

- EG/RL/65/2005 (Erhöhung der Gefahrenabwehr in Häfen). Dabei handelt es sich um die Etablierung eines europaweiten Systems der Gefahrenabwehr, das durch Hafensicherheitsgesetze der Bundesländer umgesetzt wurde.
- EG/VO/450/2008 (Zollkodex für zugelassene Wirtschaftsbeteiligte).

### 3. Sicherheit als Marktfunktion

#### a) Sicherheit als Aufgabe der Eigenverantwortung und der Unternehmenssicherheit

##### aa) Sicherheit als Folge der Privatautonomie

- 29 Insbesondere die Ausführungen zum europäischen Binnenmarkt haben verdeutlicht, dass Sicherheit nicht nur eine Angelegenheit von Staaten und Staatengemeinschaften ist. Vielmehr besteht **Sicherheit** auch aus **Waren und Dienstleistungen**, die auf einem Markt erbracht werden können, dem sog. **Sicherheitsmarkt** (s. u. A I 3 d).<sup>45</sup> Gegen diese Annahme scheint zwar zunächst zu sprechen, dass das Grundgesetz dem Staat das **Gewaltmonopol** zuweist. Es ist als Ausübung und Durchsetzung von Zwangsbefugnissen zu verstehen und Grundlage der Umsetzung rechtsstaatsrechtlichen Handelns. Dieses Monopol wird dem Staat eingeräumt, weil private Gewalt und mögliche Konflikte bereits im Vorfeld unterbunden werden sollen. Insofern dient das Gewaltmonopol der Prävention und Schadensabwendung. Es steht, abgesehen von speziell normierten Sondersituationen, nicht zur Disposition.

Die Wahrnehmung des Gewaltmonopols ist jedoch nur ein Ausschnitt aus dem vielfältigen Feld von Sicherheitsaufgaben. Sie müssen nicht sämtlich vom Staat und seinen Einrichtungen selbst erledigt werden.<sup>46</sup> Tatsächlich kennt die Rechtsordnung viele **Sicherheitsaufgaben**, die als **Privataufgabe** von Bürgerinnen und Bürgern sowie Unternehmen ausgestaltet sind. Diese Aufgaben wurzeln letztlich in der **Privatautonomie** und sind die Folge davon, dass Private Pflichten haben und **Verantwortung** für die von Ihnen verursachten Gefahren und Schäden übernehmen müssen. Klassisches Muster ist die **Eigenverantwortung** für die **Verkehrssicherheit** von Gebäuden, Einrichtungen und Wegen sowie die Verantwortung der Arbeitgeber für die **Arbeitssicherheit** (§ 823 und §§ 836 – 838 BGB).

##### bb) Kein staatliches Sicherheitsmonopol

- 30 In jüngerer Zeit baut die Gesetzgebung die **Eigenverantwortung der Unternehmen** im Interesse der **Prävention und Risikominimierung** aus. Die **Vorsorge** hat sich als allgemeines **Rechtsprinzip** etabliert.<sup>47</sup> D. h., dass zunehmend Sicherheitsaufgaben insbesondere auf Unternehmen mit dem Ziel übertragen werden, die **Eigenüberwachung und Eigensicherung** zu stärken. Folglich lässt sich schon an dieser Stelle als Zwischenergebnis festhalten, dass es **kein staatliches Sicherheitsmonopol** gibt. Es müsste auch scheitern, weil der Staat und seine Einrichtungen nicht in der Lage sind, in sämtlichen Bereichen umfassend Sicherheit zu garantieren. Moderne Repräsentanten dieser Entwicklung sind die **technische Sicherheit**, die in zahlrei-

---

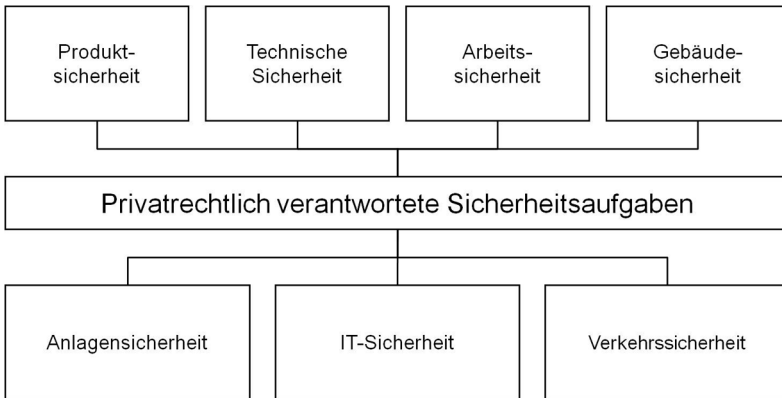
45 Der Begriff Sicherheitsmarkt wird auch von *Pitschas, Rainer*: in: Festschrift für Wolf-Rüdiger Schenke, 2011, S. 481, 491 verwendet.

46 Siehe auch die Antwort der Bundesregierung auf eine Große Anfrage zum Einsatz privater Militär- und Sicherheitsfirmen, BTDrucks 17/6780 v. 9. 8. 2011.

47 Siehe näher *Thiel, Markus*: Die „Entgrenzung“ der Gefahrenabwehr, Tübingen 2011, S. 75 ff.

chen von Privaten geschaffenen Regelwerken (DIN-Normen) und insbesondere im Anlagen- und Produktsicherheitsrecht ihren Niederschlag gefunden hat (§ 4 GPSG; § 58a BImSchG), die teilweise als „Grundpflichten“ ausgestalteten **Vorsorgepflichten** (§ 41 Thüringer Brand- und Katastrophenschutzgesetz) oder das **Eigensicherungsmodell** für die Hafensicherheit in NRW.<sup>48</sup>

In Anlehnung an das Schaubild „Sicherheit als offener Brücken- und Verbundbegriff“ (vgl. RdNr. 13, Bild 4) lassen sich in der nachfolgenden Übersicht u. a. folgende Aufgabenbereiche für privatrechtlich verantwortete Sicherheitsaufgaben ableiten. 31



**Bild 7:** Privatrechtlich verantwortete Sicherheitsaufgaben

**cc) Eigensicherungspflichten und Sicherheitsmanagement**

Insgesamt zeigen die Beispiele und Aufgabenfelder, dass Unternehmen zur Realisierung gemeinwohlorientierter Sicherheitsinteressen erheblich in die Pflicht genommen (sog. **Indienstnahme**)<sup>49</sup> werden, ohne dass sie dabei Staatsaufgaben erledigen oder hoheitliche Befugnisse wahrnehmen.<sup>50</sup> So heißt es etwa generalisierend im Programm Innere Sicherheit, Fortschreibung 2008/2009 der Ständigen Konferenz der Innenminister und -senatoren unter Punkt V 1:

„... wird privaten Organisationen und Personen grundsätzlich eine höhere Gefahrenvorsorge aberlangt, wenn ihr Handeln gefahren erhöhend wirken kann.“

Konkretisierend auf einzelne Sicherheitsfelder bedeutet das beispielhaft: Gefahrenvorbeugung durch Eigensicherungspflichten von Flughäfen nach §§ 5 LuftSiG, von

48 Siehe näher *Thiel, Markus*: Die „Entgrenzung“ der Gefahrenabwehr, Tübingen 2011, S. 127 ff.

49 Näher *Waechter, Kay*: Verwaltungsrecht im Gewährleistungsstaat, Tübingen 2008, S. 129 ff.

50 *Nünke, Anja*: Verwaltungshilfe und Inpflichtnahme des Sicherheitsgewerbes, Hamburg 2005, S. 103 ff.; *Fischer, Uwe Christian*: Sicherheitspartnerschaften zwischen Staat und Wirtschaft, in: *Borchert, Heiko* (Hrsg.), Wettbewerbsfaktor Sicherheit, Baden Baden 2008, S. 36 ff.; *Schoch, Friedrich*: Privatisierung polizeilicher Aufgaben, in: *Wirtschaft-Recht-Verwaltung*, FS Rolf Stober, Köln 2008, 559, 563; *Braun, Frank*: Privatisierung der Polizei, in: *Die Polizei*, 2008, S. 350, 353 f.; *Thiel, Markus*: Die „Entgrenzung“ der Gefahrenabwehr, Tübingen 2011, S. 125 ff.; OVG Bremen, Urteil v. 31. 10. 2006, AZ. 1D 41/06, Nord ÖR 2007, S. 177.

Industrieunternehmen durch Vorhaltung eines Werkschutzes, von Handelsunternehmen durch Beschäftigung eigener Detektive, von Dienstleistungsunternehmen wie Reiseveranstaltern durch Einschaltung von Sicherheitsberatern, von Schiffseigentümern und Eigentümern von Hafenanlagen gegen Terrorismus/Piraterie gemäß der VO EG/725/2004 und der RL EG/65/2005 sowie der Hafensicherheitsgesetze der Bundesländer oder von Energieunternehmen nach § 7 Abs. 2 Nr. 5 AtG (hinsichtlich der Pflicht zur Einführung eines mit Faustfeuerwaffen ausgestatteten Objektsicherungsdienstes<sup>51</sup>).

Und unter Punkt XIV 3 des Programms Innere Sicherheit Fortschreibung 2008/2009 der Ständigen Konferenz der Innenminister und -senatoren der Länder, S. 64, wird ausgeführt:

„Für den Schutz kritischer Infrastrukturen ist die Zusammenarbeit aller staatlichen Ebenen noch weiter zu intensivieren. Private Betreiber von Infrastruktureinrichtungen sind entsprechend ihrer Verantwortlichkeit einzubinden.“

- 33 Aus dieser besonderen Erwähnung der Privatwirtschaft in einem Sicherheitsprogramm lässt sich entnehmen, dass die Sicherheitsaufgaben für Unternehmen künftig wachsen werden.

Gleichzeitig liegt es im wohlverstandenen Eigeninteresse der Unternehmen, dass sie auf **hohem Sicherheitsniveau** und nach **anerkannten Sicherheitsstandards** arbeiten. Denn das ist eine zentrale Bedingung für einen langfristigen Unternehmenserfolg. Wesentliches Element einer sicheren Unternehmensführung ist in diesem Zusammenhang nach modernem Verständnis ein wirkungsvolles **Sicherheitsmanagement** für die **Corporate Security** einschließlich der **Standort- oder Site Security** (s. Kapitel D II. 2.). Es spiegelt die Eigenverantwortung des Unternehmens im Rahmen der Eigensicherungs- und Eigenüberwachungspflichten.<sup>52</sup>

- 34 In diesem Sinne ist **Sicherheitsmanagement** die Gesamtheit der Tätigkeiten zur Planung, Organisation, Leitung und Kontrolle von Personen und Arbeitsaktivitäten im Hinblick auf die effiziente Erreichung einer hohen Sicherheitsleistung, d. h. zur Erreichung einer hohen Qualität aller für die Sicherheit bedeutsamen Tätigkeiten. Sicherheitsmanagement bildet ein Instrument zur Erfüllung der durch Gesetze, Rechtsverordnungen und Verwaltungsakte festgelegten Anforderungen an den Anlagenbetrieb.<sup>53</sup>

Zusammengenommen lassen diese Ausführungen erkennen, welche Rolle der Unternehmenssicherheit in der Praxis zukommt. Es besteht eine **Verantwortungsteilung zwischen Staat und Unternehmen**. Dementsprechend lässt sich **Unternehmenssicherheit** definieren als den internen Schutz von Personen, Objekten, Transporten und anderen Werten privater Unternehmen.

- 35 Der **Schutz von Personen** meint die Beschäftigten einschließlich der Leitungsebene, die Kooperationspartner, die innerhalb des Unternehmens Leistungen erbringen

---

51 BVerwGE 81, 185, in: NVwZ 1989, S. 864 ff.

52 Otten, Wolfgang: Eigensicherung, Köln 2006.

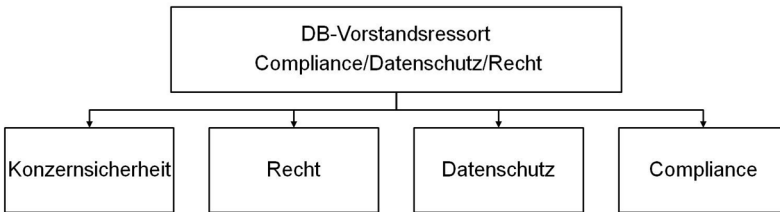
53 Grundlagen für Sicherheitsmanagementsysteme in Kernkraftwerken v. 27. 7. 2004, Bundesanzeiger Nr. 138, S. 16275; s. auch Müller, Klaus-Rainer: Unternehmenssicherheit, Wiesbaden 2005; von zur Mühlen, Rainer: Sicherheits-Management, Stuttgart 2006; Gundel, Stephan/Müll, Lars: Unternehmenssicherheit, München 2009; Gundel, Stephan: Supply Chain Security Management, in: Stober, Rolf (Hrsg.): Sicherheitsgewerbe und Unternehmenssicherheit, Köln 2011, S. 55 ff.

(z. B. Subunternehmer) sowie die Verbraucher, die von den Leistungen profitieren (z. B. Einzelhandel). Der **Schutz von Objekten** meint die Gebäude, die Produktionsanlagen, die Lagerhaltung und die Standorte des Unternehmens. Der **Schutz von Werten** betrifft vornehmlich immaterielle Werte wie Patentschutz, Software, Verfahren, Know-how und Good Will, die vor unbefugten Zugriffen bewahrt werden müssen.

**dd) Unternehmenssicherheit als Herausforderung für das Compliance-Management**

Das Thema Unternehmenssicherheit wird in jüngerer Zeit des Öfteren mit dem Stichwort **Compliance-Management** in Verbindung gebracht.<sup>54</sup> Diesem Zusammenhang kann man sich am besten nähern, wenn man die Organigramme von Großunternehmen betrachtet, bei denen Konzernsicherheit und **Compliance** unter einem organisatorischen Dach und eventuell mit der gemeinsamen Verantwortung eines Vorstandsmitgliedes zusammengefasst sind.

36



**Bild 8:** Organigramm der Deutschen Bahn

Die Frage nach Schnittmengen zwischen Sicherheit und Compliance lässt sich nur nach einer Klärung des Begriffes Compliance zuverlässig beantworten. Compliance meint Rechts- und Regelkonformität, das heißt die Übereinstimmung des Handelns der Unternehmensführung (Vorstand, Aufsichtsrat, Gesellschafter), der Beschäftigten und anderer in den Betriebsablauf eingebundener Personen (z. B. Lieferanten, Subunternehmen) mit der Rechtsordnung sowie betrieblichen und anderen Regeln.<sup>55</sup> Legt man diese Definition zugrunde, dann gibt es auf den ersten Blick scheinbar keine Überschneidungen mit dem Sicherheitsbegriff, da Compliance primär auf gute Unternehmensführung abstellt. Überlappungen existieren aber insoweit, als die Sicherheit auch den regelhaften Ablauf betrieblicher Prozesse betrifft und sie deshalb letztlich essentieller Bestandteil einer verantwortungsvollen Unternehmensleitung ist. Das sollen die nachfolgenden Erläuterungen aufzeigen:

37

- Im Rahmen der Rechtskonformität ist sicherzustellen, dass gesetzliche Anforderungen hinsichtlich konkreter organisatorischer oder sonstiger Sicherheitsmaßnahmen erfüllt werden.

<sup>54</sup> *Sorge, Michael:* Compliance und Security müssen Partner sein, in: Security Insight 3/11, S. 8 ff.; *Remberg, Meinhard:* Angst oder Überzeugung, Wirtschaftsschutz und Sicherheitstechnik, in: W&S; August 2011, S. 14 ff.; WIK-Sicherheits-Enquête 2010/2011, in: WIK 3/11, S. 76.

<sup>55</sup> Siehe dazu *Keller, Rainer/Schünemann, Wolfgang/Stober, Rolf* (Hrsg.), Compliance-Textsammlung, Köln 2011.

- Rechtskonformität und Unternehmenssicherheit können sich wechselseitig ergänzen und verstärken.
- Die Verhinderung und Bekämpfung von Unternehmenskriminalität (Betrug, Untreue, Korruption) fällt in die gemeinsame Verantwortung beider Bereiche.
- Maßnahmen der Unternehmenssicherheit können der Rechtskonformität widersprechen oder die Rechtskonformität erhöhen.

**38** Im Bereich „**Safety**“ (**Arbeitssicherheit, Technische Sicherheit, Brandschutz, Störfallvorsorge**, usw.) haben Unternehmenssicherheit und Compliance gemeinsam dafür zu sorgen, dass die einschlägigen gesetzlichen Bestimmungen eingehalten werden.<sup>56</sup> Man denke nur an die öffentliche Auftragsvergabe von Sicherheitsleistungen, wonach von dem Auftragnehmer u. a. verlangt wird, dass er „gesetztreu“ ist (§ 97 Abs. 4 GWB). Im Bereich „**Security**“ besteht aus Sicht der Unternehmenssicherheit der Wunsch nach umfassender Überwachung zur Aufklärung von Schadensfällen durch Videoüberwachung. Gleichzeitig muss das Compliance-Management, etwa bei der Sammlung und Auswertung von Daten, die Grenzen des § 6 b BDSG einhalten. Danach ist eine Videoüberwachung nur zulässig und damit compliant, wenn sie zur Wahrnehmung des Hausrechts oder anderer berechtigter Interessen erfolgt. Bei einer prozessorientierten Betrachtung der Wertschöpfungskette stehen deshalb **Sicherheit und Compliance** nicht in einem Wettbewerbs- sondern in einem **Kooperations- und in einem Komplementärverhältnis**.

## **b) Sicherheit als Aufgabe der Sicherheitswirtschaft**

### **aa) Sicherheitswirtschaft als Faktor ökonomischer Arbeitsteilung**

- 39** Unternehmer, Eigentümer, Besitzer, Pächter usw. müssen die ihnen obliegende Sicherheitsverantwortung in Gestalt von Eigensicherungs- und Überwachungspflichten nicht selbst erfüllen. Sie können im Rahmen der **ökonomischen Arbeitsteilung** andere Unternehmen oder Personen mit dem Schutz ihrer Sicherheitsinteressen (Leben, Gesundheit, Eigentum, Besitz) beauftragen. Dabei handelt es sich um **Sicherheitsunternehmen**, die vielfältige Sicherheitsleistungen zur Gefahrenabwehr und Risikovorsorge für die jeweiligen Auftraggeber auf privatrechtlicher Basis erbringen.<sup>57</sup> Die nachfolgende Übersicht vermittelt einen ersten generalisierenden Eindruck der Haupteinsatzgebiete:
- Objekt- und Werksicherheit,
  - Transport- und Logistiksicherheit,
  - Personen- und Veranstaltungssicherheit,
  - IT- und Datensicherheit,
  - Notrufsicherheit.
- 40** Insbesondere für Unternehmen liegen die Gründe für die Auslagerung von Sicherheitsdienstleistungen, das sogenannte **Outsourcen der Sicherheit**, auf der Hand, weil es Sinn macht, sich auf die jeweiligen Kernkompetenzen zu konzentrieren.

---

<sup>56</sup> Siehe den Codes of Conduct der Siemens AG unter Punkt F, abgedruckt in: *Keller, Rainer/Schünemann, Wolfgang/Stober, Rolf* (Hrsg.), *Compliance Textsammlung*, Köln 2011, S. 507 ff.

<sup>57</sup> Siehe schon *Wackerhagen, Rolf*: Die Zukunft liegt in der Fremdvergabe und Privatisierung öffentlicher Sicherheitsaufgaben, in: *Der Sicherheitsdienst 2001*, S. 157 ff.

Und Politiker wie Behörden können auf der Grundlage positiver Ergebnisse einer solchen Analyse in der Überzeugung gestärkt werden, dass das Sicherheitsgewerbe künftig ein verlässlicher und kompetenter Partner der Polizei sein wird.

### c) Methodik

#### 3 **Zukunftsanalysen** können nach verschiedenen Methoden erfolgen:

- Bei der sog. Szenario-Methode werden Einflussfaktoren bestimmt, beschrieben und alternative Annahmen für ihre künftige Ausprägung unter prozentualer Angabe der Eintrittswahrscheinlichkeit festgelegt. Alle Entwicklungsannahmen aller Faktoren werden in einer formalisierten Wechselwirkungsanalyse aufeinander bezogen und mittels einer Rechnersoftware daraus **Szenarien-“Gerüste“** errechnet. Je mehr dieser „Gerüste“ identisch oder ähnlich sind, umso wahrscheinlicher ist das ihnen entsprechende Szenario. Aus anderen Gerüsten lassen sich alternativ andere Zukunftsszenarien entwickeln.
- Weniger aufwändig ist die **Trendmethode**. In Zeitreihen vorliegende Messwerte werden trendhaft in die Zukunft hinein verlängert. Voraussetzung ist die anzunehmende Stabilität der die Zeitreihe bestimmenden Einflussfaktoren.
- Verknüpft werden kann mit dieser Methode die Befragung von Experten in den einschlägigen Wissensgebieten, im vorliegenden Zusammenhang vor allem die Befragung von Experten der Unternehmenssicherheit, des Sicherheitsgewerbes und der Öffentlichen Sicherheit. Eine solche Befragung kann durch formatierte Umfragen ebenso erfolgen wie durch qualitative Interviews. Die Ergebnisse müssen mit anderen Quellen abgeglichen werden. Die Aufrichtigkeit der Antworten und Stellungnahmen lässt sich durch eindeutige Fragestellungen und durch Abgleich der Antworten auf verschiedene Fragen überprüfen.

Die in diesem Beitrag erstellten **Zukunftsanalysen** basieren im wesentlichen auf der Trendmethode und Befragungen.<sup>1</sup> Die Ergebnisse wurden mit fachliterarischen Analysen und Annahmen abgeglichen.<sup>2</sup>

## 2. Einflussfaktoren für die Entwicklung des Sicherheitsgewerbes

#### 4 Eine Analyse künftiger Entwicklungen muss auf der bisherigen Entwicklung und dem Status quo aufbauen. Über das Sicherheitsgewerbe hinaus werden dabei auch die **wichtigsten Rahmenbedingungen** betrachtet:

- Die Sicherheitslage, insbesondere Kriminalitätsbereiche, zu deren Prävention Sicherheitsunternehmen eingesetzt werden,
- die wirtschaftliche Entwicklung, die die Bereitschaft beeinflusst, kostenträchtige Sicherheitsmaßnahmen zu veranlassen,
- der Schutzbedarf von Unternehmen und Organisationen, der auch vom Sicherheitsgefühl abhängig ist,
- Rechtsnormen, die sowohl Sicherheitsmaßnahmen vorschreiben, begrenzen, oder die das Sicherheitsgewerbe direkt betreffen,

---

1 Im Zweijahresabstand durchgeführte Sicherheits-Enquete der WIK – Zeitschrift für die Sicherheit der Wirtschaft, SecuMedia VerlagsGmbH; *Lünendonk-Studie 2010: Führende Sicherheitsdienstleister in Deutschland*, Lünendonk GmbH 2010.

2 Vor allem *Glavic, Jürgen* (Hrsg.): *Handbuch des privaten Sicherheitsgewerbes*, Stuttgart 1995; *Sto-ber, Rolf/Olschok, Harald* (Hrsg.): *Handbuch des Sicherheitsgewerberechts*, München 2004; *Olschok, Harald* (Hrsg.): *Jahrbuch Unternehmenssicherheit*, Köln 2010 und 2011.

- das Ausmaß der Belastung der Polizei und ihre Bereitschaft, Aufgaben dem Sicherheitsgewerbe zu übertragen,
- die Bereitschaft von Kommunen, die Sicherheit ihrer Bürger über polizeiliche Maßnahmen hinaus zu erhöhen, vor allem in ihren Hausrechtsbereichen,
- die Einstellung von Gesellschaft und Politik zum Sicherheitsgewerbe und die damit verknüpfte Bereitschaft, bestimmte Funktionen der Öffentlichen Sicherheit durch Sicherheitsunternehmen wahrnehmen zu lassen.

**a) Sicherheitslage**

Die Sicherheitslage hat sich in den letzten Jahrzehnten unterschiedlich entwickelt. Der die Sicherheit der Bundesrepublik Deutschland schwer belastende Terrorismus der RAF und anderer terroristischer Organisationen ist vor etwa zwei Jahrzehnten beendet worden. Dem internationalen **islamistischen Terrorismus** ist zwar in Deutschland noch kein folgenschwerer Anschlag gelungen – sieht man von der Tötung von zwei US-Soldaten am Frankfurter Flughafen im März 2011 durch einen Kosovaren ab, der durch das Verbrechen verhindern wollte, dass die Soldaten in Afghanistan zum Einsatz kommen. Insgesamt hat aber der islamistische Terrorismus in seiner **Bedrohlichkeit nicht nachgelassen**. Ob die erst 2011 entdeckte mehr als 12jährige Mordserie der Gruppe „Nationalistischer Untergrund“ (NSU) den Anfang eines neuen Rechtsterrorismus oder eher die singuläre Entwicklung einer Mörderbande darstellt, lässt sich im derzeit bekannten Ermittlungsstadium noch nicht abschätzen.

Die Kriminalitätsbelastung ist beständig leicht zurückgegangen. Die **Häufigkeitszahl**<sup>3</sup> betrug

1993	8.337
1998	7.869
2003	7.963
2008	7.436
2011	7.328

Zurückgegangen sind insbesondere Deliktsarten, zu deren **Prävention vor allem das Sicherheitsgewerbe** eingesetzt wird:

	<b>schwerer Diebstahl</b>	<b>einfacher Diebstahl</b>
1993	2.545.000	1.606.000
2011	1.113.000 (./ 56 %)	1.290.500 (./ 18 %)

Raubüberfälle auf Banken und Poststellen sind von 1998 bis 2011 von 1016 auf 324 gesunken, Raubüberfälle auf Geld- und Werttransporte in dieser Zeitspanne von 224 auf 129.

Dagegen ist der Betrug seit 1993 um 76 % auf 935.000 Fälle gestiegen.

Insgesamt ist in den vergangenen Jahren tendenziell die physische Kriminalität (soweit sie angezeigt wurde) eher zurückgegangen, die durch Täuschung, Miss-

---

<sup>3</sup> Zahl der angezeigten Verdachtsfälle von Straftaten je 100.000 Einwohner – also ohne Einpendler und Touristen – eines örtlichen Bereichs.

brauch und Ausspähung – also mit geistigen Mitteln – begangene Kriminalität eher angestiegen. Sicherheitsdienstleistungen und Sicherheitstechniken, die diese Kriminalitätsphänomene abwehren, sind daher in den letzten Jahren besonders gefordert.

### b) Volkswirtschaftliche Entwicklung

- 8 Trotz Phasen eines zeitweiligen wirtschaftlichen Abschwungs
- 1967 nach Abschluss des Wiederaufbaus nach 1945,
  - 1973 bis 1975 nach dem weltweiten Ölschock,
  - 1982 nach der Ölkrise infolge der iranischen Revolution und dem iranisch-irakischen Krieg,
  - 1993 nach der deutschen Vereinigung (mit einem Rückgang des BSP um 0,8 %),
  - 2003 nach dem Platzen der „Internet-Blase“ und als Reaktion auf 9/11,
  - 2008/2009 als Zuspitzung der globalen Finanzkrise
- war der Trend der deutschen Volkswirtschaft nicht nur in den Zeiten des „Wirtschaftswunders“ (1948 – 1966), sondern auch nach 1970 auf Wachstum ausgerichtet.

BSP <sup>4</sup>	bis zur Vereinigung	Zuwachs	preis- und saisonbereinigt (1991 = 100 %)
1970	361 Mrd. €	57 %	
1980	789 Mrd. €	+ 119 %	76 %
1990	1.307 Mrd. €	+ 66 %	95 %
<b>BSP nach der Vereinigung</b>			<b>(2000 = 100 %)</b>
2000	2.012 Mrd. €	+ 54 %	100 %
2010	2.499 Mrd. €	+ 24 %	109 %

- 9 Diese insgesamt wachstumsorientierte volkswirtschaftliche Entwicklung bedeutete Zuwachs an industrieller Produktion, Handel, Export und Bautätigkeit mit der Folge eines zunehmenden Schutzbedarfs für Güter und Objekte und mit der wirtschaftlichen Fähigkeit, die zunehmende Beauftragung des Sicherheitsgewerbes mit diesen Schutzfunktionen zu finanzieren.

### c) Schutzbedarf von Unternehmen und Organisationen

- 10 Der Schutzbedarf von Unternehmen ist nach der Überzeugung der Manager in den Funktionsbereichen Unternehmenssicherheit und Sicherheitsdienstleistung<sup>5</sup> im vergangenen Jahrzehnt eher gestiegen, freilich vor allem für die IT-Sicherheit. Das lässt sich an den Ergebnissen der WIK-Sicherheitsenquete 2006/2007 und 2008/2009 ablesen.

So bezeichneten die Befragten als **aktuelle besondere Bedrohungsphänomene** (in einer Bewertungsskala von 1(niedrigste) bis 6 (höchste Bewertung))<sup>6</sup>

4 Bruttosozialprodukt.

5 WIK-Sicherheits-Enquete 2006/2007, in: WIK 1/07, S. 7/8; 2/07 S. 8–12; WIK-Sicherheits-Enquete 2008/2009, in: WIK 2/09 S. 10–15; WIK-Sicherheits-Enquete 2010/2011 in: WIK 2/11 S. 12–16.

6 WIK-Sicherheits-Enquete 2006/2007, in: WIK 1/07, S. 8; ab 2008/2009 wurden differenziertere Deliktskategorien bewertet.



	1998	2006
Massendelikte (Diebstahl etc.)	4,3	3,7
Organisierte Kriminalität	3,7	3,4
Wirtschaftsspionage	3,1	2,7
Produktpiraterie	3,4	3,7
Korruption	3,5	3,7
Internetkriminalität	3,8	4,2

Und auf die Frage, in welchen Funktionsbereichen die Ausgaben im Sicherheitsbudget steigen, gaben in der WIK-Sicherheits-Enquete 2006/2007 einerseits und 2010/2011 andererseits an:<sup>7</sup> **11**

	2006/2007	2010/2011
IT-Sicherheit	87,4 %	86,9 %
Datenschutz	72,5 %	77,0 %
Informations-/Geheimchutz	40,6 %	41,3 %
Brandschutz	28,6 %	26,6 %

Erheblich angewachsen ist von 2007 bis 2009 die angenommene Häufigkeit der Unternehmen (Prozentzahl der Befragten), bei denen Investitionen in die nachfolgenden sicherheitstechnischen Anlagen erwartet wurden: **12**

	2007–2009	2011–2013
Biometrie	34,3 %	42,2 %
IP-Einbindung der Sicherheitstechnik	26,5 %	37,3 %
Videoüberwachung	23,5 %	43,1 %
Verschlüsselung von Daten/Kommunikation	22,5 %	34,3 %
Brandmeldetechnik	14,7 %	27,5 %
Einbruchmeldetechnik	14,7 %	25,5 %
Alarmierungssysteme	13,7 %	27,5 %

#### d) Rechtsnormen und technische Regelwerke

Das Recht und die Normung haben die Entwicklung des Sicherheitsgewerbes in mehrfacher Hinsicht beeinflusst<sup>8</sup>: **13**

- a) – Die Erweiterung der Unterrichtung und die Einführung des **Sachkundenachweises** für bestimmte Tätigkeiten im öffentlichen Bereich im Jahr 2003 haben zur Qualifizierung der Beschäftigten von Sicherheitsunternehmen beigetragen.

<sup>7</sup> WIK-Sicherheits-Enquete 2006/2007, in: WIK 2/07; S. 9; WIK 2/11, S. 14.

<sup>8</sup> Im Einzelnen Peilert, Andreas: Das Datenschutzrecht des Sicherheitsgewerbes und Videoüberwachung, in: Stober, Rolf/Olschok, Harald (Hrsg.): Handbuch des Sicherheitsgewerberechts, München 2004, S. 223 ff.; Rupprecht, Reinhard/Rieche, Helmut: Rechtliche Rahmenbedingungen und Technische Regelwerke für den Einsatz von Sicherheitstechnik, in: Handbuch des Sicherheitsgewerberechts, München 2004, S. 296 ff.

- Die Einführung des Ausbildungsberufs „**Fachkraft für Schutz und Sicherheit**“ im Jahr 2002 hat die Tätigkeit im Sicherheitsgewerbe attraktiver gemacht. Ähnliches gilt für die Nachfolgerregelung für die „**Geprüfte Schutz- und Sicherheitskraft IHK**“ am 1. Januar 2006.
  - Die Einführung von Studiengängen für **Sicherheitsmanager** seit 1999 an mehreren Fachhochschulen professionalisiert den Führungskräftenachwuchs im Sicherheitsgewerbe.
- b) Das **Datenschutzrecht** schränkt die Tätigkeit des Sicherheitsgewerbes ebenso wie den Einsatz von Sicherheitstechnik dort ein, wo das Recht von Personen auf Datenschutz und informationelle Selbstbestimmung verletzt werden kann. Das gilt für die Kontrolle von Personen und vor allem für die Videoüberwachung im öffentlichen Raum ebenso wie für die Überwachung von Mitarbeitern im Unternehmen.
- c) **Technische Regelwerke** (Normen und technische Richtlinien) haben in den zurückliegenden Jahrzehnten zunehmend den Einsatz von Sicherheitstechnik erleichtert und zugleich sicherheitstechnische Investitionen gefördert. Soweit diese Technik von Sicherheitsunternehmen angeboten und betrieben wird, wird dadurch der Umsatz dieser Unternehmen gesteigert. Auch international dient die Normung als Marktöffner für die deutsche Sicherheitswirtschaft.<sup>9</sup> Mit der **Koordinierungsstelle Sicherheitswirtschaft** (KoSi) hat das DIN eine Plattform geschaffen, Normung und Standardisierung frühzeitig für die Gestaltung des zivilen Sicherheitsmarktes zu nutzen. Die KoSi berät die interessierten Kreise bei der Zusammenarbeit in Normungs- und Standardisierungsprozessen zur besseren Vertretung deutscher Interessen auf internationaler Ebene.
- 14 Es gibt eine Vielzahl von Normungsaktivitäten im Sicherheitsbereich. Sowohl die zeitlichen Phasen vor, während wie nach einem sicherheitsrelevanten Ereignis und Zuständigkeits- wie Funktionsbereiche sollen mit Normen erfasst werden.<sup>10</sup> Deutsche Normungsgremien sind
- der Normenausschuss Feuerwehrwesen (FNFW) im DIN<sup>11</sup>
  - der Normenausschuss Dienstleistungen (NADL) als Spiegelausschuss zu den CEN/TC-Gremien<sup>12</sup> für Transport-Logistik und Sicherheit von Lieferketten
  - die Kommission Elektrotechnik Elektronik Informationstechnik (DKE) im DIN und VDE<sup>13</sup>
  - die Kommission Transportkette (KTK) für Schiene und Straße, Luft- und Schifffahrt
  - der Normenausschuss Informationstechnik und Anwendung (NIA) als Spiegelausschuss zum Internationalen Komitee ISO/EC JTC 1/SC 27 (Information technology – Security techniques) mit den Arbeitsgruppen für Information Security Management Systems, Cryptography and Security Mechanisms, Security

---

9 Inga Schlüter: Koordinierungsstelle Sicherheitswirtschaft im DIN, in: DSD, 3/11, S. 10,11.

10 Im einzelnen Hövel, Albert: Nationale und Internationale Normung in der Unternehmenssicherheit – Sicherheitswirtschaft inklusive IT-Sicherheit, in: Olschok, Harald (Hrsg.): Jahrbuch Unternehmenssicherheit, Köln 2011, S. 113 ff.

11 Deutsches Institut für Normung e. V.

12 Europäisches Komitee für Normung/Technisches Komitee.

13 Verband der Elektrotechnik Elektronik Informationstechnik.

### 3. Normung

*Dipl.-Ing. Gerhard Henninger und Dipl.-Ing. Henryk Sieradzki,  
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik  
im DIN und VDE, Frankfurt/Main*

#### a) Einleitung

47 Die Normung wurde vor mehr als 100 Jahren von den am Wirtschaftsleben Beteiligten ins Leben gerufen, und zwar vor dem Hintergrund der Industrialisierung der Gesellschaft. Von Beginn an war der Aspekt der Sicherheit von hoher Bedeutung. Die Berücksichtigung der Sicherheit bezog sich darauf, den Endverbraucher vor möglichen **Folgen der Nutzung technischer Produkte** zu schützen.

Normen haben sich als ein wesentliches Instrument für die Unternehmen, aber auch für die Gesellschaft, zur Generierung von technischem Fortschritt entwickelt. Normen sind elementar für die Öffnung von Märkten und haben eine hohe Bedeutung für den freien Handel.

Durch Normung lassen sich hervorragende Leistungs- und Kostenvorteile generieren. Unzureichendes Wissen über Normung ist längst ein veritabler Nachteil in der betriebswirtschaftlichen Wettbewerbspositionierung. Normung spielt sich seit langem nicht mehr nur im Bereich ingenieurtechnischer Intelligenz ab: mannigfaltige Schnittstellen zum Recht heben das Thema auf ein Niveau, das vielen Unternehmen oft zu spät bekannt wird, nämlich dann, wenn bereits der Schadensfall eingetreten ist.

Gerade die industriepolitische Rechtsetzung der *Neuen Konzeption* zeigt die große **Steuerungskraft technischer Normung**. Wer da bei Normen noch schlicht an DIN A4 denkt, übersieht leicht die enormen betriebs- wie volkswirtschaftlichen Steuerungsmöglichkeiten des Normungswesens.

Dieser Abschnitt soll einen Überblick geben, wie Normen entstehen und wie sie die Rahmenbedingungen der Wettbewerbspositionierung verändern. Dem Leser soll der Einstieg in diese Materie erleichtert werden und die Darstellung der verschiedenen Mechanismen, die auf die Normung einwirken oder durch die Normung beeinflusst werden, soll dazu anregen sich intensiver mit der bedeutenden Rolle der Normung für die Sicherheitswirtschaft zu beschäftigen.

#### b) Wie Normen entstehen

##### aa) Normungsorganisationen

48 Die **Normungsorganisationen** sind auf drei Aktionsebenen tätig – national, europäisch (regional) und international. Auf allen drei Ebenen sind unterschiedliche Organisationen für die Normung in den Bereichen Allgemeine Normung (nicht-elektrotechnisch), Elektrotechnik und Telekommunikationstechnik zuständig. Die folgende Tabelle gibt einen Überblick der Organisationen, wobei auf nationaler Ebene exemplarisch die deutschen Normungsorganisationen dargestellt sind.

Normung	national	europäisch	international
Allgemein	DIN	CEN	ISO
Elektrotechnik	DKE	CENELEC	IEC
Telekommunikationstechnik	DKE	ETSI	ITU

**Tabelle 1:** Übersicht der zuständigen Normungsorganisationen

Das **DIN** (Deutsches Institut für Normung e. V.) ist die zuständige Normungsorganisation für Deutschland. Dies beruht auf dem zwischen dem DIN (gegründet 1917) und der Bundesregierung am 5. Juni 1975 geschlossenen Vertrag, dem sog. „Normenvertrag“. Das DIN vertritt die deutschen Interessen in den europäischen und internationalen Normungsorganisationen im Bereich der nicht-elektrotechnischen Normung.

Die **DKE** (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE) wurde durch den Vertrag vom 13. Oktober 1970 gegründet und ist ein gemeinsames Organ des DIN und des VDE (gegründet 1893). Die DKE vertritt die deutschen Interessen in den europäischen und internationalen Normungsorganisationen im Bereich der elektrotechnischen Normung.

Der **VDE** (Verband der Elektrotechnik Elektronik Informationstechnik e. V.) ist ein technisch-wissenschaftlicher Verein und verfolgt ausschließlich und unmittelbar gemeinnützige Zwecke.

**CEN** (Europäisches Komitee für Normung) wurde 1961 gegründet und befasst sich auf europäischer Ebene mit nicht-elektrotechnischer Normung. Im CEN sind die nationalen Normungsorganisationen der EU- und EFTA-Länder sowie deren Beitrittskandidaten vertreten.

**CENELEC** (Europäisches Komitee für elektrotechnische Normung) wurde 1972 als Nachfolgeorganisation von drei bestehenden Organisationen gegründet und befasst sich auf europäischer Ebene mit elektrotechnischer Normung. Im CENELEC sind die nationalen Normungsorganisationen der EU- und EFTA-Länder sowie deren Beitrittskandidaten vertreten.

**ETSI** (Europäisches Institut für Telekommunikationsnormung) wurde 1988 gegründet und befasst sich auf europäischer Ebene mit Normung auf dem Gebiet der Telekommunikationstechnik und angrenzenden Themengebieten. Mitglieder des ETSI sind Hersteller, Verwaltungen, Dienstanbieter, Netzbetreiber und Anwender.

**ISO** (Internationale Organisation für Normung) wurde in ihrer heutigen Form 1946 gegründet und befasst sich weltweit mit nicht-elektrotechnischer Normung.

**IEC** (Internationale Elektrotechnische Kommission) wurde 1906 gegründet und befasst sich weltweit mit Normung auf dem Gebiet der Elektrotechnik und Elektronik.

Die **ITU** (Internationale Fernmeldeunion) geht zurück auf den am 17. Mai 1865 gegründeten Internationalen Telegraphenverein und befasst sich weltweit mit Aspekten der Telekommunikation. Innerhalb der ITU werden die meisten technischen Spezifikationen (streng genommen „Empfehlungen“, englisch „recommendations“) von der ITU-T (Telecommunication Standardisation Sector) verabschiedet.

Abschließend ist festzustellen, dass durch die zunehmende Technikkonvergenz, die Grenzen zwischen den Zuständigkeiten und Aufgaben der Normungsorganisationen immer mehr verschwimmen und fachübergreifende Normungsprojekte in allen Organisationen üblich sind.

## bb) Der Normungsprozess

Der nationale **Normungsprozess** durchläuft in der Regel fünf Phasen:

- Normungsantrag (Initiierung durch jedermann, Annahme ausgerichtet am Bedarf der Wirtschaft);
- Erarbeitung des Norminhalts und -textes (im Fachgremium unter Einhaltung von Grundsätzen und Regeln);

- Veröffentlichung eines Norm-Entwurfs (Norminhalt wird in der Entwurfsfassung der Öffentlichkeit zur Kommentierung vorgestellt, z. B. über Kommentierungsportale);
- Einspruchsverfahren (zur Behandlung der zum Norm-Entwurf eingegangenen Einsprüche aus der Öffentlichkeit; im Bedarfsfall unter Einbeziehung eines Schlichtungs- und Schiedsverfahrens);
- Veröffentlichung der Norm (DIN-Normen, elektrische Sicherheitsnormen mit VDE-Klassifikation).

**51** Die nationalen Normungsorganisationen sind zuständig für die **Übernahme europäischer und internationaler Normen**, welche nach festgelegten Regeln erfolgen. Für europäische Normen (EN) besteht eine Übernahmeverpflichtung in das nationale Normenwerk, die Übernahme internationaler Normen ist freiwillig. Hieraus ergibt sich auch die hohe Bedeutung der Ausarbeitung europäischer Normen bzw. der Übernahme internationaler Normen als europäische Normen (siehe auch Abschnitt 3.5). Die Mitarbeit auf europäischer oder internationaler Ebene erfolgt über die Mitarbeit in einem nationalen Gremium.

**cc) Grundprinzipien der Normungsarbeit**

**52** **Normung und Standardisierung** sollen der Allgemeinheit zugute kommen und nicht zu einem wirtschaftlichen Sondervorteil Einzelner führen. Deshalb arbeiten Normungsgremien unter Einhaltung folgender Grundsätze:

- Beteiligung aller interessierten Kreise (Zusammensetzung der Normungsgremien),
- Öffentlichkeit (z. B. Ankündigung der Normungsprojekte und öffentliches Einspruchsverfahren),
- Freiwilligkeit (freiwillige Beteiligung an der Normung und freiwillige Anwendung der Normen),
- Konsens (Akzeptanz des Ergebnisses),
- Einheitlichkeit und Widerspruchsfreiheit,
- Sachbezogenheit,
- Ausrichtung am Stand der Technik (z. B. regelmäßige Überprüfung der Normen),
- Ausrichtung an den wirtschaftlichen Gegebenheiten,
- Ausrichtung am allgemeinen Nutzen,
- Internationalität (Mitarbeit in europäischen und internationalen Normungsorganisationen).

**dd) Normen und Recht**

**53** Die Anwendung von Normen ist grundsätzlich freiwillig, sie kann aber durch Verweisung auf Normen in rechtsverbindlichen Regelungen zwingend oder durch Verweisung in Verträgen bindend werden.

Darüber hinaus sind Normen oft **anerkannte Regeln der Technik** und spiegeln den **Stand der Technik** wieder, wodurch sie bei der Beurteilung von Streitfällen eine bedeutende Rolle spielen. Im Rechtsstreit billigt ein Richter der DIN-Norm den Beweis des ersten Anscheins zu, d. h. er geht erst einmal vom korrekten Handeln des Normenanwenders aus bzw. von der Fehlerfreiheit des Produktes. Dies führt zu einer Beweislastumkehr, bietet aber keine absolute Sicherheit, denn das Anwenden von DIN-Normen alleine reicht gegebenenfalls nicht aus. **DIN-Normen** sind für den Regelfall ausgelegt und decken nicht alle denkbaren Fälle ab. Das führt zu der Situa-

tion, dass die Anwendung von DIN-Normen den Anwender nicht vom eigenverantwortlichen Handeln und den dazu notwendigen Fachkenntnissen befreit.

Gesetze schaffen den rechtlichen Rahmen und geben Schutzziele vor, Normen konkretisieren den **Stand der Technik** und schreiben ihn flexibel fort. Normen entlasten den Staat in seiner Gesetzgebungstätigkeit.

#### ee) Normen und Patente

Während Patente die Wahrung von Schutzrechten verfolgen und unerlaubte, also nicht lizenzierte, Nutzung unterbinden sollen, müssen Normen der Öffentlichkeit zugänglich gemacht und sollen möglichst von jedermann angewendet werden. **54**

An der Normung beteiligte Interessenvertreter treten Ihre „Urhebernutzungsrechte“ an das DIN und den VDE ab. Weiterhin sind sie verpflichtet, ihnen bekannte Patente, die von der Norm betroffen sein könnten, zu identifizieren, damit schon während der Normenerstellung entsprechend reagiert werden kann.

Ziel ist es, die Norm nicht auf Sachverhalte zu erstrecken, auf denen Schutzrechte ruhen. Lässt sich dies nicht vermeiden, muss in der Norm darauf hingewiesen werden. Darüber hinaus bemühen sich die Normungsorganisationen, mit dem Schutzrechtsinhaber Vereinbarungen zu treffen, die dem Normenanwender die Anwendung der Norm zu vernünftigen Bedingungen erlauben. Das kann z. B. sein

– **eine gebührenfreie Lizenz**

oder

– **eine entgeltliche Lizenz**

beides zu angemessenen und nicht diskriminierenden Bedingungen.

Ist der Schutzrechtsinhaber nicht gewillt, **Lizenzen** zu vergeben, darf die Norm nicht veröffentlicht werden oder muss, falls bereits veröffentlicht, zurückgezogen werden.

#### ff) Arten von Normen

Normen können nach Anwendungsmöglichkeit, Inhalt oder auch anderen Kriterien **55** unterschieden werden.

Beispiele für die Unterscheidung nach **Anwendungsmöglichkeit** sind:

– **Grundnormen** (Normen mit allgemeiner grundlegender Bedeutung),

– **Fachgrundnormen** (Normen mit allgemeinen Festlegungen für ein bestimmtes Fachgebiet)

und

– **Fachnormen** (Normen mit detaillierten Festlegungen für ein bestimmtes Fachgebiet).

Beispiele für die Unterscheidung nach **Inhalt** sind:

– **Sicherheitsnormen,**

– **Qualitätsnormen,**

– **Dienstleistungsnormen,**

– **Verfahrensnormen,**

– **Maßnormen**

usw.

Darüber hinaus gibt es normative Dokumente, die nicht Bestandteil des Deutschen Normenwerkes sind, aber eine ähnliche Aufgabe wie Normen erfüllen. Das sind **Spezifikationen**, die nach verschiedenen Verfahren erstellt werden können, oder auch nicht öffentlich zugängliche Dokumente wie Werknormen. **56**

Eine interessante Option ist die nationale Spezifikation nach dem Vornorm-Verfahren. Für ihre Erstellung gelten die gleichen Regeln wie für eine Norm, mit einigen Abweichungen. So darf z. B. die Entwurfsveröffentlichung entfallen und sie kann, als erster Schritt in Richtung Norm, ohne europäische Genehmigung/Beteiligung erstellt werden. In unserer schnelllebigen Zeit ist das eine Möglichkeit, in Kürze ein normatives Dokument zu erstellen, mit dem man Erfahrung in der Anwendung sammeln und so eine Norm vorbereiten kann. Technische Spezifikationen werden zunehmend auch von Behörden als **normative Dokumente** akzeptiert und können, falls sie Sicherheitsbestimmungen im Bereich der Elektrotechnik enthalten, eine VDE-Klassifikation erhalten. Ein Beispiel dafür ist der Bundeseinheitliche Pflichtenkatalog für Errichterunternehmen von Überfall- und Einbruchmeldeanlagen der Kommission Polizeiliche Kriminalprävention, Stand August 2007, der neben Normen auch die Einhaltung von Vornormen oder Entwurfsfassungen empfiehlt. Im Bereich der Sicherheitstechnik gibt es dazu beispielsweise die Vornorm DIN V VDE V 0826-1 (VDE V 0826-1) „Überwachungsanlagen – Teil 1: Gefahrenwarnanlagen (GWA) für Wohnhäuser, Wohnungen und Räume mit wohnungsähnlicher Nutzung – Planung, Einbau, Betrieb und Instandhaltung“.

### gg) Normung und Standardisierung

- 57 Die bei der Normung durchgeführte Konsensbildung kann zu einem länger andauernden **Normungsprozess** führen. Für dynamische Zukunftsmärkte wie z. B. der Informations- und Telekommunikationstechnologie (IKT) sind daher Veröffentlichungsformen erforderlich, die in einer kurzen Zeitspanne erarbeitet werden können. Diese Möglichkeit bieten sog. Spezifikationen, die z. B. Verbands- oder auch innerbetriebliche Regelwerke sein können. Im Unterschied zur konsensbasierten Normung wird die Erarbeitung von Spezifikationen als Standardisierung bezeichnet. Spezifikationen können später die Basis von nationalen, europäischen und internationalen Normen sein.
- 58 Zum Beispiel sind mit **VDE-Anwendungsregeln** (VDE-AR) und DIN-Spezifikationen (DIN-SPEC) Veröffentlichungsformen verfügbar, die das leisten. Bevor z. B. eine VDE-Anwendungsregel in das VDE-Vorschriftenwerk aufgenommen wird, müssen die Anforderungen erfüllt sein, die als Kriterien in der Satzung für das VDE-Vorschriftenwerk aufgeführt sind. Eine VDE-Anwendungsregel kann durch jedermann initiiert werden und bei Verzicht auf ein Einspruchsverfahren innerhalb von zwei bis drei Monaten publiziert sein. VDE-Anwendungsregeln wurden bisher z. B. in den Bereichen Qualitätsmanagement für Telemonitoring in medizinischen Anwendungen und induktive Ladung von Elektrofahrzeugen veröffentlicht.
- Sowohl Normen als auch Spezifikationen sind Handlungsempfehlungen, die den Stand der Technik und ein Mindestniveau an Sicherheit definieren.
- 59 Neben Normen existieren **Industriestandards**, die von Unternehmen bzw. Organisationen entwickelt werden, die ein gemeinsames Standardisierungsziel verfolgen und sich dazu in Foren oder Konsortien zusammenschließen. In zunehmendem Maße ermöglichen die nationalen Normungsorganisationen inzwischen die Zusammenarbeit mit Foren oder Konsortien. Ergebnisse der Arbeiten von Foren oder Konsortien können jedoch nur die Akzeptanz von Normen erhalten, wenn Sie von den Normungsorganisationen übernommen und in das Normenwerk eingebunden werden.

### c) Nutzen der Normung

#### aa) Normung als Wirtschaftsfaktor

Normung erzeugt Dokumente, die ein hohes Maß an systematisch zusammengefasstem Wissen enthalten und für Jedermann zugänglich sind. Der Nutzen entsteht durch die **Verbreitung von technologischem Wissen** in möglichst vielen Unternehmen, dadurch steigt die Innovationskraft der Volkswirtschaft insgesamt. Das DIN hat bereits im Jahr 2000 anerkannte Wirtschaftsfachleute mit einer Studie über den Nutzen der Normung beauftragt. Diese kamen zu dem Ergebnis, dass Normen mit ca. 1 % zum Brutto sozialprodukt beitragen, das waren in 1998 ca. 15,8 Mrd. Euro. 60

Aufgrund neuer Erkenntnisse und der seit der letzten Studie verstrichenen Zeit schien es empfehlenswert, die damaligen Ergebnisse zu überprüfen, so dass eine neue Studie unter Berücksichtigung der alten beauftragt wurde. Die in 2011 veröffentlichte Studie kommt zu ähnlichen, wenn auch nicht identischen, Ergebnissen. Der gesamtwirtschaftliche Nutzen wurde jetzt mit 0,72 % vom Bruttoinlandsprodukt ermittelt, das entspricht ca. 16,77 Mrd. Euro.

#### bb) Gesellschaftlicher Nutzen der Normung

Der gesellschaftliche Nutzen der Normung ist allgegenwärtig. Angefangen bei der Kompatibilität von Dingen, die wir im täglichen Leben nutzen, wie Steckverbindungen, Datenträger, Schrauben, Batterien, Leuchtmittel, Reifen usw. bis zur Sicherheit von Geräten und Einrichtungen. Unser Leben wäre unendlich komplizierter ohne **Festlegungen in Form von Normen**. Wir können darauf vertrauen, dass genormte Dinge bestimmte Eigenschaften besitzen, ohne uns mit den technischen Details auseinandersetzen zu müssen. 61

Normen, die Sicherheitsbedingungen festlegen, reduzieren die Anzahl von Unfällen und schützen damit unsere Gesundheit. Umweltnormen schützen die Umwelt und verbessern damit die Lebensqualität. Dienstleistungsnormen definieren Dienstleistungen und verbessern damit deren Qualität. Dadurch haben Normen einen hohen gesellschaftlichen Nutzen.

#### cc) Beispiele für den Nutzen der Normung im Bereich Sicherheitstechnik

Neben Produktnormen, die zur Vergleichbarkeit und Kompatibilität von Produkten beitragen, lassen sich beispielhaft folgende Normungsbereiche und der damit verbundene Nutzen identifizieren: 62

Normen, die **Wartung und Betrieb von Sicherheitsanlagen** betreffen, tragen zur Vereinheitlichung des Betriebszustands bei und legen Mindestanforderungen für diesen fest. Sie helfen damit, Falschalarme zu vermeiden und die Verfügbarkeit und Zuverlässigkeit der Anlagen zu steigern.

Normen, die **Übertragungsanlagen für Sicherheitsanlagen** betreffen, steigern die Zuverlässigkeit der Alarmübertragung und sorgen so innerhalb der Alarmübertragungskette dafür, dass der Alarm seinen Bestimmungsort erreicht.

Normen, die **Alarmempfangsstellen für Sicherheitsanlagen** betreffen, legen Mindestanforderungen an diese fest und verbessern eine strukturierte und klar definierte Bearbeitung und Weiterleitung des Alarms. Darüber hinaus definieren sie auch die bauliche Ausstattung und das damit verbundene Sicherheitsniveau der Alarmempfangsstelle, z. B. durch Überspannungsschutz, durch eine Notstromversorgung, durch Einbruch- und Überfallschutzmaßnahmen usw., wodurch die Verfügbarkeit und die Betriebssicherheit der Alarmempfangsstelle steigen.



- Brenneisen, Hartmut*: Das Makromodul Kriminalitätskontrolle im akkreditierten Bachelorstudiengang. In: *Kriminalistik* 7/2007, S. 469–475.
- Dalton, Dennis R.*: *Rethinking Corporate Security in the Post 9/11 Era. Issues and Strategies for the Today's Global Business Community*, Oxford 2003.
- Gesemann, Frank*: *Öffentliche Sicherheit durch private Dienste. Rechtsgrundlagen, Aufgabenfelder, Qualifikationsbedarf*, Berlin 2004.
- Gundel, Stephan; Mülli, Lars*: *Unternehmenssicherheit*, München 2009.
- Kovacich, Gerald L.; Halibozeck, Edward P.*: *The Manager's Handbook for Corporate Security. Establishing and Managing a Successful Assets Protection Program*, Amsterdam u. a. 2003.
- Krueger, Otto-Gert*: Vom Wachmann zum Sicherheitsmanager. In: Brenneisen, Hartmut; Kischewki, Susanne; Raschke, Siegfried: *Studium und Lehre. Reihe Polizei und Sicherheitsmanagement*, Bd. II, Hamburg 2007, S. 52–60.
- Olschok, Harald* (Hrsg.): *Jahrbuch Unternehmenssicherheit 2011*, Köln 2011.

## 2. Unternehmenssicherheit als Bestandteil des unternehmerischen Risikomanagements

*Dr. Stephan Gundel, Leiter Abteilung Sicherheit, Gefahrenabwehr, Gruner AG, Basel*

### a) Entwicklung des unternehmerischen Risikomanagements

**Unternehmenssicherheit** bzw. Corporate Security bewegt sich, wie die Bezeichnung bereits verdeutlicht, in einem unternehmerischen Umfeld. Wesentliche Aufgabe der Corporate Security ist die eines sog. „**business enablers**“, mit deren Hilfe die Kernprozesse und somit die Leistungserstellung eines Unternehmens ermöglicht werden.<sup>1</sup> Hierin liegt ein wesentlicher und grundsätzlicher Unterschied zur staatlichen Sicherheitsgewährleistung, die letztendlich nicht einem wirtschaftlichen Zweck, sondern der Durchsetzung eines rechtlichen Regelrahmens dient. 80

Die Notwendigkeit einer eigenen Unternehmenssicherheit ergibt sich daher (vgl. Kapitel D I. 1.) im Wesentlichen immer **aus originär wirtschaftlichen Bedürfnissen der betroffenen Unternehmen**: Durch die Unternehmenssicherheit sollen spezifische Gefährdungen für Prozesse und Werte des betroffenen Unternehmens erkannt, analysiert und minimiert werden, wobei die zu betrachtenden Gefährdungen mit dem unternehmerischen Umfeld einem stetigen Wandel unterliegen. Mit diesem Tätigkeitsgebiet ist die Unternehmenssicherheit allerdings, zumindest seit dem ausgehenden 20. Jahrhundert, nicht singularär im Unternehmen. Im Zusammenhang mit verschiedenen Bilanzskandalen und Unternehmenskrisen traten Ende der 90er Jahre in fast allen westlichen Ländern mit marktwirtschaftlichem Wirtschaftsrahmen handelsrechtliche Bestimmungen in Kraft, die von Unternehmen ein systematisches Risikomanagement verlangen.<sup>2</sup> 81

1 Der Begriff wurde im Werk *Dalton, Denis R.: Rethinking Corporate Security in the Post-9/11 Era*, Waltham MA, 2003 geprägt und danach in den Sprachgebrauch des deutschen Sicherheitsmanagements übernommen – im vorliegenden Werk beispielsweise in den Beiträgen von *Haacke, Sack* und *Schmidt* in Kapitel D.

2 In Deutschland finden sich entsprechende Regelungen im sog. Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), das am 1. Mai 1998 in Kraft getreten ist und vor allem Vorschriften des Handelsgesetzbuchs bzw. des Aktiengesetzes erweitert.

- 82 Diese handelsrechtlichen Bestimmungen wenden sich in recht allgemeiner Form primär an die Unternehmensleitung und verlangen grundsätzlich den **Aufbau eines Risikomanagements** im Unternehmen, um den „*Fortbestand des Unternehmens gefährdende Entwicklungen früh zu erkennen*“.<sup>3</sup> Spezielle Bestimmungen bezüglich des Risikomanagements gelten zudem für Banken und Versicherungen, die gemäß den Basel II-Richtlinien (Rahmenvereinbarung Internationale Konvergenz der Eigenkapitalmessung und Eigenkapitalanforderungen des Basler Ausschusses für Bankenaufsicht) bzw. dem Solvency II-Projekt der EU-Kommission (Reform des Versicherungsaufsichtsrechts in Europa) der Ermittlung, Erfassung, Überwachung und dem Management ihrer Risiken erhöhte Beachtung schenken müssen.<sup>4</sup> Dabei stehen zwar naturgemäß (**finanz-)wirtschaftliche Risiken**, insbesondere Liquiditätsrisiken, im Vordergrund, letztlich befasst sich aber auch das Risikomanagement mit der gleichen zentralen Fragestellung wie die Unternehmenssicherheit: Welche Ereignisse können den Betrieb oder sogar den Fortbestand des betrachteten Unternehmens gefährden?
- 83 Da sich die Anforderungen an das unternehmerische Risikomanagement primär an die Unternehmensführung wenden, lohnt zum Verständnis der Bedürfnisse und Vorstellungen dieser internen „Auftraggeber“ des Risikomanagements und der Unternehmenssicherheit ein kurzer Blick auf die **Entwicklung der Unternehmensführung** in der jüngeren Zeit. Eine Unternehmenssicherheit, die sich nicht an den Bedürfnissen der Unternehmensführung orientiert, wird mittel- bis langfristig wenig Akzeptanz im Unternehmen finden und ihre Aufgaben nur schwer erfüllen können. Gerade für Sicherheitsmanager in Unternehmen, die in ihrem bisherigen beruflichen Werdegang wenige Berührungspunkte mit Unternehmensführung in einem marktwirtschaftlichem Umfeld hatten (typischerweise ehemalige Mitarbeiter aus Sicherheitsbehörden), stellt diese Umstellung regelmäßig eine große Herausforderung dar.
- 84 Der Begriff und die Inhalte der Unternehmensführung (häufig umgangssprachlich auch als **Management** bezeichnet) haben sich im Laufe der letzten 50 Jahre erheblich gewandelt – interessanterweise in einer ähnlichen Form, wie die Anforderungen an die Unternehmenssicherheit den von Sack geschilderten Veränderungen unterlagen.<sup>5</sup> Bei der lange Zeit dominierenden, sog. herkömmlichen Betrachtungsweise der Unternehmensführung wird der Blick fast ausschließlich auf die Innenbeziehungen eines Unternehmens gerichtet.<sup>6</sup> Demnach müssen i. S. einer wertorientierten Unternehmensführung **die vorhandenen Produktionsfaktoren** (Personal, Anlagen, Sachmittel etc.) so eingesetzt werden, dass optimale Faktorkombinationen erreicht werden und somit der höchstmögliche Gewinn für die Anteilseigner (Shareholder) erzielt wird. Im Rahmen hierarchischer Organisationen mit Entscheidungsträgern auf verschiedenen Ebenen, die Unternehmen typischerweise sind, muss die Unternehmensführung dann das Unternehmen so steuern,

---

3 Diese Formulierung stammt aus § 91, Abs. 2 des deutschen Aktiengesetzes.

4 Vgl. zu einer detaillierten Auseinandersetzung mit den genannten Richtlinien im Zusammenhang mit der Unternehmenssicherheit *Gundel, Stephan/Müllli, Lars: Unternehmenssicherheit*, München 2009, S. 36 ff.

5 Vgl. Kapitel D I. 1. von *Dieter K. Sack* zur historischen Entwicklung der Unternehmenssicherheit.

6 Vgl. *Macharzina, Klaus: Unternehmensführung*, Wiesbaden 2003, S. 9

das Entscheidungen auf allen Hierarchieebenen i. S. der Shareholder koordiniert werden.<sup>7</sup> Unternehmensführung ist nach dieser Ansicht also primär die optimale interne Organisation eines Unternehmens – und Unternehmenssicherheit dient dann primär der Sicherung der eingesetzten Produktionsfaktoren im fast wörtlichen Sinn eines „Werkschutzes“.

Im Laufe der Zeit hat sich allerdings die Erkenntnis durchgesetzt, dass die Unternehmensführung nicht nur die (aktuellen) Gewinninteressen der Anteilseigner durch effiziente Unternehmensorganisation, sondern auch jene der Beschäftigten, der Kundschaft, der Lieferanten oder Gläubiger (sog. **Stakeholder**) durch langfristig ausgerichtete Entscheidungen berücksichtigen muss.<sup>8</sup> Nach diesem Verständnis gehen die **Aufgaben der Unternehmensführung** immer weiter über die Organisation interner Abläufe hinaus. Mittlerweile wird, vor dem Hintergrund der globalisierten Wirtschaft mit ihrer großen Dynamik, unter Unternehmensführung die „*Bewältigung der Umwelтанforderungen durch das Unternehmen*“<sup>9</sup> verstanden. Moderne Unternehmensführung bezieht sich somit auf die gesamte Gestaltung der Innen- und Außenverhältnisse eines Unternehmens. Ziel dieses weit gefassten Verantwortungsbereichs ist, den langfristigen und nachhaltigen Erfolg des Unternehmens (in der Regel ausgedrückt in monetären Größen) sicherzustellen.

Entsprechend dem modernen Ansatz der Unternehmensführung ist **unternehmerisches Risikomanagement notwendig**, um Faktoren, die den langfristigen und nachhaltigen Erfolg des Unternehmens gefährden, frühzeitig identifizieren und durch geeignete Maßnahmen adressieren zu können. Dadurch schließt die Bewältigung der Umwelтанforderungen im Rahmen der Unternehmensführung nicht nur die zunehmende Internationalisierung oder die sich stetig wandelnden technischen Rahmenbedingungen ein, sondern sicherheitsrelevante Entwicklungen müssen ebenfalls antizipiert und berücksichtigt werden. Hier schließt sich der Kreis von der Unternehmensführung zur **Unternehmenssicherheit** – sie wird im Rahmen des unternehmerischen Risikomanagements integraler Bestandteil der Unternehmensführung und muss ihrer Rolle als „business enabler“ viel mehr gerecht werden als zu früheren Zeiten, als sie vorrangig dem Schutz der (sachlichen) Produktionsfaktoren bzw. dem Werkschutz diente.

Unternehmenssicherheit wird also zumindest theoretisch durch zwei eng miteinander verknüpfte Entwicklungen stark wie selten zuvor in die Unternehmenspolitik integriert: Auf der einen Seite stehen die aktuellen Anforderungen an die Unternehmensführung, die in einem dynamischen und komplexen Umfeld den Fortbestand des Unternehmens und seine Zukunftsfähigkeit gewährleisten muss. Hierbei ist fundierte Expertise in sicherheitsrelevanten Fragestellungen für die Unternehmen unabdingbar. Gleichzeitig reagiert auch der Gesetzgeber im Rahmen handelsrechtlicher Bestimmungen immer stärker auf das volatile wirtschaftliche und gesellschaftliche Unternehmensumfeld und verlangt explizit **die Einführung eines unternehmerischen Überwachungs- und Risikomanagementsystems**.

7 Vgl. *Laux, Helmut*: Unternehmensrechnung, Anreiz und Kontrolle, Berlin 1999, S. 1.

8 Vgl. *Macharzina, Klaus*: Unternehmensführung, Wiesbaden 2003, S. 9.

9 Ebenda: S. 9.

**88** Für die Unternehmenssicherheit, die in Deutschland bisher nur auf wenigen gesetzlichen Grundlagen basiert,<sup>10</sup> sollte dies eigentlich einen erheblichen Bedeutungszuwachs mit sich bringen. Dieser anzunehmende Bedeutungszuwachs wird jedoch in der Unternehmenspraxis häufig nicht zugunsten des Sicherheitsmanagers wahrgenommen. Vielmehr besetzen andere Mitarbeitende aus dem Umfeld des unternehmerischen Risikomanagements wesentliche **Schlüsselpositionen im Bereich der Unternehmenssicherheit**, da sie für Führungspositionen in Unternehmen typische Ausbildungen (z. B. juristisches oder wirtschaftswissenschaftliches Studium), einen entsprechenden beruflichen Werdegang sowie dadurch a priori eine größere Nähe zum Denkmodell der Unternehmensführung aufweisen. Für einen modernen Sicherheitsmanager, der in einem modern geführten Unternehmen reüssieren will, sind daher umfassende Kenntnisse und Fähigkeiten im gesamten unternehmerischen Risikomanagement unabdingbar. Nur dann kann er mindestens auf Augenhöhe mit anderen Managern die Notwendigkeit des „Security Risk Managements“ argumentativ verdeutlichen und allenfalls sogar angrenzende Bereiche des unternehmerischen Risikomanagements betreuen.

**b) Bestandteile des unternehmerischen Risikomanagements**

**89** Aufgrund der vorgängig skizzierten Entwicklungen werden in den meisten mittleren und großen Unternehmen **Instrumente und Maßnahmen des Risikomanagements** eingesetzt. Größere Unternehmen verfügen dazu über spezialisierte Organisationseinheiten, in mittleren oder kleineren Unternehmen sind häufig aufgrund des starken Zusammenhangs mit der Unternehmensfinanzierung Controlling- oder sonstige Organisationseinheiten des betrieblichen Rechnungswesens mit dem Risikomanagement betraut. Analog zur Unternehmenssicherheit hängt der Stellenwert des unternehmerischen Risikomanagements dabei stark mit dem konkreten Unternehmensumfeld (Regulierung, Besitzverhältnisse, Produkte und Leistungen etc.) und der Persönlichkeit des Risikomanagement-Verantwortlichen zusammen.

**90** Was ist nun Inhalt des unternehmerischen Risikomanagements? Umgangssprachlich, aber nichtsdestoweniger treffend wird **Risiko als die Möglichkeit eines negativen Ausgangs** eines Ereignisses oder einer Handlung bezeichnet. Ereignis oder Handlung lassen jedoch grundsätzlich auch einen positiven Ausgang („Chance“) zu, wobei Unsicherheit über das Ergebnis des Handelns besteht. Sowohl die möglichen Ergebnisse des Handelns (positiv oder negativ) als auch die Eintretenswahrscheinlichkeiten dieser möglichen Ergebnisse lassen sich aber hinlänglich genau abschätzen. Beispielsweise lassen sich bei einer Auslandsreise der deutschen Delegation eines Unternehmens nach Afghanistan die möglichen Konsequenzen (Anschläge, Entführungen, Bedrohungen oder auch „glücklicher“ Ausgang) mit dem entsprechenden Aufwand zumindest näherungsweise bezüglich Konsequenzen und Eintrittswahrscheinlichkeit abschätzen. Sind Ergebnisse eines Handelns oder deren Eintrittswahrscheinlichkeit nicht zu bestimmen, ist auch kein Risikomanagement möglich – sinnvolles Risikomanagement basiert also stark auf verfügbaren Informationen!

**91** Das unternehmerische Risikomanagement betrachtet nun die Möglichkeiten der negativen Zielverfehlung bezogen auf die von der Unternehmensführung vorgege-

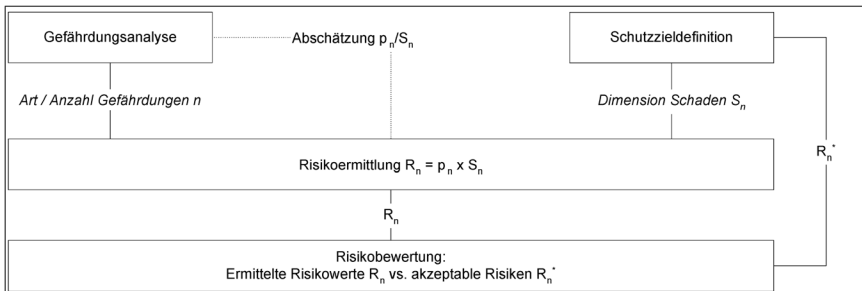
---

<sup>10</sup> Vgl. von *Michael Schmidt* Kapitel D 3. über Umfang, Bedeutung und Ziele der Unternehmenssicherheit.

benen Ziele und versucht, Risiken zu erfassen, zu bewerten und durch geeignete Maßnahmen zu minimieren. Da viele Risiken, denen ein Unternehmen ausgesetzt ist, nicht durch unternehmensinterne Maßnahmen minimiert werden können, **spielen Versicherungen im Risikomanagement eine wesentliche Rolle**. Sie dienen dem Risikoausgleich zwischen von derselben Gefahr bedrohten Wirtschaftseinheiten, im betrachteten Fall Unternehmen, und können über das Gesetz der großen Zahlen Eintrittswahrscheinlichkeiten und Schäden gleichartiger Ereignisse vergleichsweise genau ermitteln sowie beherrschbar machen.<sup>11</sup>

92

Risiken werden im Rahmen des unternehmerischen Risikomanagements entweder quantitativ oder qualitativ bewertet. Dafür sind zunächst die für das Unternehmen relevanten Schadensszenarien  $n$  im Rahmen einer **Gefährdungsanalyse** zu identifizieren. Bereits hierzu ist fundiertes Wissen über die unternehmensspezifische Bedrohungslage notwendig. Daraus aufbauend müssen die aus einer Gefährdung resultierenden **Schäden**  $S^n$  bestimmt werden. Da Schäden im unternehmerischen Risikomanagement zumeist monetär bewertet werden, gestaltet sich dies für Risiken aus dem Bereich der Unternehmenssicherheit (z. B. Schaden einer Entführung) teilweise schwierig – es besteht die Gefahr, dass Risiken dann „unterbewertet“ werden. Schließlich muss auch eine **Eintrittswahrscheinlichkeit**  $p^n$  für die Gefährdung abgeschätzt werden, damit diese mit dem vermuteten Schaden multiplikativ zu einem Risikowert  $R^n$  verdichtet werden kann. Dieser Risikowert kann dann mit den Risikowerten anderer Gefährdungen oder aber einem zuvor als akzeptabel definierten Risikowert  $R^*$  verglichen werden. Bild 1 zeigt das Verfahren bei einer Risikobewertung schematisch auf.



**Bild 1:** Methodik der Risikobewertung (vgl. Gundel/Müllli, 2009: 54)

Verfahren zur **Risikobewertung** werden, nicht nur im Umfeld der Unternehmenssicherheit, als kompliziert und trotzdem ungenau kritisiert, da sie sehr stark von den verfügbaren Informationen abhängen. Eine Bewertung des sich für das Unternehmen ergebenden Gefahrenbilds ist aber auf jeden Fall notwendig – **Risikoanalysen** stellen dazu ein methodisch sauberes und interdisziplinär anerkanntes Werkzeug dar. Zu ihrer konkreten Durchführung sowie möglichen Vereinfachungen,

93

<sup>11</sup> Die Funktionsweise von Versicherungen im Bereich der Unternehmenssicherheit sind in Gundel, Stephan/Müllli, Lars: Unternehmenssicherheit, München 2009 auf den S. 33–35 beschrieben.