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

BOORBERG

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

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

Inhaltsverzeichnis

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 risikominimerende 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** entspräche 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/Mülli (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 rückwärtsgewandte 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 unsichereren, 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 Einflusssphären (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 müss(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) Durchsetzungsinstanz international anerkannten 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.