuen Technologien, die über Netzwerkeffekte zunehmend eine wirtschaftliche Vormachtstellung begründen oder weiter ausbauen können, ist dabei immens. Insbesondere für die international agierenden Unternehmen, aber auch für die vermeintlich auf ihren Heimatmärkten geschützten, innovationsstarken kleinen und mittleren Unternehmen in den export-orientierten Volkswirtschaften Deutschlands, Österreichs und der Schweiz ergeben sich daraus erhebliche Implikationen: Sie müssen mit einer Vielzahl von Herausforderungen im Bereich **Sicherheit (Security), Verfügbarkeit und Wirtschaftsschutz** zurechtkommen, ohne dass es bis heute eine effektive, internationale Kriminalitätsbekämpfung oder sogar auch nur (völkerrechtlich anerkannte) Durchsetzungsinstantz international anerkannter Rechts gäbe.¹⁹ Demgegenüber steht die seit Jahrzehnten **stark wachsende, internationale (Organisierte) Kriminalität**, was den langjährigen Sicherheitschef der BASF, Dieter K. Sack, bereits 2012 zur These veranlasste, dass der Globalisierung der Wirtschaft die Globalisierung der Kriminalität gefolgt wäre, nicht jedoch die Globalisierung oder zumindest Europäisierung staatlicher Si-

¹⁹ Vgl. ausführlich ebenda, S. 72–93.

cherheitsstrukturen – die international tätigen Unternehmen müssten sich daher selbst helfen.²⁰

Erstaunlicherweise befinden sich **Unternehmen in diesem Spannungsfeld** verschiedenster Sicherheitsinteressen bis heute noch in einem **zusätzlichen Spagat**: Sie verlangen einerseits Freiheiten und Eigenverantwortung, welche als zentrale Standbeine liberaler Wirtschaftssysteme erachtet werden, rufen aber im Ereignis- oder Krisenfall nach dem Staat oder Versicherungen, welche die seitens der Unternehmen häufig bewusst eingegangenen Risiken bzw. deren Folgen dann bewältigen und nach Möglichkeit noch dafür haften sollen. Diese paradoxe Herangehensweise zeigt sich nicht nur im Handeln der Wirtschaftsakteure, sondern vielmals bereits bei der Anhörung bzw. Vernehmlassung von normativen Vorgaben in sicherheitsrelevanten Bereichen.

Zusammenfassend darf die **aktuelle Situation für Sicherheitsverantwortliche in Unternehmen als herausfordernd betrachtet** werden. Auf einer **strategischen Ebene** haben die aktuellen geopolitischen Entwicklungen zwar die hohe Bedeutung von Sicherheitsmaßnahmen verdeutlicht, die vermeintlichen unternehmerischen Zwänge und Bedürfnisse verhindern aber nicht selten eine konsequente Durchsetzung. Die bereits 2012 im „*Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit*“ insbesondere von Sack, Schmidt und Haacke angesprochenen Problemfelder hinsichtlich Qualifikation und Anerkennung, Tätigkeitsgebiet und Aufgabenzuschnitt sowie Kompetenzen und Ressourcen der Sicherheitsverantwortlichen sowie Sicherheitsabteilungen, sind auch über 10 Jahre später offensichtlich hochaktuell und erschweren eine bessere Positionierung der Unternehmenssicherheit.²¹ Auf **operativer Ebene** sehen sich die Sicherheitsverantwortlichen mit einer erheblichen Breite an Herausforderungen, zu berücksichtigenden Risiken sowie korrespondierenden Maßnahmen konfrontiert, die mit großem Fingerspitzengefühl unter den Augen einer kritischen Unternehmensleitung und Öffentlichkeit umgesetzt werden müssen. Wenn die amtierende deutsche Bundesinnenministerin in einem Interview prominent die zukünftige gesetzliche Pflicht der deutschen Unternehmen zum Schutz kritischer Infra-

20 Vgl. Sack (2012): Vom Werkschutz zur Unternehmenssicherheit, in: Stober/Olschok/Gundel/Buhl (2012), *Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit*, Stuttgart, S. 851–852.

21 Vgl. dazu die entsprechenden Beiträge in Teil D Unternehmenssicherheit (Corporate Security) von Stober/Olschok/Gundel/Buhl (2012), *Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit*, Stuttgart.

strukturen hervorhebt,²² dann darf man dies einerseits als Bestätigung der seit vielen Jahren schwierigen Rahmenbedingungen für die Unternehmenssicherheit werten und andererseits gespannt sein, ob und wie sich diese gesetzgeberische Initiative in den nächsten 10 Jahren auf die tatsächliche Rolle von Sicherheitsabteilungen in Unternehmen auswirkt.

4. Handlungsfelder und Rolle der Unternehmenssicherheit

Aus dem vorangegangenen Abriss der Entwicklungen im Bereich Unternehmenssicherheit seit der Jahrtausendwende sowie der aktuellen und absehbaren Entwicklung des geopolitischen und wirtschaftlichen Umfelds lassen sich verschiedenste Handlungsfelder für die Unternehmenssicherheit identifizieren. Sie bilden die Grundlage für die weiteren Teile des vorliegenden Buchs und ergeben sich wie folgt:

- **Klimawandel und globale Umweltveränderungen** haben immer deutlich sichtbarere Auswirkungen auf die Sicherheit von Unternehmen. Die entsprechenden Auswirkungen müssen daher im nationalen sowie insbesondere internationalen Kontext analysiert und in Risikobeurteilungen sowie Sicherheitsmaßnahmen berücksichtigt werden. Neben der praktischen Notwendigkeit für die Gewährleistung von Sicherheit und Verfügbarkeit sind dabei auch die steigenden Anforderungen von Kunden, Geschäftspartnern und Investoren bezüglich der Einhaltung einschlägiger ESG-Kriterien relevant. Diese werden stetig nachgeführt und ihre Einhaltung immer anspruchsvoller.
- In zunehmend polarisierten Gesellschaften im In- und Ausland sowie unter Berücksichtigung der diesbezüglichen Erwartungshaltungen, insbesondere der jüngeren Arbeitsgenerationen, wird die **Einhaltung der Fürsorgepflichten** im Bereich Safety und Security für Unternehmen immer wichtiger. Ergänzend kommen demografische Entwicklungen, Fachkräftemangel sowie eine steigende Multikulturalität mit all ihren Vor- und Nachteilen hinzu, welche die **Gewährleistung von Arbeitssicherheit und Gesundheitsschutz** in einem rasch wandelnden, hoch dynamischen Umfeld immer herausfordernder machen. Dies gilt sinngemäß auch für den **Personenschutz** exponierter Verantwortungsträger sowie das allgemeine **Bedrohungsmanagement** hinsichtlich Gewalt und Übergriffen am Arbeitsplatz.
- Durch die technologischen Entwicklungen gehen Handlungsfelder in den Bereichen **physische Sicherheit** (Brandschutz, Standort- und Infra-

22 Vgl. Der Spiegel (2023): „Enorme Auswirkungen“, Interview mit Bundesinnenministerin Nancy Faeser, Der Spiegel Nr. 35/26.08.2023, S. 31.

- struktursicherheit), **Informations- und Cybersicherheit** sowie **Business Continuity** praktisch nahtlos ineinander über. Durch die Unternehmenssicherheit müssen Risiken und Maßnahmen ganzheitlich gedacht und implementiert werden – mit einer Vielzahl interner und externer Partner.
- Die **integrale Informationssicherheit**, Konzepte und Maßnahmen der Cybersicherheit, die Beherrschung von Analysefähigkeiten und Maßnahmen in den sozialen Medien sowie generell die sichere Nutzung diesbezüglicher Methoden und Hilfsmittel sind für Sicherheitsverantwortliche essenziell – auch für die Etablierung einer „**intelligence-led security**“. Bei aller notwendigen Fokussierung auf neue Technologien dürfen dabei jedoch auch **andere Informationsträger** nicht vernachlässigt werden.
 - Durch die Corona-Pandemie und die Auswirkungen des russischen Überfalls auf die Ukraine wurde die Bedeutung **sicherer und verfügbarer Lieferketten** nochmals verdeutlicht. Ihre sichere Gestaltung im In- und Ausland ist daher ein zentrales, aber aufgrund der direkten wirtschaftlichen Implikationen sehr sensibles Handlungsfeld für die Unternehmenssicherheit.
 - Der Schutz vor **Wirtschafts- und Industriespionage** sowie **Produkt- und Markenpiraterie** ist in einem verschärften internationalen Wettbewerb von erheblicher Bedeutung für die wirtschaftliche Widerstandsfähigkeit einzelner Unternehmen, aber auch der deutschsprachigen Volkswirtschaften insgesamt. Dies erfordert ebenfalls eine entsprechende Schwerpunktsetzung durch die Unternehmenssicherheit.
 - Sobald Unternehmen selbst international agieren, sehen sie sich einem anspruchsvollen bis zunehmend feindlichen Umfeld ausgesetzt, welches durch geopolitische Konflikte, scharfen internationalen Wettbewerb, Kampf um knappe Ressourcen sowie regelmäßige Unterbrüche von Leistungsprozessen und Lieferketten gekennzeichnet ist. Umfassenden **Konzepten der Auslandssicherheit** kommt daher, in Verbindung mit den bereits genannten, stetig steigenden Ansprüchen an Fürsorgepflichten für (internationale) Mitarbeitende eine immer wichtiger werdende Rolle zu.
 - Zur Vermeidung und Bewältigung sicherheitskritischer Ereignisse ist der **Einbezug der gesamten Belegschaft eines Unternehmens** unabdingbar. Neben dem Verhalten im digitalen Umfeld (korrektes, zurückhaltendes Verhalten im Umgang mit Internet, Mail, Messengers, Social-Media etc.) zählt dazu auch das Verhalten in der physischen Realität – beispielsweise hinsichtlich persönlicher Integrität, Wachsamkeit an Standorten und auf Reisen, Mitwirkung am Informationsschutz etc.

Diese einzelnen, teilweise unabhängigen, teilweise miteinander verknüpften Tätigkeitsfelder der Unternehmenssicherheit können aus Sicht der Autoren nur dann adäquat bewältigt werden, wenn Sicherheitsverantwortliche in Unternehmen ihre Rolle entsprechend definieren und wahrnehmen (können).

Eine effektive Herangehensweise bedingt fast zwangsläufig, dass sich die **Unternehmenssicherheit auf strategischer und operativer Ebene zumindest methodisch in das unternehmerische Risikomanagement integriert**.²³ Hier ist nicht nur eine auf Basis der gesetzlichen Vorgaben häufig notwendige Verankerung in „Corporate Governance“-Strukturen gewährleistet, sondern es kann in der Unternehmenspraxis fundiert und faktenbasiert sowie frühzeitig und nachhaltig auf das unternehmerische Handeln Einfluss genommen werden.

Tatsächlich sind, trotz aller Entwicklungen der letzten Jahre, in der Praxis vielfach **Ressourcenknappheit im Bereich Unternehmenssicherheit** (auch durch den besonders starken Fachkräftemangel in diesem Bereich) sowie häufig verzernte, d. h. zu optimistische Risikowahrnehmungen in Politik, Wirtschaft und Gesellschaft und dadurch **Beharrungstendenzen** zu erkennen. In einem derartigen Spannungsfeld beschränken sich dann einige Sicherheitsverantwortliche auf die eher reaktive und nicht zuletzt stimmungsgeladene Bearbeitung bekannter, zumeist regulativ vorgegebener Themen wie Arbeitssicherheit und Gesundheitsschutz, Standortsicherheit und Brandschutz, Reisesicherheit oder betriebliches Notfallmanagement. Dies liegt möglicherweise auch an den hohen rechtlichen Anforderungen an die Gewährleistung der Sicherheit verschiedenster, vorgenannter operativer Prozesse, sodass die zwingend notwendige Herstellung einer **„Compliance“ mit einschlägigen Gesetzen, Normen und anerkannten Regeln der Technik** immer aufwendiger wird. Erschwerend kommt hinzu, dass der regulative Regelrahmen immer komplizierter, undurchsichtiger und teilweise auch widersprüchlicher wird, was nochmals zu Ressourcen- und Reibungsverlusten führt.

Um dennoch eine moderne und effektive Rolle einnehmen zu können, müssten sich im Sinne eines **Idealfalls für die Unternehmenssicherheit folgende Rahmenbedingungen** ergeben:

- Unternehmen bzw. deren Führungskräfte, die den Mehrwert einer Risiko- und Informations-basierten, umfassenden Unternehmenssicherheit erkennen und entsprechend fördern.

²³ Vgl. Gundel/Müllli (2009): Unternehmenssicherheit, München, S. 5.

- Im höchsten Maß interdisziplinär denkende, vernetzt handelnde und vielseitig interessierte Sicherheitsverantwortliche, die das Geschäftsmodell ihres Unternehmens sehr gut kennen und die damit verbundenen, aktuellen wie auch künftigen sicherheitsrelevanten Herausforderungen zu analysieren vermögen sowie als Grundlage ihres Handelns betrachten.
- Der Verantwortung entsprechende Positionierung der Sicherheitsverantwortlichen bzw. Sicherheitsabteilungen im Unternehmen.
- Nachhaltig ausgerichtete und zur Verfügung gestellte Strukturen und Ressourcen der Unternehmenssicherheit auf strategischer und operativer Ebene.

Die Realität zeigt aus der Sicht und langjährigen Erfahrung der Autoren demgegenüber ein **heterogenes Bild** – von einer idealtypischen Ausgestaltung der Unternehmenssicherheit bis hin zu völlig dysfunktionalen Strukturen, Prozessen und Personalentscheidungen. Die leider sehr langsam, aber dennoch stetig weiter voranschreitende Akademisierung, Diversifizierung und Professionalisierung der Sicherheitsverantwortlichen in den Unternehmen macht dennoch Hoffnung auf eine mittel- bis langfristige Verbesserung.

III. Unternehmenssicherheit als Bestandteil des unternehmerischen Risikomanagements

1. Grundlagen des Risikomanagements

Insbesondere die wirtschaftlichen Verwerfungen aufgrund der sogenannten „Dotcom-Blase“ sowie der in etwa zeitgleich aufgedeckten Bilanzfälschungen namhafter Unternehmen in den USA, aber auch Deutschland, führten um die Jahrtausendwende dazu, dass Anforderungen an die **Corporate Governance**, die Bewertung von Bilanzwerten und Risiken sowie deren Prüfung durch unabhängige Instanzen verschärft wurden. Maßgebliche, insbesondere für börsennotierte Unternehmen geltende Rechtsgrundlagen, sind seither:

- der sog. Sarbanes Oxley Act (SOX) in den USA,
- die EU-Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über die Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen (umgangssprachlich als Euro-SOX bezeichnet),

- die Regelungen des schweizerischen Obligationenrechts, insbesondere im Dritten Abschnitt (Rechnungslegung für größere Unternehmen).

Diese Regelwerke verlangen unter anderem eine Risikobeurteilung wesentlicher Risiken auf Basis einer nachvollziehbar dargestellten Methodik des Risikomanagements, wobei dabei vor allem auf Risiken erheblicher Tragweite einzugehen ist. Für einzelne Branchen gibt es zudem weitergehende Anforderungen und Standards, insbesondere in der Banken- und Versicherungsbranche.

Eng mit der Etablierung des Risikomanagements auf Basis der vorgenannten Rechtsgrundlagen ist auch die Bedeutung des sog. „**Compliance-Managements**“ gestiegen, welches die Einhaltung aller normativen Vorgaben durch Unternehmen und ihren handelnden Personen meint.²⁴ Wie Schünemann treffend darstellt, kann dies keinesfalls als selbstverständlich erachtet werden und muss durch entsprechende Managementsysteme und Maßnahmen erreicht werden.²⁵

Zur konkreten **Umsetzung des Risikomanagements** haben sich mittlerweile verschiedene **Standards** etabliert, wobei sich insbesondere

- die ISO 31000:2018 Risk Management-Guidelines sowie
- das Enterprise Risk Management – Integrated Framework der COSO (The Committee of Sponsoring Organizations of the Treadway Commission, eine US-amerikanische, private Organisation zur Verbesserung der Kontrollen im Finanz- und Rechnungswesen)

hoher praktischer Relevanz erfreuen. Ein klassischer Risikomanagement-Ansatz sieht dabei vor, dass die Risiken systematisiert und hinsichtlich ihrer Häufigkeit (falls bekannt) bzw. abgeschätzten Eintretenswahrscheinlichkeit sowie ihres Ausmaßes anhand zuvor definierter Ziele bzw. Kriterien beurteilt werden. Das diesbezügliche methodische Vorgehen ist in Gundel/Müllli (2009) ausführlich dargestellt und soll daher an dieser Stelle nicht wiederholt werden.²⁶ Darauf aufbauend können im Rahmen des Risikomanagements dann die korrespondierenden Maßnahmen festgelegt und umgesetzt werden, insbesondere Maßnahmen

- zur **Risikovermeidung** (z. B. Verzicht auf bestimmte Tätigkeiten und Aktivitäten),

24 Vgl. Schünemann (2012): Rechtliche Grundlagen der Unternehmenssicherheit, in: Stober/Olschok/Gundel/Buhl (2012), Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit, Stuttgart, S. 934–935.

25 Vgl. ebenda.

26 Vgl. Gundel/Müllli (2009): Unternehmenssicherheit, München, S. 17–73.

- zur **Risikominimierung** im Sinne konkreter Sicherheitsmaßnahmen oder
- zur **Risiküberwälzung auf Dritte** (Kunden, Lieferanten etc.) im Rahmen von Verträgen sowie insbesondere auf Versicherungen.

Ebenfalls Bestandteil des Risikomanagement-Prozesses ist schließlich die regelmäßige Überprüfung der Risikosituation und Wirksamkeit der ergriffenen Maßnahmen.

Die **tatsächliche Eignung des klassischen Modells des Risikomanagements** wird allgemein sowie spezifisch für die Unternehmenssicherheit regelmäßig **kritisch betrachtet**. Häufige Anmerkungen betreffen einerseits den als sehr theoretisch erachteten Vorgehensansatz, der trotz mitunter fehlender valider Daten zu Wahrscheinlichkeiten und Ausmaß eine „**Scheingenauigkeit**“ suggeriere und tatsächliche Risiken sowie deren Auswirkungen über- bzw. vor allem unterschätze. Die wohl populärste Kritik in diesem Sinne stammt vom Publizisten Nassim Nicholas Taleb, der mit seinem Buch „**Der Schwarze Schwan: Die Macht höchst unwahrscheinlicher Ereignisse**“ ins allgemeine Bewusstsein rief, dass (negative) Extremereignisse bei ihrem tatsächlichen Eintreten einen deutlich höheren Einfluss haben, als ihnen ex ante durch u. a. herkömmliche Risikoanalysen zugeschrieben wird.²⁷ Auch die oft abweichenden Ergebnisse sog. „Business Impact Analysen“ im Rahmen des Business Continuity Managements würden dafür sprechen, dass klassische Risikoanalysen nicht notwendigerweise eine realitätsgetreue Abbildung der „größten“ Sicherheitsrisiken ermöglichen. Spezifisch auf diese Sicherheitsrisiken wird andererseits angeführt, dass die üblichen Methoden des Risikomanagements die Unternehmensrisiken typischerweise finanziell abbilden und somit für die Unternehmenssicherheit weniger geeignet erscheinen bzw. deren Risiken unterbewerten.²⁸

Tatsächlich stellt eine passgenaue Anwendung auf die im Sinne der Unternehmenssicherheit relevanten Risiken sowie Einbettung in das allgemeine, unternehmerische Risikomanagement erfahrungsgemäß eine individuell zu lösende Herausforderung dar. Dennoch ist es aus Sicht der Autoren ein methodisch sauberer und durchaus praxiserprobter Ansatz, der überhaupt erst eine risikogerechte Gestaltung der Unternehmenssicherheit, ihrer Handlungsschwerpunkte und Maßnahmen erlaubt.

²⁷ Vgl. Taleb (2007). *The Black Swan – The Impacts of the highly improbable*, New York.

²⁸ Vgl. Schmidt (2012): Umfang, Bedeutung und Ziele der Unternehmenssicherheit, in: Stober/Olschok/Gundel/Buhl (2012), *Managementhandbuch Sicherheitswirtschaft und Unternehmenssicherheit*, Stuttgart, S. 875.