Claudia Kestermann, Martin Langer & Arthur Hartmann

Konzernsicherheit in den **TOP100-Unternehmen** Deutschland Österreich Schweiz

Impressum

Diese Publikation wurde gemeinsam von der Hochschule für Öffentliche Verwaltung Bremen und der FH Campus Wien erstellt und herausgegeben. AutorenInnen für den Inhalt verantwortlich: Prof. Dr. Claudia Kestermann (Hochschule für Öffentliche Verwaltung Bremen), FH-Prof. DI Martin Langer (FH Campus Wien), Prof. Dr. Arthur Hartmann (Hochschule für Öffentliche Verwaltung Bremen)
Produktionsleitung: DI (FH) Mag. Thomas Goiser MA; Lektorat: Mag.a Verena Brinda www.verenabrinda.at; Grafik: Doris Grussmann (www.dggd.at).
Die Texte und Daten wurden sorgfältig ausgearbeitet, dennoch können wir keine Haftung für die Richtigkeit der Angaben übernehmen.

Wien/Bremen, November 2014

Inhalt

Vorwort

FH Campus Wien

Prof.in Dr.in Luise Greuel
Rektorin der Hochschule für Öffentliche Verwaltung Bremen

ao. Univ.-Prof. Mag. Dr. Arthur Mettinger
Rektor der FH Campus Wien

Pioniere geben Orientierung

Sicherheit ist ein Grundbedürfnis und betrifft uns alle. Heute nehmen Bürgerinnen und Bürger ihr Vorhandensein meist als etwas Selbstverständliches an. Das ist einerseits eine Folge der glücklichen Lage, in der wir uns seit einigen Jahrzehnten im Zentrum Europas in unseren Gemeinwesen befinden: Rechtsstaatlichkeit, funktionierende Institutionen, sozialer und politischer Friede sowie (im Großen und Ganzen) gemeinsam getragene Werte. Das war hier nicht immer der Fall und ist heute bei weitem nicht überall so. Andererseits sind hohe Sicherheitsstandards und ein hohes subjektives Sicherheitsgefühl auch Folge der täglichen engagierten Arbeit von Behörden, couragierten Einzelpersonen, Zivilgesellschaft und Wirtschaft.

Unternehmen – und gerade jene im internationalen Wettbewerb – wissen, dass sie über wertvolle Ressourcen verfügen und schützen diese entsprechend: Ideen und Informationen, Prozesse und Verfahren, Patente und Rechte, Rohstoffe, Gebäude und Maschinen sowie nicht zuletzt Mitarbeiterinnen und Mitarbeiter. Die Bedrohungen und Herausforderungen sind zahlreich, höchst unterschiedlich und entwickeln sich ständig weiter.

Die Sicherheit in den TOP100-Unternehmen in Deutschland, Österreich und der Schweiz und damit die Umsetzung und Organisation von Konzernsicherheit sowie die Rolle der dafür verantwortlichen Personen ist in diesem Zusammenhang ein besonders wichtiges Forschungsthema. Denn die Sicherheit ist Teil des wirtschaftlichen Erfolgs dieser Unternehmen. Gleichzeitig sind die Sicherheitsverantwortlichen großer Konzerne Pioniere und Taktgeber neuer Entwicklungen; sie sind bei Innovationen wie bei Organisations- oder Sicherheitsthemen beispielgebend für andere Unternehmen.

Die Arbeit der Chief Security Officers in diesen Unternehmen ist daher von ganz besonderer Bedeutung. Wir freuen uns, dass an unseren beiden Hochschulen dieses Thema als Forschungsprojekt im Rahmen der vorliegenden Studie aufgegriffen wurde, und wir sehen uns bestärkt in unserer Haltung, der Sicherheitsforschung einen besonderen Stellenwert beizumessen und in diesem Kontext der Arbeit der CSOs im deutschsprachigen Raum eine besondere wissenschaftliche Aufmerksamkeit zu kommen zulassen.

Das Thema „Sicherheit in Unternehmen“ wird weiter an Relevanz gewinnen. Daher wünschen wir allen Beteiligten, dass diese Studie und die vorliegende Publikation aus unseren Hochschulen zu einem Erkenntnisgewinn und zur vertieften Diskussion aktueller Fragen beizutragen vermag.

Luise Greuel, Arthur Mettinger

Vorwort und Danksagung

Prof.in Dr.in
Claudia Kestermann
Hochschule für
Öffentliche
Verwaltung
Bremen

FH-Prof.
Martin Langer
Fachhochschule
Campus Wien

Prof. Dr.
Arthur Hartmann
Hochschule für
Öffentliche
Verwaltung
Bremen

Am Puls der Zeit

Unsere beiden Hochschulen verbinden Wissenschaft, Sicherheit und Wirtschaft. Gerade im Risiko- und Sicherheitsmanagement aufgrund der fortschreitenden Vernetzung und steigenden Komplexität der einzige Weg zum Erfolg. Dieser interdisziplinäre Ansatz zeigt sich in den Curricula unserer Studiengänge, in unseren vielfältigen Kooperationen in Lehre und Forschung sowie nicht zuletzt in unseren Forschungsthemen. In der Ausbildung war und ist es unser Ziel, möglichst praxisrelevante Studiengänge anzubieten, so dass die Beschäftigung unserer Absolventen und Absolventinnen mit ihren Kenntnissen und Fähigkeiten einen Gewinn für Unternehmen darstellt. Für diesen Anspruch und die Weiterentwicklung unserer Studieninhalte ist es wichtig zu wissen, welche Fähigkeiten jetzt und in Zukunft gebraucht werden.

In der Forschung, die für uns alle und unsere Hochschulen einen hohen Stellenwert hat, befassen wir uns aus unterschiedlichen Perspektiven mit Sicherheitsfragestellungen. So ist an der HfÖV Bremen bspw. das Institut für Polizei- und Sicherheitsforschung (IPoS) angesiedelt. In dem hier vorgestellten Projekt bündeln wir nun erstmalig unsere Ressourcen und vertiefen eine Zusammenarbeit, die im „Cooperation Network for Risk, Safety and Security Studies“ (CONRIS), das unsere Institute mitbegründet haben, begonnen hat.

Das Projekt „Konzernsicherheit TOP100“ werden wir auf den folgenden Seiten näher darlegen und die ersten Ergebnisse vorstellen. Mit dieser Studie haben wir nicht nur unsere eigenen Forschungsinteressen verfolgt, sondern sind Anfragen aus der Wirtschaft nachgekommen. Aus den Unternehmen sind wir wiederum durch die Beteiligung an unserer Befragung unterstützt worden. Allen Teilnehmenden – den „Chief Security Officers“ der jeweils größten Unternehmen aus Deutschland, Österreich und der Schweiz – ein herzliches Dankeschön!

Von unserem Forschungsvorhaben konnten wir ganz zentrale Personen und Organisationen überzeugen, die in besonderer Weise für die Sicherheit in den beteiligten Ländern stehen, namentlich

- Jörg Ziercke, Präsident des Bundeskriminalamtes der Bundesrepublik Deutschland
- General Franz Lang, Direktor des Bundeskriminalamt im Bundesministerium für Inneres der Republik Österreich
- Dr. Jean-Luc Vez, bis August dieses Jahres Direktor des Bundesamtes für Polizei (der Schweiz).

Für das gezeigte Vertrauen und die Unterstützung möchten wir uns auf diesem Weg ebenfalls herzlich bedanken. Unser Ziel war es, mit den Ergebnissen des Forschungsprojekts für die Beteiligten und alle am Thema Interessierten aktuelle Erkenntnisse sowie Denk- und Diskussionsansätze für ihr Tätigkeitsfeld zu bieten.

Wir hoffen, dass dies gelungen ist und freuen uns auf Ihre Rückmeldung.

Claudia Kestermann, Martin Langer, Arthur Hartmann

1. Vorstellung der Studie

Im Winter 2013/2014 wurde durch die Hochschule für Öffentliche Verwaltung in Bremen und die Fachhochschule Campus Wien eine Befragung von bedeutenden Wirtschaftsunternehmen in Deutschland, Österreich und der Schweiz (D-A-CH-Region) im Hinblick auf sicherheitsrelevante Aspekte durchgeführt. Das Ziel der Studie „Unternehmenssicherheit CSO Top100“ bestand darin, länderübergreifend in Deutschland, Österreich und der Schweiz Informationen zu Aufbau und Struktur von Sicherheit ebenso wie zur Sicherheitskultur und Kriminalitätsbelastung in führenden Wirtschaftsunternehmen zu gewinnen.

Die Studie soll Erkenntnisse zur Organisation von Sicherheit in Unternehmen in der D-A-CH Region liefern und eine vertiefende Analyse verschiedener interagierender Faktoren ermöglichen, deren Ergebnisse wiederum für die Praxis nutzbar gemacht werden können.

Die hier dargestellten Ergebnisse beziehen sich auf ausgewählte Ausschnitte aus der Gesamterhebung. Übergeordnete Themenfelder werden im Folgenden primär deskriptiv dargestellt und in Verbindung mit zentralen Faktoren untersucht. Differenzierte Analysen spezifischer Fragestellungen werden in weiteren Sonderauswertungen vorgenommen und an anderer Stelle publiziert.

2. Methodisches Vorgehen

2.1 Inhalt und Operationalisierung der Untersuchungsfragestellung

Der Fragebogen gliedert sich in drei zentrale Bereiche, die nachstehend kurz skizziert werden: Organisation und Sicherheitsstruktur, Unternehmens- und Sicherheitskultur, Kriminalitätsbelastung sowie Aufgabenfelder und Kooperationen.

Organisations- und Sicherheitsstruktur

Bei der Erhebung struktureller Aspekte im Hinblick auf Organisation und Sicherheit in den Unternehmen standen die Positionen der Leitung der Sicherheitsabteilung bzw. der Sicherheitsverantwortlichen im Mittelpunkt des Interesses, insbesondere deren Anbindung an den Vorstand, inhaltliche Zuständigkeiten, mögliche Weisungsbefugnisse und strategische Einflussmöglichkeiten.

Unternehmens- und Sicherheitskultur

Unter dieses Themenfeld lassen sich verschiedene sicherheitsrelevante Haltungen, Verhaltensweisen und Maßnahmen subsumieren. Einen Überblick zu den einzelnen Aspekten liefert die nachfolgende Tabelle.

Die Fragen zum Themenkomplex „Unternehmenskultur“ wurden u.a. mittels eines standardisierten Instruments erhoben, der Kurzskala zur Erfassung der Unternehmenskultur von Jöns, Hodapp und Weiss (2006). Die Skala erfasst Aspekte der Unternehmensstrategie, der Unternehmensstruktur, des Führungsverhaltens und der Zusammenarbeit.[1]

Tabelle 1: Aspekte der Sicherheitskultur

- Aspekte der Unternehmenskultur mit sicherheitsrelevanten Auswirkungen
- Verhaltensrichtlinien, Code of Conduct und Evaluation zur Effekt- bzw. Qualitätskontrolle
- Hinweisgebersysteme / Umgang mit Whistleblowing
- Maßnahmen zu Awareness / Sensibilisierung für Sicherheitsbelange
- Fehlerkultur im Unternehmen

Im Hinblick auf die Verhaltensrichtlinien wurden neben der personellen Beteiligung bei der Entwicklung insbesondere die Art und Weise, wie Unternehmensangehörige über diese informiert werden, deren Implementierung und die Überprüfung der Auswirkungen thematisiert. Die Erhebung in Bezug auf Zugänglichkeit und Präsentation des Code of Conduct sowie die Verpflichtung zur Einhaltung der Verhaltensrichtlinien erfolgte auf Basis der Ausführungen von Erwin (2011).

In der Folge wurden der Themenbereich „Whistleblowing“ und die Implementierung von Hinweisgebersystemen betrachtet sowie die Einschätzung der Befragten dazu erhoben. Anschließend beschäftigte sich dieser Abschnitt mit Maßnahmen zur Sensibilisierung für Sicherheitsbelange und deren Eignung für die Steigerung des Sicherheitsbewusstseins in der Organisation. Dieser Abschnitt endete mit Fragen zu Fehlerkultur und Fehlermanagement im Unternehmen.[2]

1 Aus methodischer Sicht ergeben sich im Hinblick auf einzelne Aspekte der Unternehmens- und Sicherheitskultur insoweit Interpretationsgrenzen, als die zu befragende Zielgruppe aus einzelnen Angehörigen eines Unternehmens besteht und somit ausschließlich die Perspektive dieser einzelnen Befragten erhoben wird. Für generalisierende Aussagen über die Unternehmens- und Sicherheitskultur wäre die Befragung einer größeren Stichprobe von Mitarbeiter und Mitarbeiterinnen sowie Führungskräften in den einzelnen Unternehmen erforderlich.

2 nach Hudson (2007), Fahlbruch, Schöbel & Domeinski (2008); Weick & Sutcliffe (2003), Buerschaper (2008).

Kriminalitätsbelastung

Im dritten Abschnitt ging es um die Erfahrungen der befragten Unternehmen als Betroffene unterschiedlicher Delikte. Neben der Prävalenz (Betroffenheit innerhalb der letzten 24 Monate) wurde auch das Schadensausmaß erhoben. Außerdem wurde der Anteil des zeitlichen Aufwands präventiver und reaktiver Maßnahmen zur Kriminalitätsbekämpfung untersucht. Darüber hinaus war von Interesse, inwieweit die Unternehmen bekanntgewordene Vorfälle systematisch erfassen, worauf sich ggf. eine solche Erfassung erstreckt und in welcher Form und Häufigkeit die Meldung und Auswertung der gewonnenen Erkenntnisse erfolgen.

Den Abschluss der Erhebung bildeten – neben Kooperationserfahrungen – die Einschätzungen zukünftiger Herausforderungen und der persönlichen Zufriedenheit mit den Arbeitsbedingungen.

Tabelle 2: Kriminalitätsbelastung

- Deliktsbereiche: Vermögensdelikte, Wettbewerbsdelikte, andere wirtschaftskriminelle Delikte, Erpressung und Sabotage
- Präventive und reaktive Maßnahmen
- Erfassung bekannt gewordener Vorfälle / Reportingsystem

2.2 Durchführung der Befragung und Anmerkungen zur Stichprobe

In den beteiligten Ländern Deutschland, Österreich und der Schweiz wurde in Abhängigkeit von Größe und Unternehmensdichte eine unterschiedlich hohe Anzahl an Unternehmen ausgewählt. Grundlage für die Einbeziehung der Unternehmen waren deren veröffentlichte Umsatzzahlen. Zudem wurden die größten Versicherungsunternehmen und Banken separat adressiert. In Deutschland wurden insgesamt N=180 Fragebögen postalisch versandt, in Österreich N=99 und in der Schweiz N=62. Die Teilnahme war entweder über den gedruckten Fragebogen oder über eine Online-Version des Fragebogens möglich.

Insgesamt wurden N=72 Fragebögen eingesandt, was einem Anteil von 21,1 % entspricht. Abzüglich der nicht annähernd vollständig ausgefüllten und somit nicht berücksichtigten Fragebögen verbleiben letztlich als Nettostichprobe N=54 Fragebögen (Rücklaufquote: 15,8 %). In Anbetracht der Besonderheit der Stichprobe auch und insbesondere vor dem Hintergrund der sicherheitsrelevanten Thematik der Befragung ist diese Beteiligung als höchst akzeptabel einzustufen.

Die N=54 Teilnehmenden verteilen sich auf die beteiligten Länder wie folgt: N=32 Teilnehmende aus deutschen, N=13 aus österreichischen und N=9 aus schweizerischen Unternehmen. Angesichts der geringen Größe der Stichprobe haben die Ergebnisse (insbesondere auf Länderebene) primär heuristischen Charakter. Damit sollen – auch im Sinne von good practice – beispielhafte Erkenntnisse generiert und Zusammenhänge identifiziert werden, die für die Praxis sowie für weitere Forschung handlungsleitend sein können.

Bei den teilnehmenden Unternehmen, Banken und/oder Versicherungen handelt es sich zum größten Teil um transnational tätige Firmen, die im Durchschnitt in 42 Ländern vertreten sind (Median: 30 Länder). Fast zwei Drittel der beteiligten Unternehmen (64,5 %) sind dabei auf mindestens vier Kontinenten aktiv.

3. Erste bedeutsame Ergebnisse

Im Folgenden werden erste ausgewählte Ergebnisse präsentiert; dabei liegt der Schwerpunkt auf der deskriptiven Darstellung. Über Häufigkeitsangaben hinaus werden zudem bivariate Zusammenhänge oder Gruppenunterschiede betrachtet.

3.1 Organisation von Sicherheit und Zufriedenheit der Sicherheitsverantwortlichen

Eigene Konzernsicherheitsabteilungen: Deutschland weit vor Schweiz und Österreich

Nahezu drei von vier (74 %) teilnehmenden Unternehmen verfügen über eine Konzernsicherheitsabteilung. Bei den beteiligten deutschen Unternehmen liegt der Anteil mit 87,5 % deutlich vor jenen aus der Schweiz (66,7 %) und jenen aus Österreich (46,2 %).

Dass das Thema „Sicherheit" als Aufgabe explizit dem Vorstand zugeordnet ist, bejahen 56 % der Teilnehmenden. Während dies in Deutschland und der Schweiz von der Hälfte der Befragten angegeben wird (DE 48,3 %, CH 50 %), liegt der Anteil in Österreich bei mehr als drei Vierteln (AT 76,9 %).

Dies zeigt sich auch anhand der Ansiedlung der Stelle der Leiterin/des Leiters der Abteilung Konzernsicherheit bzw. der/des Sicherheitsverantwortlichen im Unternehmen (siehe Abb.1).

In Österreich sind drei Viertel der Stellen der Sicherheitsleitung organisatorisch in den ersten beiden Ebenen angesiedelt, in Deutschland und der Schweiz jeweils ca. 44 %.

Je höher angesiedelt, desto zufriedener

Die Hierarchie-Ebene, in der die Konzernsicherheitsabteilung angesiedelt ist, korreliert signifikant positiv mit der Ebene, auf der die eigene Stelle angesiedelt ist.[3]

Rahmenbedingungen und Ressourcen: Sehr unterschiedliche Einschätzungen

Einige spezifische Fragen behandelten die Zufriedenheit der Sicherheitsverantwortlichen mit den Rahmenbedingungen im Unternehmen, ihrer Position und den zur Verfügung stehenden Ressourcen (siehe nachfolgende Abb.2).

Die Zufriedenheit mit der eigenen Position ist bei den Befragten relativ hoch ausgeprägt (87,5 %: „trifft voll zu" / „trifft eher zu"). Fast ebenso deutlich ist die positive Einschätzung der Unterstützung durch den Vorstand (83,4 %: „trifft voll zu" / „trifft eher zu") und der fachlichen Anbindung an den Vorstand (73 %: „trifft voll zu" / „trifft eher zu"). Allerdings ist ein nicht unerheblicher Anteil der Befragten durchaus unzufrieden mit der aktuellen Situation.

Mit der Verantwortung für das Budget ist ein großer Teil der Befragten zumindest bedingt zufrieden (wobei 90,7 % über ein eigenes Budget verfügen). Auch im Hinblick auf die Höhe des zur Verfügung stehenden Budgets kann von einer relativ hohen Zufriedenheit ausgegangen werden – nur ungefähr jede/r Fünfte (20,9 %) gibt an, „eher unzufrieden" bzw. „sehr unzufrieden" zu sein. Mit 41,7 % ist der Unmut über die personelle Situation dagegen wesentlich höher ausgeprägt.

3 Spearman rho=.505, p<.01

Abbildung 1: Ebene der Leitung der Abt. Konzernsicherheit oder der/des Sicherheitsverantwortlichen

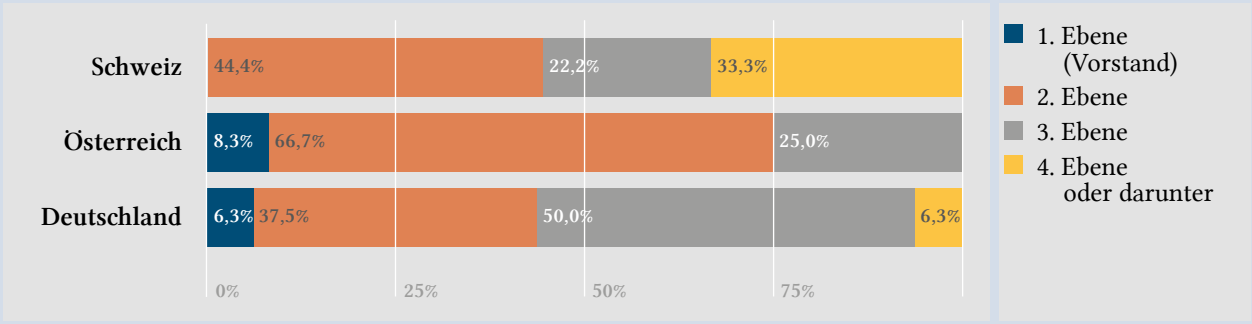
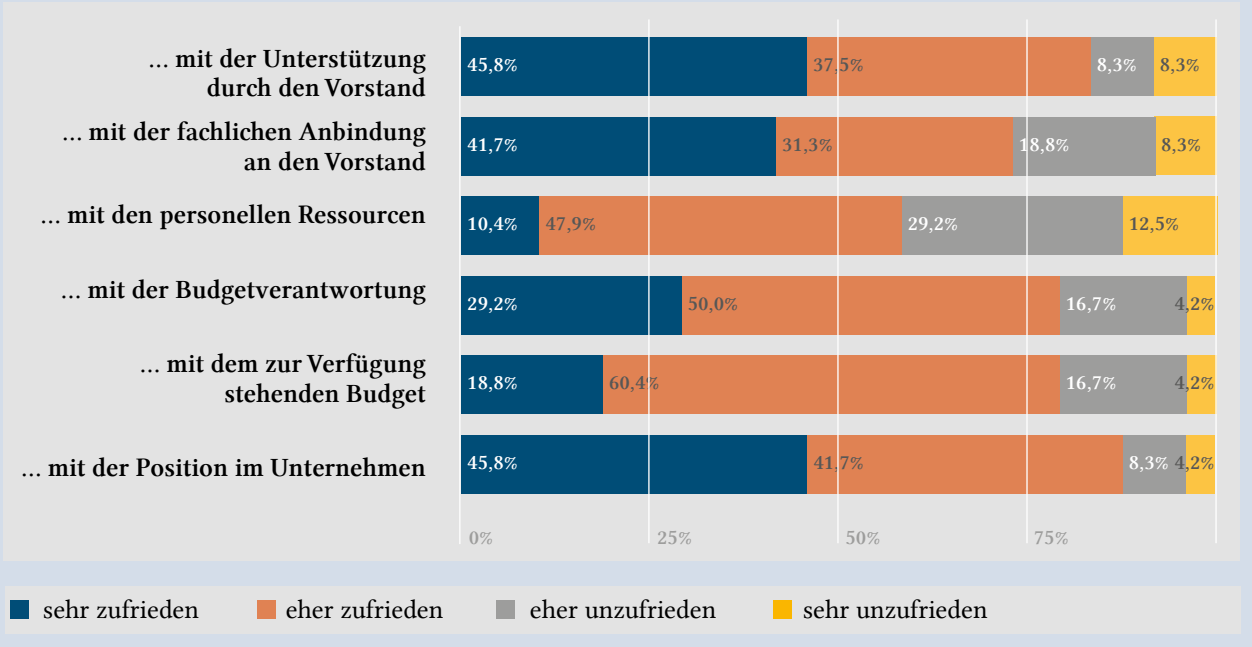


Abbildung 2: Zufriedenheit der Befragten



Zufriedenheitsranking: Schweiz hinter Österreich und Deutschland

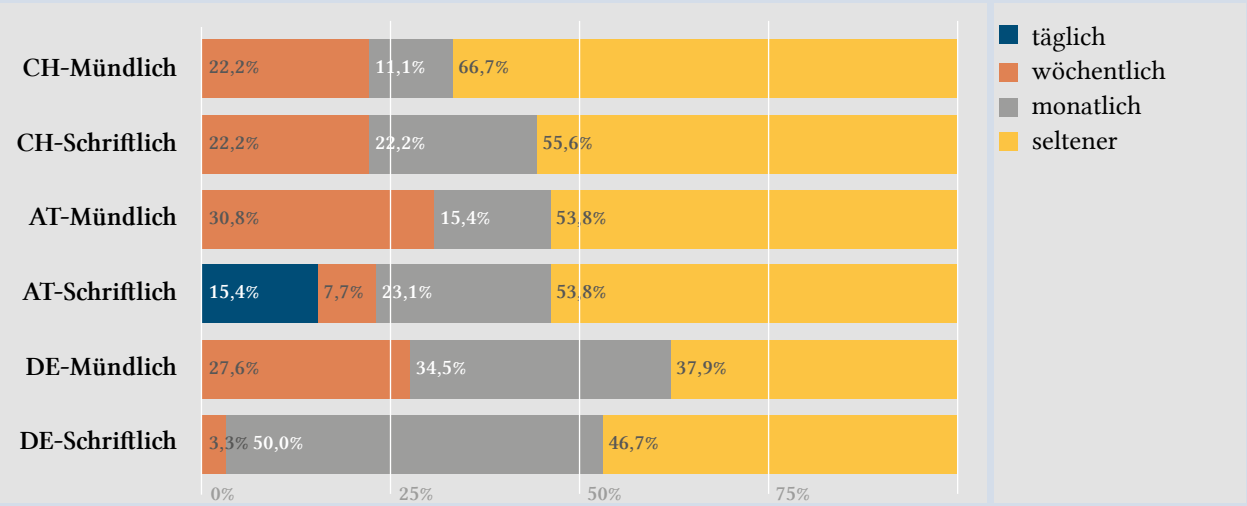
Mit einer durchschnittlichen Bewertung der Zufriedenheitsaspekte mit einem Mittelwert von 2,5 (Skala: 1=„sehr zufrieden“ bis 4=„sehr unzufrieden“) sind die schweizerischen Befragten deutlich weniger zufrieden mit der aktuellen Situation als die deutschen (M=1,9) und die österreichischen Teilnehmenden (M=1,8).

Zusammenhang von Einbindung und Zufriedenheit

Inwiefern die Zufriedenheit mit den verschiedenen oben genannten strukturellen Aspekten mit der Häufigkeit des mündlichen bzw. schriftlichen Kontakts zum Vorstand in Zusammenhang steht, soll nachfolgend geprüft werden. Zunächst werden Kontakthäufigkeit und -möglichkeit in den Unternehmen (nach Ländern) dargestellt.

Während in Deutschland dem Vorstand weit weniger häufig als in den anderen Ländern regelmäßig schriftlich berichtet wird, erfolgt ein häufigerer mündlicher Bericht. Zudem geben 80,6 % der deutschen Befragten an, bei Bedarf mit dem Vorstand in Kontakt treten zu können. Befragte aus Österreich geben zu 69,2 %, Befragte aus der Schweiz nur zu 44,4 % an, eine solche zusätzliche Kommunikationsmöglichkeit zu haben. Die Häufigkeit schriftlicher Berichterstattung steht in keinem Zusammenhang mit Aspekten der Zufriedenheit, der häufigere mündliche (und damit persönliche) Kontakt allerdings schon: Dieser korreliert signifikant mit der Zufriedenheit mit der eigenen Position sowie mit der Zufriedenheit mit der Höhe des zur Verfügung stehenden Budgets.[4]

Abbildung 3: Häufigkeit, mit der dem Vorstand berichtet wird

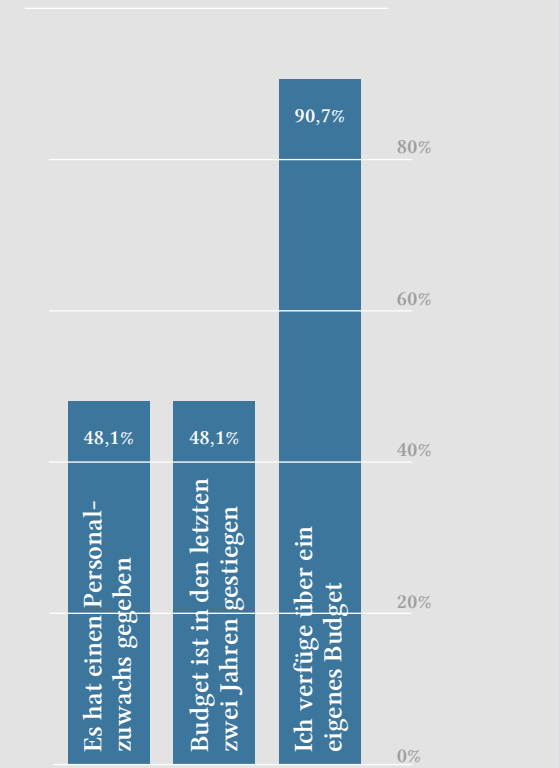


4 Spearman rho=.472, p<.001; Spearman rho=.307, p<.05

3.2 Finanzielle und personelle Ressourcen

Im Hinblick auf die Budgetverantwortlichkeit gibt es zwischen den Befragten aus den drei Ländern leichte Unterschiede: Der Anteil der Teilnehmenden aus Deutschland, der über ein eigenes Budget verfügt, ist mit 96,9 % am höchsten, während dies in Österreich von 84,6 % und in der Schweiz noch von 77,8 % angegeben wird. Diejenigen, die über ein eigenes Budget verfügen können, zeigen im Hinblick auf alle erhobenen Zufriedenheitsdimensionen signifikant positivere Werte als jene, die keine Budgetverantwortung haben. Dies gilt unabhängig von den eigentlichen finanziellen und personellen Ressourcen. Eine Zunahme des Budgets oder des Personals wird von jeweils ca. 50 % der deutschen und österreichischen Befragten konstatiert, während es von nur ca. 35 % der schweizerischen Teilnehmenden bejaht wird.

Abbildung 4: Finanzielle und personelle Ressourcen



Werden nun diejenigen, die eine Erhöhung des Budgets in den letzten zwei Jahren verzeichnen konnten, mit denen verglichen, deren Budget nicht gestiegen ist, so hat dies im Hinblick auf die untersuchten Zufriedenheitsaspekte Auswirkungen auf die Wahrnehmung des Vorstands: In der letztgenannten Gruppe ist die Zufriedenheit mit der fachlichen Anbindung an den Vorstand ebenso wie die Zufriedenheit mit der Unterstützung durch den Vorstand signifikant geringer[5]. Auch im Hinblick auf personelle Veränderungen wird ein Zusammenhang mit der wahrgenommenen Unterstützung durch den Vorstand evident; die Kontakthäufigkeit mit dem Vorstand ist hier auch besonders bedeutsam.[6]

5 T=-2.318; p<.05; T=-2.108; p<.05
6 T=-2.429; p<.05; T=-2.895; p<.01

Tabelle 3: Anstieg des Budgets und des Personals in Verbindung mit Aspekten der Zufriedenheit

	Das Budget ist in den letzten beiden Jahren gestiegen	**Mittelwert**
Zufriedenheit mit der fachlichen Anbindung an den Vorstand	Budget gestiegen Budget nicht gestiegen	1.55 2.15
Zufriedenheit mit der Unterstützung durch den Vorstand	Budget gestiegen Budget nicht gestiegen	1.45 1.96
	In den letzten beiden Jahren hat ein Personalzuwachs stattgefunden	**Mittelwert**
Zufriedenheit mit der Unterstützung durch den Vorstand	Personalzuwachs Kein Personalzuwachs	1.43 2.04
Häufigkeit, mit der dem Vorstand mündlich vorgetragen wird	Personalzuwachs Kein Personalzuwachs	2.83 3.48

Skalen: Zufriedenheit – 1=„sehr zufrieden“ bis 4=„sehr unzufrieden“;
Häufigkeit - 1=„täglich“ bis 4=„seltener als monatlich“

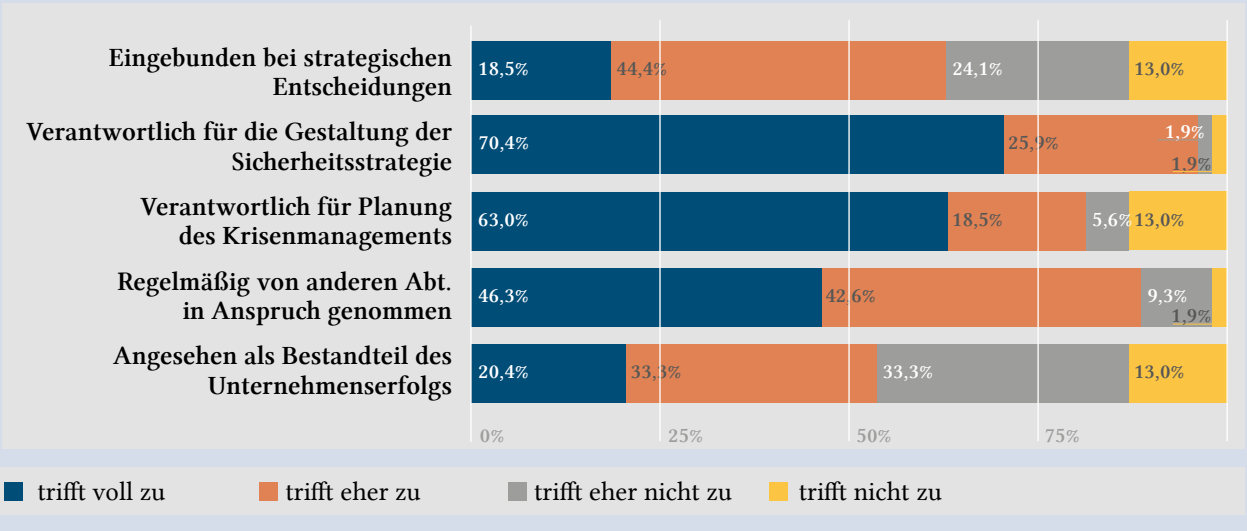
3.3 Strategische Entscheidungsmöglichkeiten im Unternehmen

Inwieweit die Befragten in strategische Entscheidungen einbezogen oder mit derartigen Aufgaben betraut bzw. Kompetenzen ausgestattet sind, zeigt Abbildung 5.

Verantwortung und Einbindung ja, Anteil am Erfolg eher nein?

Bei Entscheidungen mit unternehmensstrategischer Bedeutung sind 63 % der Befragten zumindest teilweise eingebunden (Antwortmöglichkeiten: „trifft voll zu“ und „trifft eher zu“). Im Hinblick auf die Gestaltung der Sicherheitsstrategie steigt der Anteil auf 96,3 %.

Abbildung 5: Bedeutung und strategische Einbindung
der Abteilung Konzernsicherheit bzw. der Sicherheitsverantwortlichen



Als (mit)verantwortlich für die Konzeption und Planung des Krisenmanagements betrachten sich 81,5 %; ein noch etwas höherer Anteil von 88,9 % wird immer wieder von anderen Abteilungen aus dem Unternehmen in Anspruch genommen bzw. hinzugezogen, was den Stellenwert im Unternehmen verdeutlicht.

Wird allerdings die Einschätzung betrachtet, ob die Abteilung Konzernsicherheit bzw. der/die Sicherheitsverantwortliche und deren/dessen Arbeit als Bestandteil des Unternehmenserfolges gesehen werde, so ist diese deutlich weniger positiv ausgeprägt. Während 53,7 % zum Teil mit Einschränkungen annehmen, dass im Unternehmen diese Wahrnehmung vorherrscht, verbleibt ein nicht unerheblicher Anteil der Befragten, der eine mehr oder weniger deutliche pessimistische Position einnimmt. Hier wird die oft angeführte Diskrepanz zwischen der Bedeutsamkeit der eigenen Arbeit und des Themas „Sicherheit" einerseits und der Fremdeinschätzung bzw. des Images von „Sicherheit" im Unternehmen andererseits offensichtlich.[7]

Kompetenzen: Governancefunktion im Regelfall und Krisenstabsleitung im Sonderfall

Mehr als drei Viertel (75,9 %) der Sicherheitsverantwortlichen sind gegenüber anderen Abteilungen in bestimmten Situationen weisungsbefugt. In Deutschland und Österreich liegt der Anteil etwas höher; in der Schweiz dagegen sind nur zwei Drittel der Befragten mit einer solchen Befugnis ausgestattet.

Neben den grundsätzlichen Kompetenzen und Befugnissen für sicherheitsrelevante Themen verfügt die Leitung des Sicherheitsbereichs in verschiedenen Themenfeldern und Situationen über ein gewisses Durchgriffsrecht. In der nachfolgenden Tabelle sind die am häufigsten angegebenen Aspekte exemplarisch aufgelistet.

Tabelle 4: Bedingungen für Weisungsbefugnisse

Grundsätzliche Befugnisse

- „Konzernsicherheit hat bei vielen Aufgaben eine Governancefunktion"
- „CSO hat ein Weisungsrecht für alle gesetzlich geregelten Sicherheitsthemen"
- „Policys, Standards und Guidelines zu allen sicherheitsrelevanten Themen"
- Fachliche Verantwortung, Richtlinienkompetenz und fachliches Weisungsrecht

Spezifische Befugnisse

- Notfall- und Krisensituationen, Evakuierungen (Incident & Crisis Management)
- Reisesicherheit (Travel Security)
- Ermittlungen, Incident Reporting
- Informationsschutz
- Veranstaltungsschutz (Event & Personnel Protection)
- Objektschutz, Brandschutz, Gefahrgut
- Umweltschutz
- Verstöße gegen Sicherheitsvorschriften

Zwischen den einzelnen Ländern zeigt sich in der Frage nach einer möglichen Leitung des Krisenstabs durch die Abteilung Konzernsicherheit bzw. die/den Sicherheitsverantwortliche/n eine erhebliche Differenz: Nur rund jeder zweite Befragte aus Österreich und der Schweiz (50 % bzw. 55,6 %) gibt an, in bestimmten Situationen oder bei besonderen Ereignissen die Leitung des Krisenstabs zu übernehmen; in Deutschland dagegen sind es bereits 4 von 5 (78,1 %).

7 Unterschiede zwischen den Ländern sind dabei statistisch nicht bedeutsam: Mittelwerte: DE 2,4; AT 2,2; CH 2,8 (Skala: 1=„trifft voll zu" bis 4=„trifft nicht zu")

3.4 Fachliche Zuständigkeiten

Die Verantwortungsbereiche der Sicherheitsabteilungen und -verantwortlichen der teilnehmenden Unternehmen sind erwartungsgemäß sehr breit gefächert, wobei die jeweiligen Zuständigkeiten von den personellen Ressourcen, der Unternehmensstruktur und der jeweiligen Branche abhängig sind.

Zu beachten ist hier die Organisationsform und damit Komplexität und Differenzierung der Verantwortungsbereiche. Bevor also etwaigen Unterschieden zwischen den beteiligten Ländern zu große Bedeutung beigemessen wird, erscheint es bedeutsamer, die Abteilungen Konzernsicherheit bzw. Corporate Security mit denjenigen zu vergleichen, die Sicherheit anders organisiert haben. Im Folgenden erfolgt zunächst ein Überblick über jene Felder, die – in Abhängigkeit von dieser Organisation – am häufigsten bzw. am wenigsten häufig in den Zuständigkeitsbereich der Befragten fallen.

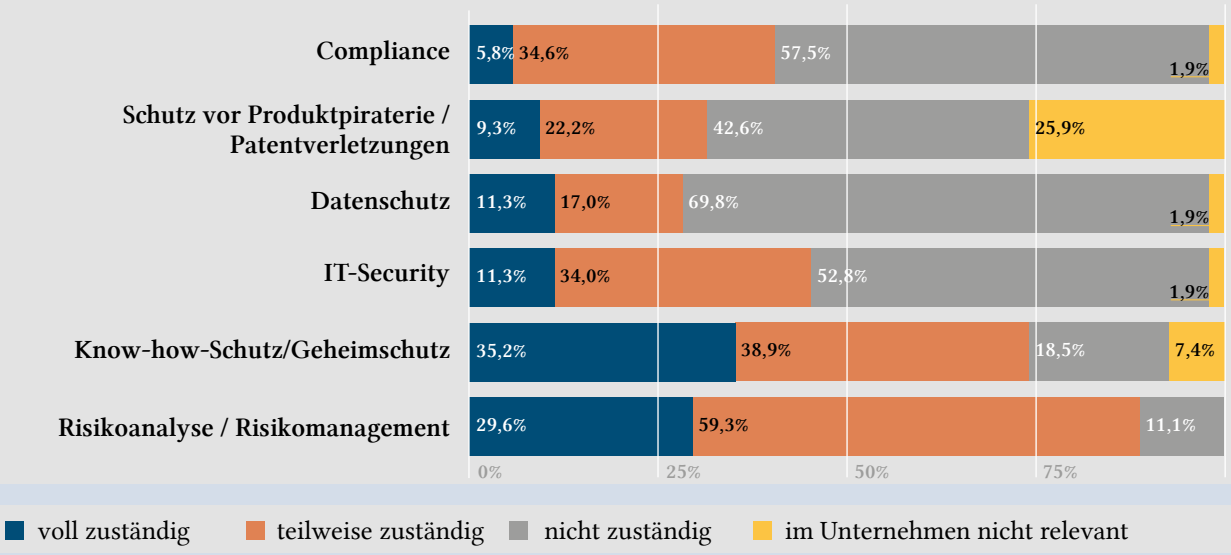
Die Angaben zu den einzelnen – im Fragebogen vorgegebenen – Zuständigkeitsbereichen werden nun zuerst

Tabelle 5: Zuständigkeitsbereiche nach Sicherheitsorganisation

Abteilung KONZERNSICHERHEIT (n=40) im Unternehmen	**Unternehmen mit einer anderen Organisation von Sicherheit (n=14)**
Hohe Zuständigkeiten (Summe aus „voll zuständig"/„teilweise zuständig", ≥ 80 %)	**Hohe Zuständigkeiten** (Summe aus „voll zuständig"/„teilweise zuständig", ≥ 60 %)
1. Unternehmensweite Sicherheitsstrategie (100 %) 2. Notfall- und Krisenmanagement (100 %) * 3. Interne Ermittlungen (95 %) ** 4. Risikoanalyse / Risikomanagement (92,5 %) 5. Werkschutz (92,5 %) 6. Event Security (92,5 %) 7. Reisesicherheit (90 %) 8. Know-how-Schutz / Geheimschutz (87,5 %) ** 9. Schutz vor Vermögens- und Wirtschaftsdelikten (87,5) * 10. Executive Protection (87,5 %) ** 11. Sicherheit am Arbeitsplatz (workplace violence) (82,5 %) 12. Business Continuity Management (80 %)	1. Unternehmensweite Sicherheitsstrategie (100 %) 2. Notfall- und Krisenmanagement (85,7 %) * 3. Werkschutz (85,7 %) 4. Arbeitssicherheit und Brandschutz (78,6 %) 5. Risikoanalyse / Risikomanagement (78,6 %) 6. Event Security (71,4 %) 7. Reisesicherheit (71,4 %) 8. Sicherheit am Arbeitsplatz (workplace violence) (71,4 %) 9. Interne Ermittlungen (69,2 %) **
Geringe Zuständigkeiten (Summe aus „voll zuständig"/„teilweise zuständig", ≤ 50%)	**Geringe Zuständigkeiten** (Summe aus „voll zuständig"/„teilweise zuständig", ≤ 50%)
1. Datenschutz (25 %) 2. Schutz vor Produktpiraterie / Patentverletzungen (35 %) 3. Compliance (37,5 %) 4. IT-Security (46,2 %) 5. Arbeitssicherheit und Brandschutz (50 %)	1. Schutz vor Produktpiraterie / Patentverletzungen (21,4 %) 2. Know-how-Schutz / Geheimschutz (35,7 %) ** 3. Datenschutz (38,5 %) 4. IT-Security (42,8 %) 5. Compliance (50 %)

Statistisch signifikante Unterschiede sind folgendermaßen gekennzeichnet: * p<.05, ** p<.01

Abbildung 6: Verantwortungs- und Zuständigkeitsbereich



in den Abbildungen für die Gesamtstichprobe (über die Organisationsformen und Länder hinweg) präsentiert. Danach werden jene Bereiche näher betrachtet, in denen die Länderergebnisse deutliche Unterschiede aufweisen.

Teilweise deutliche Unterschiede zwischen den Ländern

Richtet man den Fokus auf die beteiligten Länder, so zeigt sich ein etwas differenzierteres Bild – insbesondere wenn zudem die Nichtzuständigkeit oder die (angenommene) fehlende Relevanz einzelner Themenfelder betrachtet wird.

Information Security

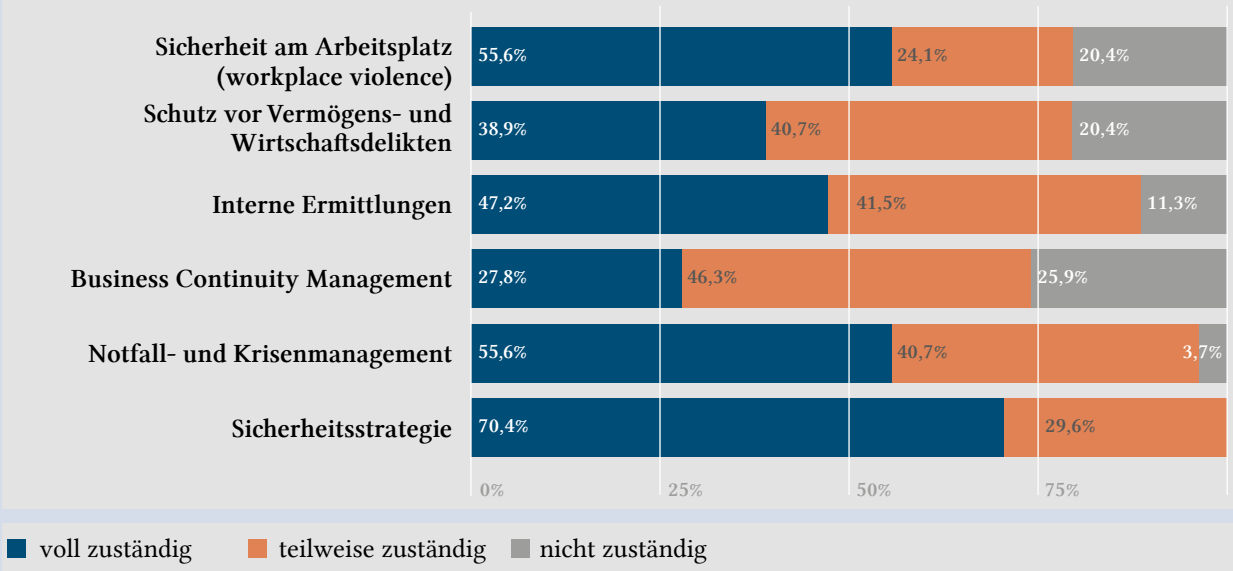
So geben 15,4 % der österreichischen Befragten an, dass „Know-how-Schutz / Geheimschutz" in ihrem Unternehmen nicht relevant sei (DE 3,1 %, CH 11,1 %). Damit wird das Thema bei einzelnen Unternehmen aus Österreich als weniger wichtig eingestuft als in den meisten Unternehmen der Nachbarländer. 30,8 % erklären, dass sie für diesen Bereich nicht zuständig seien (DE 15,6 %, CH 11,1 %).[8] Während in Deutschland und der Schweiz alle Abteilungen Konzernsicherheit für dieses Thema zuständig sind, ist dies in Österreich nicht der Fall.

Ein anderes interessantes Feld ist der Datenschutz: Während sich die Befragten aus deutschen Unternehmen mit 87,5 % als nicht zuständig beschreiben, sind dies mit 58,3 % bereits viel weniger Teilnehmende aus Österreich. In der Schweiz hingegen sind zwei Drittel der Befragten für den Datenschutz zumindest teilweise zuständig (DE 12,5 %, AT 41,7 %). Dieses Themenfeld scheint in einer Vielzahl von Unternehmen nicht der Sicherheit federführend zugeordnet zu werden.

Im Gegensatz dazu sind zwei von drei Teilnehmenden aus der Schweiz (66,7 %) für die IT-Security nicht zuständig. Dieser Anteil liegt bei den österreichischen Unternehmen

8 Allerdings sollte hier methodenkritisch angefügt werden, dass nicht ausgeschlossen werden kann, dass es bei der Beantwortung evtl. durch die gemeinsame Nennung von Know-how-Schutz und Geheimschutz zu Irritationen gekommen sein könnte.

Abbildung 7: Verantwortungs- und Zuständigkeitsbereiche



bei 58,3 % und bei den deutschen bei 46,9 %. In mehr als der Hälfte der deutschen Unternehmen – und damit in einem größeren Ausmaß als in Österreich und der Schweiz – besteht für dieses Thema (zumindest teilweise) eine fachliche Zuständigkeit.

Business Security – Unterschiede nach Ländern

Bei der Betrachtung von Risikoanalyse und Risikomanagement überrascht das Ergebnis aus Österreich: Insgesamt erklären sich nur 61,6 % der Befragten für diesen Bereich zuständig (15,4 % „voll zuständig"; 46,2 % „teilweise zuständig"); in Deutschland und der Schweiz sind es nahezu alle Teilnehmenden („voll zuständig": DE 37,5 %; CH 22,2 %; „teilweise zuständig"; DE 59,4 %; CH: 77,8 %).

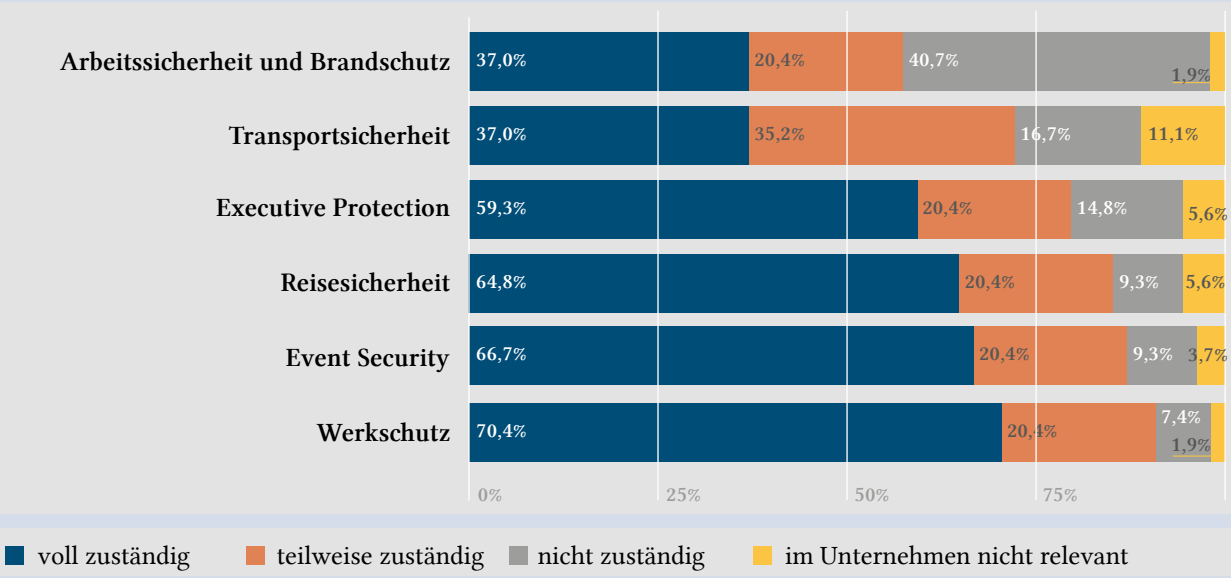
Ein ähnliches Bild ergibt die länderspezifische Untersuchung der Aufgabenwahrnehmung im Bereich des Schutzes vor Vermögens- und Wirtschaftsdelikten. In den befragten deutschen und schweizerischen Unternehmen liegt der Anteil der für diesen Bereich Zuständigen („voll zuständig"; „teilweise zuständig") mit 84,4 % bzw. 88,9 % (jeweils ca. 44 % „voll zuständig") vergleichbar hoch, während in den Unternehmen aus Österreich sich nur 61,5 % für zuständig erklären (nur 23,1 % „voll zuständig").

Physical Security – Unterschiede nach Ländern

Unter dieser Thematik sind diverse Verantwortungsbereiche subsumiert; die Antworten lassen meist keine deutlichen Länderunterschiede erkennen (wohl aber Unterschiede in Abhängigkeit vom Aufbau der Sicherheitsstruktur im Unternehmen, s.o.).

In folgenden Bereichen wiederholt sich allerdings das zuletzt beschriebene Verantwortlichkeitsmuster mit einem geringen Anteil an Teilnehmenden aus österreichischen Unternehmen, die für diese Bereiche zuständig sind (aufgelistet wird die Summe aus „voll zuständig"/„teilweise zuständig"): Event Security (AT 61,5 %, DE 93,8 %, CH 100 %), Reisesicherheit (AT 46,2 %, DE 96,9 %, CH 100 %), Executive Protection (AT 46,2 %, DE 90,6 %, CH 88,9 %).

Abbildung 8: Verantwortungs- und Zuständigkeitsbereiche



Ein anderes Bild hingegen zeigt sich bei den Bereichen Sicherheit am Arbeitsplatz (workplace violence) sowie Arbeitssicherheit und Brandschutz. Während Arbeitssicherheit und Brandschutz bei über 80 % der teilnehmenden schweizerischen und österreichischen Unternehmen in den Verantwortungsbereich der Sicherheitsverantwortlichen fallen (CH 88,9 %, AT 84,6 %), geben nur 37,5 % der deutschen Teilnehmenden hier eine Zuständigkeit an. Für die Sicherheit am Arbeitsplatz sind 92,3 % der Befragten aus Österreich und 100 % jener aus der Schweiz zuständig. In Deutschland ist dieses Feld für etwas mehr als zwei Drittel ein Zuständigkeitsbereich der Sicherheitsverantwortlichen. Insbesondere in den deutschen Unternehmen mit Konzernsicherheitsabteilungen liegt dieser Bereich in fast zwei Drittel der Unternehmen in einer anderen personellen Verantwortung (bspw. Brandschutzbeauftragter, Fachkraft für Arbeitssicherheit).

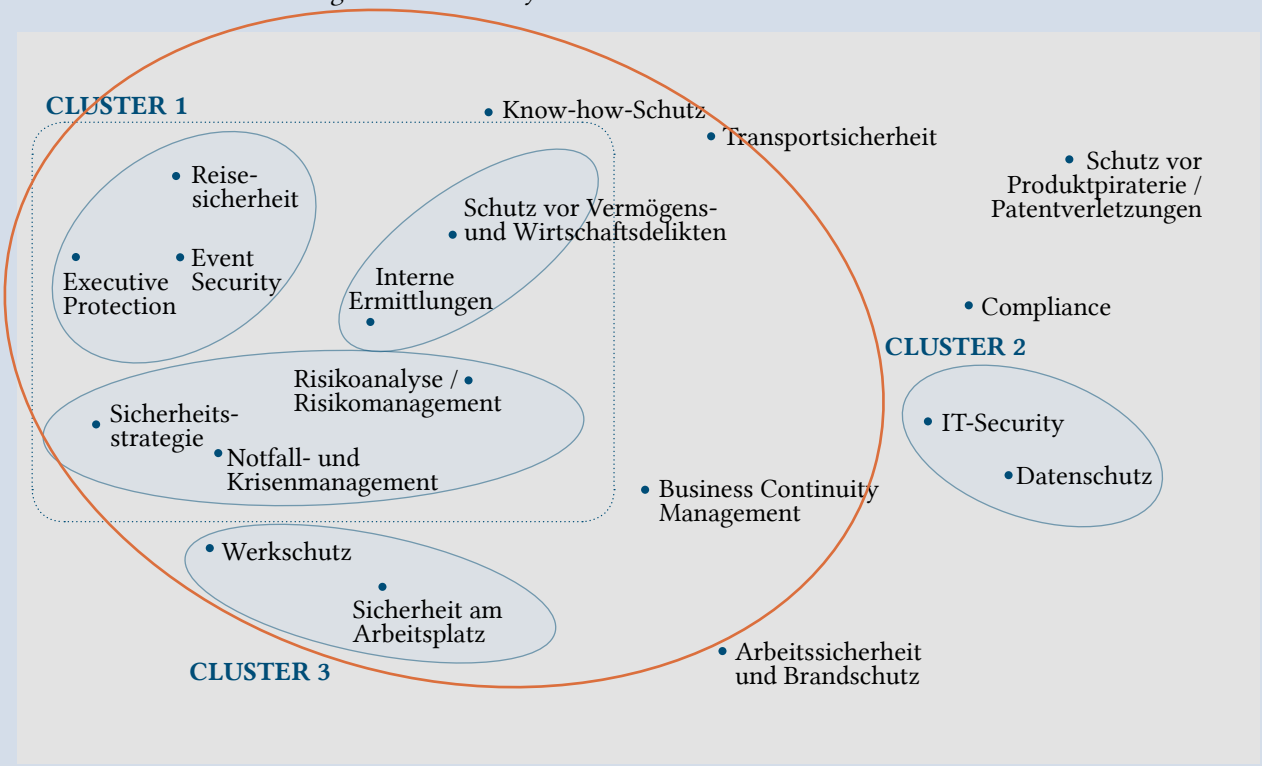
Drei Zuständigkeitscluster dominieren die Tätigkeit

Im Folgenden soll der Zusammenhang zwischen den einzelnen Tätigkeitsfeldern betrachtet werden.

Hierzu wird mittels einer multidimensionalen Skalierung auf Basis der Angaben der Befragten die relative Lage der Verantwortungsbereiche in einem mehrdimensionalen Raum untersucht, um durch die resultierende Konfiguration besondere Ähnlichkeiten und/oder Unähnlichkeiten aufzudecken. Über eine ebenfalls durchgeführte Clusteranalyse können homogene Objektgruppen identifiziert werden.

Die Aufgabenbereiche in Cluster 1 fallen am häufigsten in den Zuständigkeitsbereich der befragten Personen und stellen damit in der Praxis die Kernbereiche der Sicher-

Abbildung 9: Verantwortungs- und Zuständigkeitsbereiche
Multidimensionale Skalierung und Clusteranalyse



Je weiter die Objekte links angeordnet sind, desto häufiger (und vollständiger) fallen diese Themenkomplexe tendenziell in den Zuständigkeitsbereich der Befragten. Bei den Objekten, die sich am oberen Rand der Abbildung befinden, ist der Anteil der Befragten, die angaben, dass dieses Thema in ihrem Unternehmen nicht relevant sei, etwas höher als bei den übrigen. Je näher Themen beieinander liegen, desto häufiger wurde die Zuständigkeit ähnlich bewertet.
Die Objekte in einem Cluster treten häufig gemeinsam auf (oder auch – im Gegenzug – gemeinsam nicht auf). Wenn eine Person also angab, für einen Bereich aus dem Cluster zuständig zu sein, so war sie vielfach auch für die anderen Themen zuständig, die sich darin befinden. Sofern sie nicht zuständig war, fielen die weiteren Themen aus einem Cluster ebenfalls häufig nicht in ihren Zuständigkeitsbereich.

heitsverantwortlichkeiten großer Unternehmen dar. Die Gemeinsamkeit der Themenbereiche aus Cluster 2 (IT-Security und Datenschutz) besteht – neben der inhaltlichen Nähe bzw. der Bedeutung des IT-Bereichs für den Datenschutz – insbesondere in der relativen Häufigkeit der Nichtzuständigkeit für diese Themenfelder. Die besondere Nähe der Objekte in Cluster 3 – Zuständigkeit für den Werkschutz und für die Sicherheit am Arbeitsplatz (Schutz vor Gewalt am Arbeitsplatz) – mag darin begründet sein, dass bei Zuständigkeit für den Produktionsbereich auch das Thema „workplace violence" von größerer Bedeutung ist und in den eigenen Aufgabenbereich fällt.

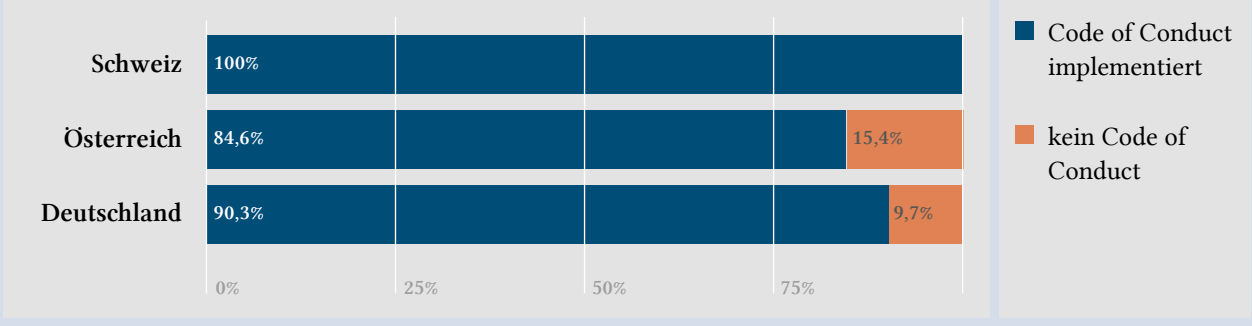
Für die Untergruppe der Unternehmen mit Konzernsicherheitsabteilungen umfasst der primäre Zuständigkeitsbereich neben den Clustern 1 und 3 die Themen „Know-how-Schutz" und „Business Continuity Management" sowie – sofern relevant – „Transportsicherheit bzw. Sicherheit der Lieferkette".

3.5 Code of Conduct, Policys und Hinweisgebersysteme

Ein weiterer Schwerpunkt der vorliegenden Untersuchung liegt in der Erhebung des Standes zur Implementierung von Verhaltensrichtlinien im Unternehmen. Im Folgenden wird zunächst die Umsetzung eines Codes of Conduct[9] behandelt; dabei wird allerdings nur auf einzelne übergeordnete Aspekte dieses Themenfelds eingegangen. Im Mittelpunkt der Erhebung standen in diesem Bereich der Umgang mit dem Thema Whistleblowing und Hinweisgebersysteme.

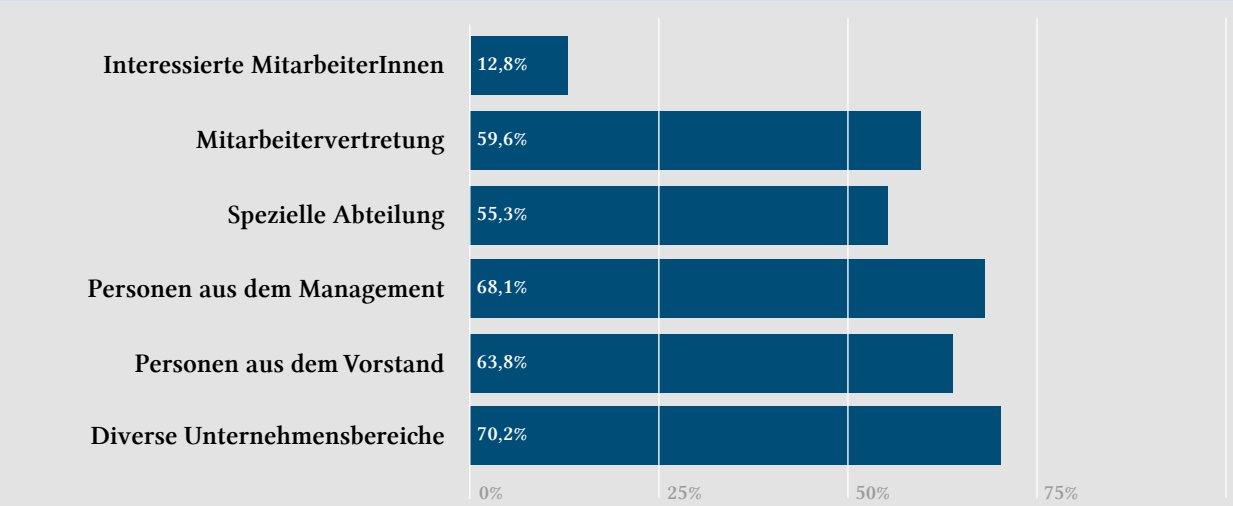
Insgesamt 90,6 % der Befragten geben an, dass in ihrem Unternehmen eine Verhaltensrichtlinie existiert, an der sich die Unternehmensangehörigen orientieren können. In der Schweiz geben sämtliche Befragten an, dass in ihrem Unternehmen ein Code of Conduct umgesetzt sei; in Deutschland sind es noch 90,3 %; in Österreich ist der Anteil mit 84,6 % am geringsten.

Abbildung 10: Code of Conduct



9 Dieser wird vielfach als Instrument der Unternehmensethik (Kaptein & Schwartz 2008), als integraler Bestandteil eines Compliancesystems (Wecker & van Laak 2009) oder sogar als „Verfassung" des Unternehmens (Hofmann 2008) umschrieben.

Abbildung 11: Beteiligte an der Entwicklung des Codes of Conduct



Wer war an der Entwicklung und Erstellung der Verhaltensrichtlinie beteiligt? Wurden unterschiedliche Abteilungen und Personengruppen einbezogen? Die Angaben beziehen sich im Folgenden auf die Unternehmen, die einen Code of Conduct haben. In einzelnen Fällen (3,4 %) wurde die Verhaltensrichtlinie nicht im eigenen Unternehmen entwickelt. Hierbei handelt es sich ausschließlich um Unternehmen aus Deutschland. In Abbildung 11 wird die Eingebundenheit in die Erstellung des Codes aufgeführt, wobei Mehrfachnennungen möglich waren. Zunächst wird deutlich, dass an der Entwicklung letztlich eine Vielzahl von Personen aus den Unternehmen beteiligt wurde.

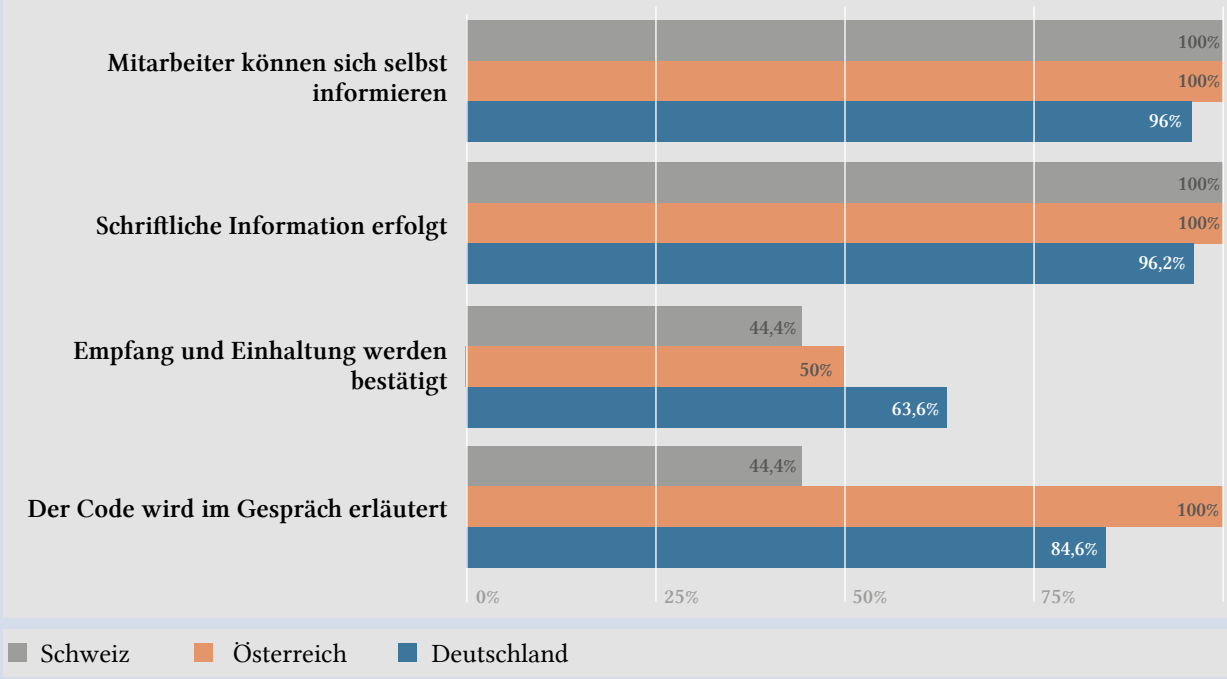
Zunächst fällt der hohe Anteil der Beteiligung des Vorstands auf. In Deutschland und der Schweiz haben jeweils zwei Drittel der Befragten dessen Mitwirken angegeben, in Österreich immerhin noch 54,5 %. Bei der Einbindung von Personen aus dem Management ist der Anteil bei den befragten schweizerischen Unternehmen mit 77,8 % erneut deutlich höher (DE 66,7 %, AT 63,6 %).

Die Beteiligung der Mitarbeitervertretung war in den Schweizer Unternehmen mit 44,4 % geringer ausgeprägt als in den Nachbarländern (DE 63 %, AT 63,6 %). Dies relativiert sich allerdings, sobald der Blick auf die Mitwirkungsmöglichkeit für interessierte Mitarbeiter und Mitarbeiterinnen fällt: Während deren Anteil in den deutschen Unternehmen bei 3,7 % und in den österreichischen bei 9,1 % lag, gaben die Schweizer Befragten einen Anteil von 44,4 % an.

Die Art und Weise der Bekanntmachung ist für die Implementierung der Verhaltensrichtlinie im Unternehmen essenziell, um die nötige Verbindlichkeit und persönliche Verpflichtung der einzelnen Unternehmensangehörigen zu erreichen.

Mitarbeitende können sich i.d.R. selbst informieren und erhalten zudem eine schriftliche Information über die unternehmensweite Verhaltensrichtlinie. Allerdings werden insgesamt nur in etwas mehr als der Hälfte der befragten Unternehmen (56,1 %) der Empfang der Un-

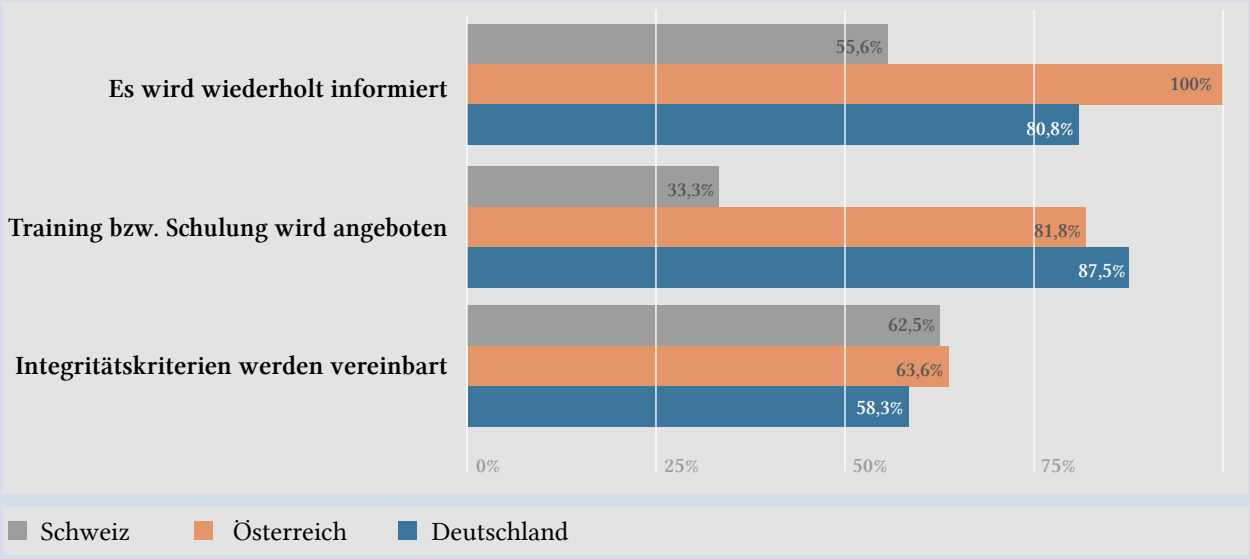
Abbildung 12: Information der Unternehmensangehörigen



terlagen und auch die Einhaltung der dort verankerten Verhaltensweisen jeweils schriftlich durch die Unternehmensangehörigen bestätigt. In vier von fünf Unternehmen (80,4 %) wird der Code of Conduct mündlich erörtert, um Verständnis und Nachvollziehbarkeit zu erhöhen. Bemerkenswert ist, dass bei den teilnehmenden schweizerischen Unternehmen die beiden letztgenannten Maßnahmen jeweils nur in 44,4 % der Fälle angewendet werden.

Eine wiederholte Information in Form von Änderungsmitteilungen oder einer Auffrischung der Inhalte erfolgt über die Gruppe hinweg im gleichen Ausmaß wie die Kommunikation über die Verhaltensrichtlinie (80,4 %); das ist bei schweizerischen Unternehmen geringer ausgeprägt. Zu einem noch geringeren Anteil wird in diesen Unternehmen ein Training oder eine Schulung zum Thema ‚Ethik' angeboten. Nur geringe Unterschiede zwischen den drei Ländern gibt es im Hinblick auf die Aufnahme von Integritätskriterien in die Zielvereinbarungen mit Führungskräften.

Abbildung 13: Information der Unternehmensangehörigen



In der Umfrage wurde auch das Vorhandensein weiterer Richtlinien bzw. Policys im Unternehmen erhoben: In sämtlichen befragten Unternehmen existiert eine Datenschutzrichtlinie, in (nur) 83 % eine Anti-Korruptions-Policy. Letztere ist am häufigsten in den teilnehmenden Unternehmen aus Deutschland und Österreich implementiert.

Abbildung 14: Vorhandensein ausgewählter Policys

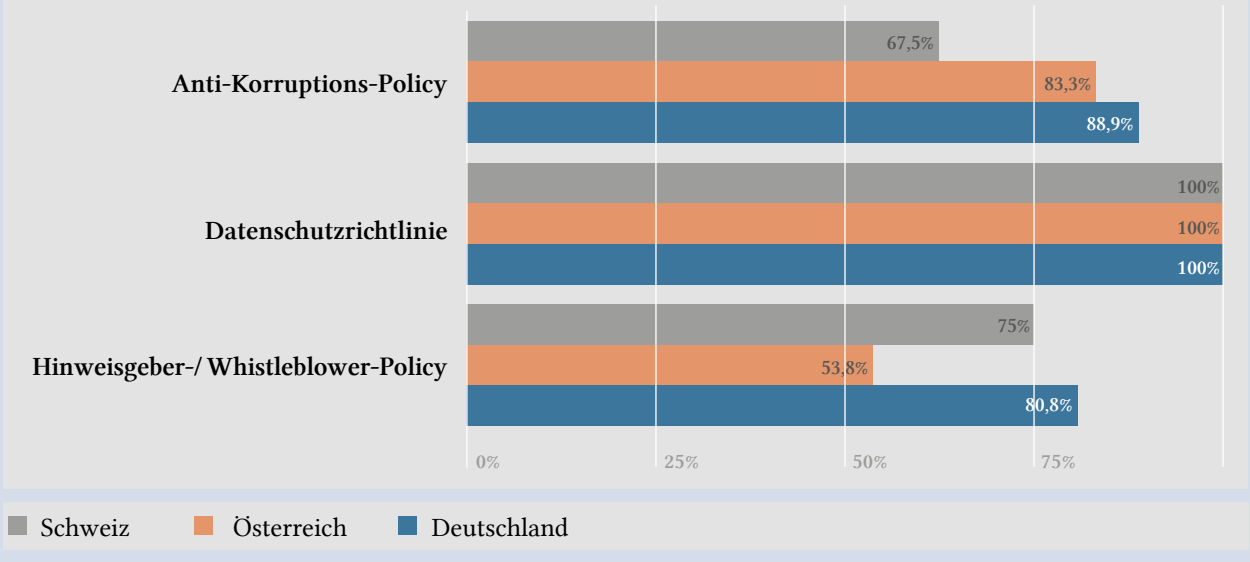
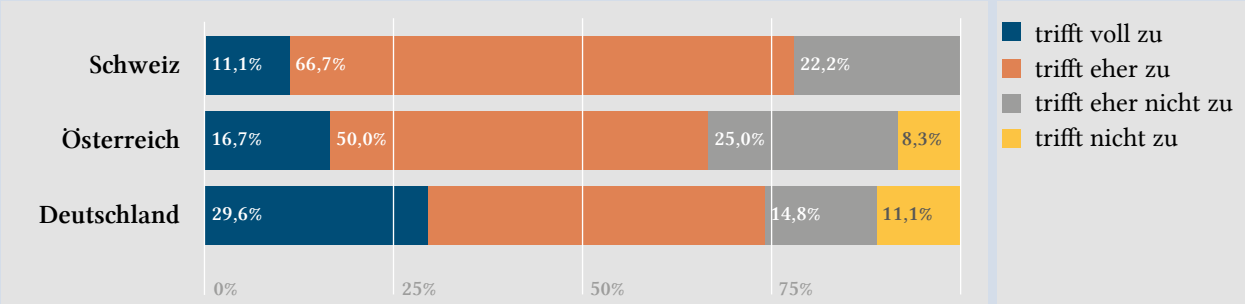


Abbildung 15: Unser Unternehmen fördert das interne Whistleblowing



Sehr unterschiedlich ist die Situation in Bezug auf eine Hinweisgeber- oder Whistleblower-Policy: Diese ist in vier Fünfteln der deutschen, drei Vierteln der schweizerischen, jedoch nur in etwas mehr als der Hälfte der österreichischen Unternehmen eingeführt. Darüber hinaus gibt es in den Unternehmen eine Vielzahl weiterer (Security-)Policies.

Hinweisegebersysteme: Nachholbedarf in Österreich

73,1 % aller befragten Unternehmen geben an, dass neben der Policy bei ihnen ein Hinweisgebersystem implementiert ist; bei weiteren 5,8 % befindet sich dieses aktuell im Aufbau. Auch in diesem Bereich sind die Unterschiede zwischen den einzelnen Ländern beträchtlich: Während von den deutschen Unternehmen nur 6,7 % und von den schweizerischen 22,2 % über kein (zumindest geplantes) Hinweisgebersystem verfügen, liegt der Anteil in Österreich mit 53,8 % deutlich höher.

Dabei gäbe es durchaus Bedarf: Betrachtet man nämlich die Einschätzungen der Befragten zur Förderung von internen Mitteilungen unternehmensschädigenden Verhaltens durch Mitarbeitende, bejahen zwei Drittel der österreichischen Befragten eine solche Förderung des internen Whistleblowings („trifft voll zu“ und „trifft eher zu“). Dies erfolgt allerdings nach o.g. Ergebnis in vielen Fällen nicht über die Verfügbarmachung eines Hinweisgebersystems.

Über die Länder hinweg sind es rund drei Viertel der befragten Unternehmen (72,9 % „trifft voll zu“ und „trifft eher zu“), die das interne Hinweisgeben zumindest in Ansätzen fördern. In einem ähnlich großen Ausmaß wird der Aussage widersprochen, dass im eigenen Unternehmen Hinweisgeber nicht von Bedeutung seien (75,5 % „trifft eher nicht zu“ und „trifft nicht zu“).

Die befragten deutschen Unternehmen sind in großem Umfang von einem (relativ) hohen Schutz für Hinweisgebende überzeugt; dieser wird weniger positiv in Österreich und der Schweiz bewertet.

Mehr als jeder dritte Befragte hält das Thema „Whistleblowing“ für (eher) überschätzt. Eine Ausnahme bilden die Befragten der schweizerischen Unternehmen, die diese Aussage mit 88,9 % für (eher) nicht zutreffend erachten.

Abbildung 16: Bei uns sind Hinweisgeber/innen nicht von Bedeutung

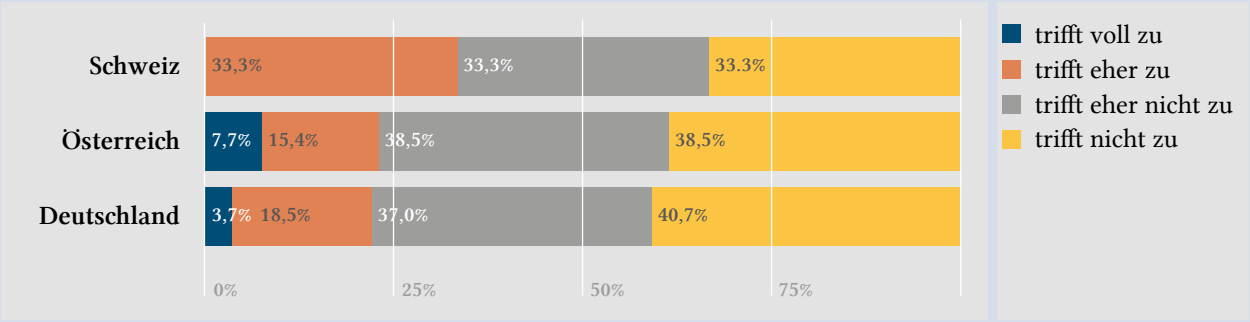


Abbildung 17: Wir haben einen sehr hohen Schutz für Whistleblower

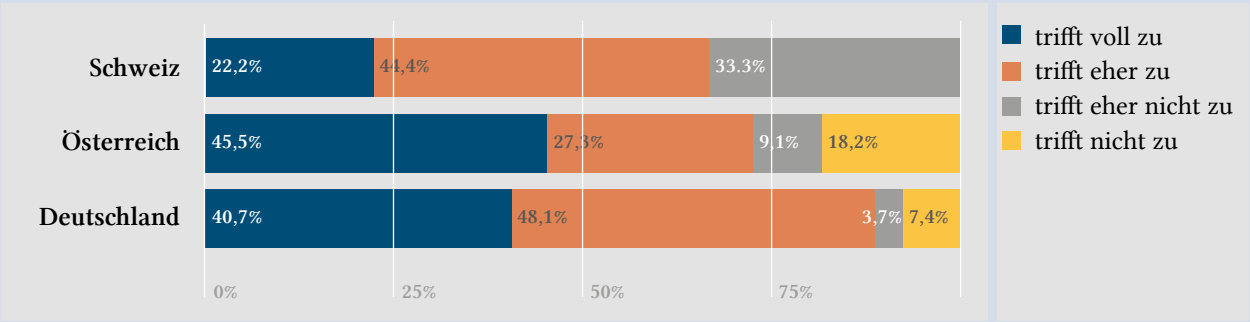
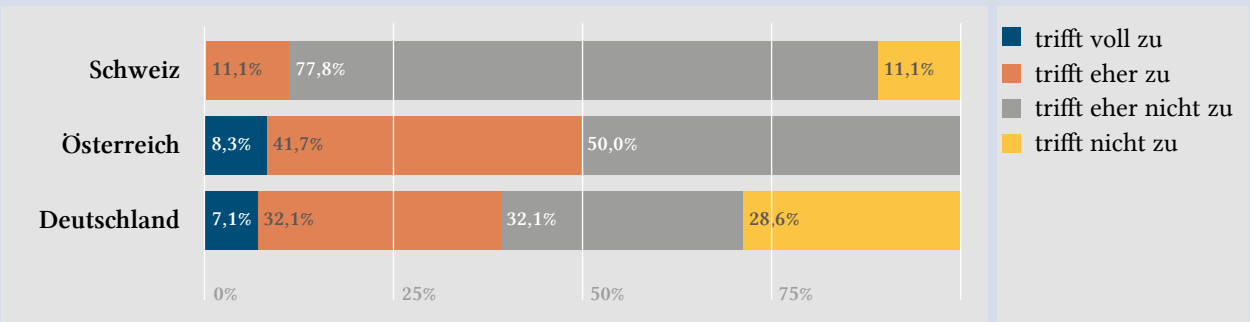


Abbildung 18: Das Thema Whistleblowing wird allgemein überschätzt



3.6 Kriminalitätsbelastung und Kriminalitätserfassung

Jedes Unternehmen kann von kriminellen Delikten betroffen sein. Gerade große Unternehmen geraten oft ins Visier und viele mögliche Delikte werden gar nicht als solche erkannt oder den Behörden mitgeteilt. Die Angaben aus der Befragung beziehen sich jeweils auf einen Referenzzeitraum von 24 Monaten. Die Antwortmöglichkeiten beinhalteten neben dem expliziten Ausschließen, Opfer eines Delikts geworden zu sein, die Möglichkeit, die einmalige oder häufigere Betroffenheit anzugeben oder eine etwaige Unsicherheit einzuräumen („nicht auszuschließen").

Im Folgenden werden zunächst die Gesamtergebnisse präsentiert, um anschließend auf Unterschiede zwischen den Ländern einzugehen sowie insbesondere etwaige Unterschiede im Hinblick auf die Sicherheitsorganisation (Konzernsicherheit ja/nein) und damit die Größe des Unternehmens in den Mittelpunkt zu stellen.

Eigentums- und Vermögensdelikte: Deutliche Unterschiede

Von den vorgegebenen Delikten haben Eigentums- und Vermögensdelikte die größte Häufigkeit. Diebstahl und Unterschlagung hat in den befragten Unternehmen eine 2-Jahres-Prävalenz von 83 %. Das nächsthäufige Delikt ist Betrug mit einer Prävalenzrate von 58,3 %, gefolgt von Untreue mit 49 %.

Bei Betrachtung der Länder zeigt sich für die beiden letztgenannten Deliktsbereiche eine besondere Situation. Österreichische Unternehmen gaben in weit geringerem Ausmaß an, betroffen zu sein: bei Betrugsfällen lediglich 18,2 % (im Gegensatz zu DE 71,5 % und CH 66,7 %), bei Untreue 36,4 % (DE 55,6 %, CH 51,8 %).

Wettbewerbsdelikte: Fälschung vor Datenverlust, hohe Unsicherheit

Bei den Wettbewerbsdelikten zeigt sich die höchste Betroffenheit bei Produktfälschungen mit 21,2 % (gleichzeitig eine hohe Nicht-Betroffenheit mit 57,4 %), gefolgt von Diebstahl von vertraulichen Unternehmensdaten (und damit Know-how-Verlust) mit 19,5 %, Diebstahl von vertraulichen Kundendaten mit 15,5 % und der Betroffenheit von

Abbildung 19: Eigentums- und Vermögensdelikte – Betroffenheit des Unternehmens

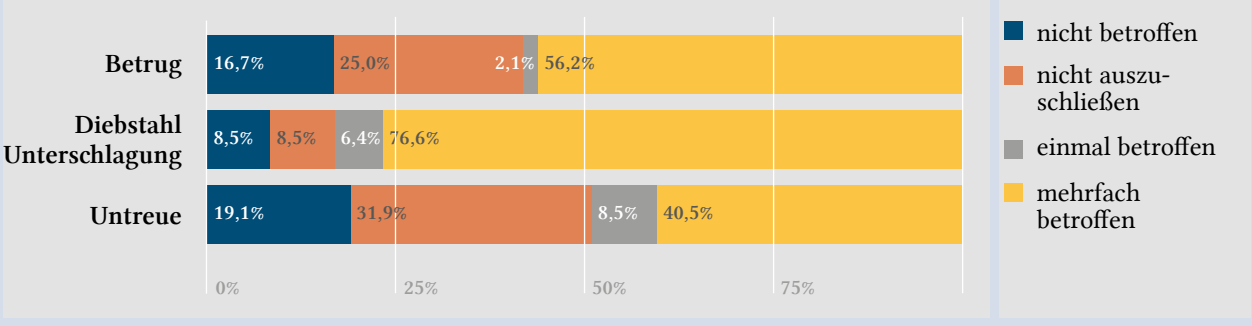
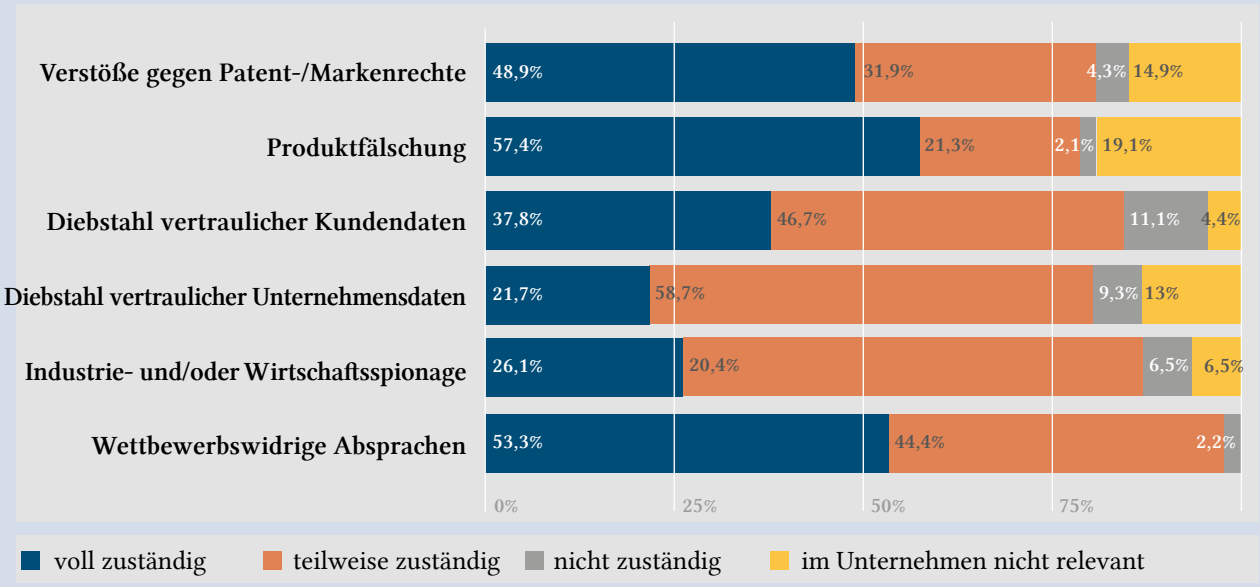


Abbildung 20: Wettbewerbsdelikte - Betroffenheit des Unternehmens



Industrie- und/oder Wirtschaftsspionage mit 13 %. In den drei letztgenannten Bereichen ist allerdings auch die Unsicherheit in Bezug auf die mögliche Betroffenheit besonders stark ausgeprägt (46,7 % bis 60,9 %).

Darüber hinaus werden von 22,7 % der befragten Unternehmen ein Fall bzw. mehrere Fälle von Korruption und Bestechung in den vergangenen 24 Monaten angegeben. Zudem sind – in geringerem Ausmaß – Fälle von Kartellrechtsverstößen (9 %) und Geldwäsche (8,8 %) bekannt geworden. Bei Falschbilanzierung gab es keine Angaben zur festgestellten Betroffenheit. Die Angaben zu „nicht auszuschließen" sind jeweils Anzeichen für die Annahme einer gewissen Dunkelziffer an unentdeckt bleibenden Fällen.

Abbildung 21: Andere wirtschaftskriminelle Delikte – Betroffenheit des Unternehmens

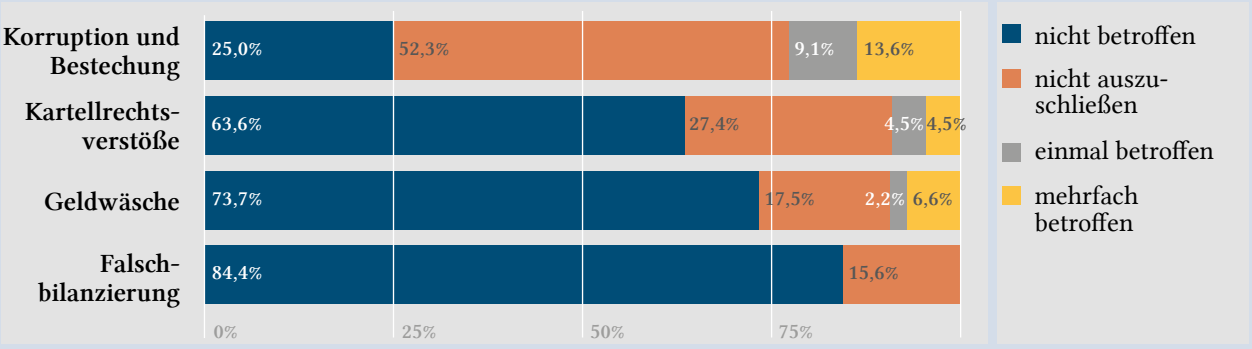
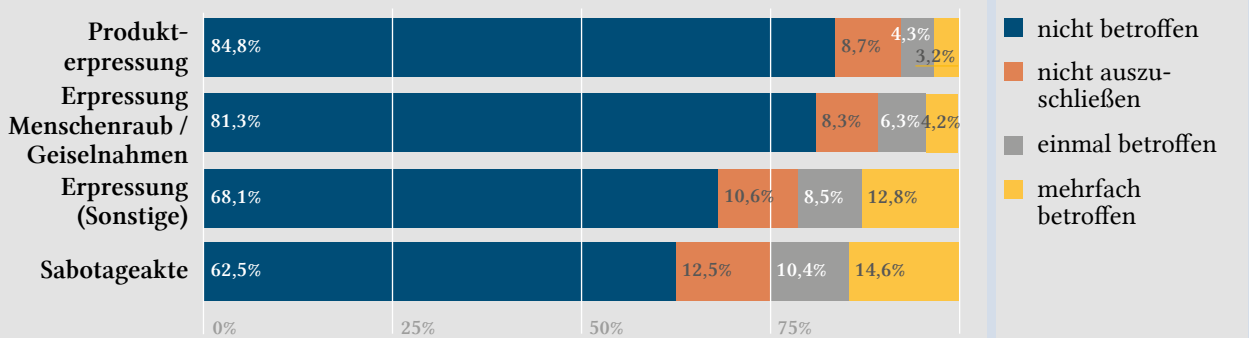


Abbildung 22: Erpressung und Sabotage – Betroffenheit des Unternehmens



Verbreitung von Erpressung und Sabotage

Eines von vier Unternehmen war in den zwei Jahren vor der Befragung Opfer von Sabotageakten. Unterschiedliche Formen der Erpressung dürften ebenfalls für einen nicht unerheblichen Anteil der Unternehmen von Bedeutung sein: 6,5 % waren in den vergangenen zwei Jahren von Fällen der Produkterpressung und sogar 10,5 % von erpresserischem Menschenraub bzw. Geiselnahmen betroffen. Weitere Formen der Erpressung wurden von 21,3 % der Befragten berichtet.

Die Prävalenz soll nachfolgend in Abhängigkeit von der Sicherheitsorganisation im Unternehmen dargestellt werden, da davon auszugehen ist, dass insbesondere die größten Konzerne (mit entsprechenden Corporate Security Abteilungen) den meisten Delikten ausgesetzt sind.

Die dargestellten Prävalenzraten zeigen in welchem außergewöhnlichen Maß große Konzerne von Delikten betroffen sind. Da die Angaben sich auf das unternehmensinterne Hellfeld beziehen, ist von weiteren – nicht bekannt gewordenen – Fällen auszugehen. Deutlich wird diese Annahme, wenn die Befragten eine Betroffenheit nicht ausschließen wollen. Die Teilnehmenden aus den Konzernsicherheiten (im Vergleich zu den anderen Si-

Tabelle 6: Kriminalitätsbelastung nach Sicherheitsorganisation (2-Jahres-Prävalenz)

Delikte	Abteilung Konzernsicherheit (n=40) im Unternehmen	Unternehmen mit einer anderen Organisation von Sicherheit (n=14)
Betrug **	69,5 %	25,0 %
Diebstahl / Unterschlagung ***	97,2 %	36,4 %
Untreue	57,2 %	25,0 %
Delikte	**Abteilung Konzernsicherheit (n=40) im Unternehmen**	**Unternehmen mit einer anderen Organisation von Sicherheit (n=14)**
Verstöße gegen Patent- / Markenrechte	22,9 %	8,3 %
Produktfälschung *	25,7 %	8,3 %
Diebstahl vertraulicher Kundendaten	14,3 %	20,0 %
Diebstahl von Know-how, von vertraulichen Unternehmensdaten *	22,8 %	9,1 %
Industrie- und/oder Wirtschaftsspionage“	14,3 %	9,1 %
Wettbewerbswidrige Absprachen	2,9 %	0,0 %
Korruption und Bestechung	30,3 %	0,0 %
Kartellrechtsverstöße	12,2 %	0,0 %
Geldwäsche	8,8 %	8,3 %
Falschbilanzierung / Fälschung von Jahresabschlüssen	0,0 %	0,0 %
Sabotageakte	29,7 %	10,0 %
Produkterpressung	5,8 %	9,1 %
Erpresserischer Menschenraub / Geiselnahme	13,5 %	0,0 %
Erpressung (sonstige)	25,0 %	9,1 %

Statistisch signifikante Unterschiede sind folgendermaßen gekennzeichnet: * p<.05, ** p<.01, p<.001

cherheitsverantwortlichen) gaben dies insbesondere bei Industrie- und/oder Wirtschaftsspionage mit 71,4 % (vs. 27,3 %), bei Diebstahl von Know-how mit 65,7 % (vs. 36,4 %) und von vertraulichen Kundendaten mit 51,4 % (vs. 30 %) sowie Wettbewerbswidrigen Absprachen mit 54,3 % (vs. 10 %) an.

Auswertung und Kommunikation von Delikten

In welcher Form werden die Delikte erfasst, ausgewertet und im Unternehmen kommuniziert? Der folgende Abschnitt befasst sich mit der Erfassung und Aufbereitung von Vorfällen.

Insgesamt 72,3 % aller befragten Unternehmen geben an, kriminelles Verhalten in allen Deliktsbereichen systematisch zu erfassen. Weitere 6,4 % beschränken die Erfassung auf spezifische Deliktsfelder. Bedeutsame Länderunterschiede gibt es in dieser Frage nicht.

Die Daten zu weiteren Details dieser systematischen Kriminalitätserfassung beziehen sich ausschließlich auf jene Unternehmen, die eine solche statistische Erhebung durchführen.

Abbildung 23: Systematische Erfassung bekannt gewordener Vorfälle/Taten

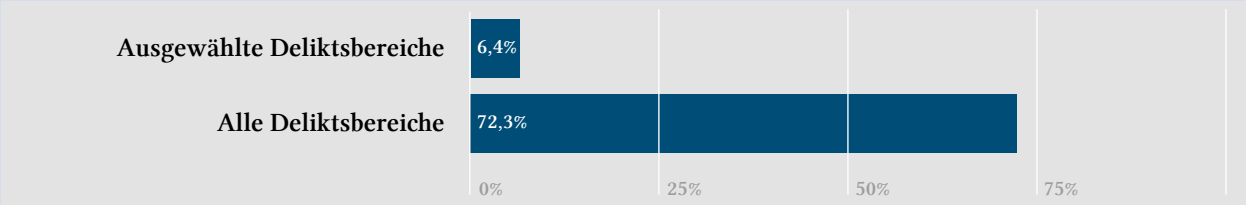
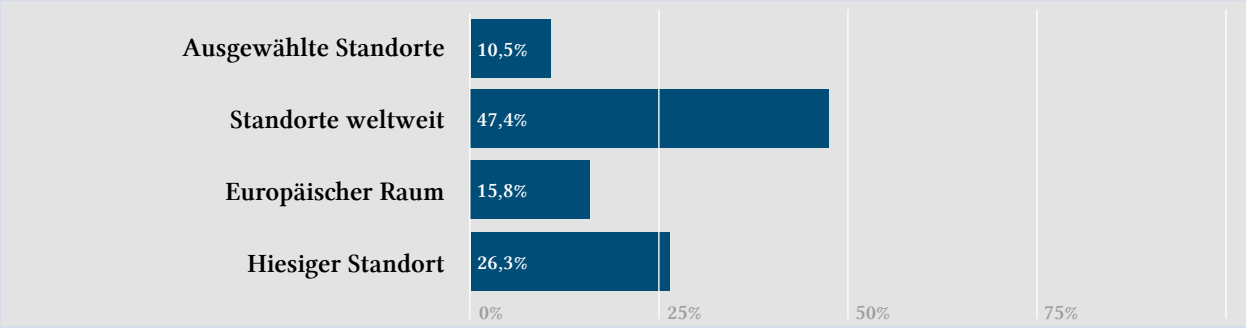


Abbildung 24: Ausdehnung der systematischen Erfassung bekannt gewordener Vorfälle/Taten

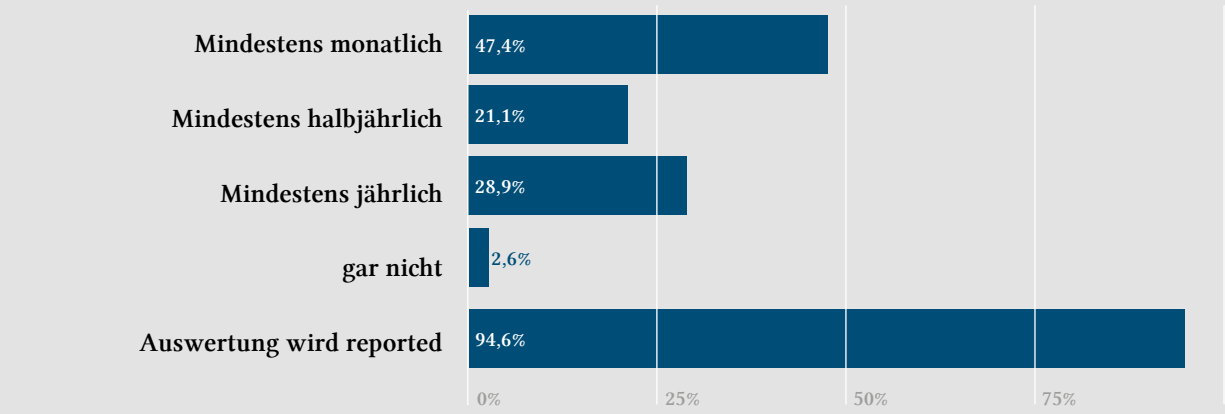


Global agieren, lokal erfassen?

Wie bereits eingangs erwähnt sind die teilnehmenden Unternehmen, Banken und/oder Versicherungen überwiegend transnational tätig. Sie sind im Durchschnitt in 42 Ländern vertreten (Median: 30 Länder); nahezu zwei Drittel (64,5 %) sind auf mindestens vier Kontinenten aktiv.

In nahezu der Hälfte der Unternehmen, die Delikte zielgerichtet erfassen, bezieht sich dieses Vorgehen auf alle Standorte des Unternehmens weltweit (47,4 %), während sich ca. ein Viertel der Unternehmen auf den Heimatstandort (26,3 %), jedes sechste auf den europäischen Raum (15,8 %) und jedes zehnte auf nach anderen Kriterien ausgewählte Standorte (10,5 %) beschränkt.

Abbildung 25: Häufigkeit und Kommunikation der Auswertung



Berichtswesen unterschiedlich organisiert

Die erhobenen Daten zu den bekanntgewordenen Vorfällen werden von annähernd der Hälfte dieser Unternehmen monatlich ausgewertet, von der anderen Hälfte halbjährlich oder jährlich. In 94,6 % der Fälle werden die Ergebnisse an das Management berichtet.

3.7 Einschätzungen zukünftiger Entwicklungen

Abschließend wurden noch Einschätzungen und konkrete Erwartungen zu möglichen künftigen Entwicklungen des Berufsfeldes abgefragt.

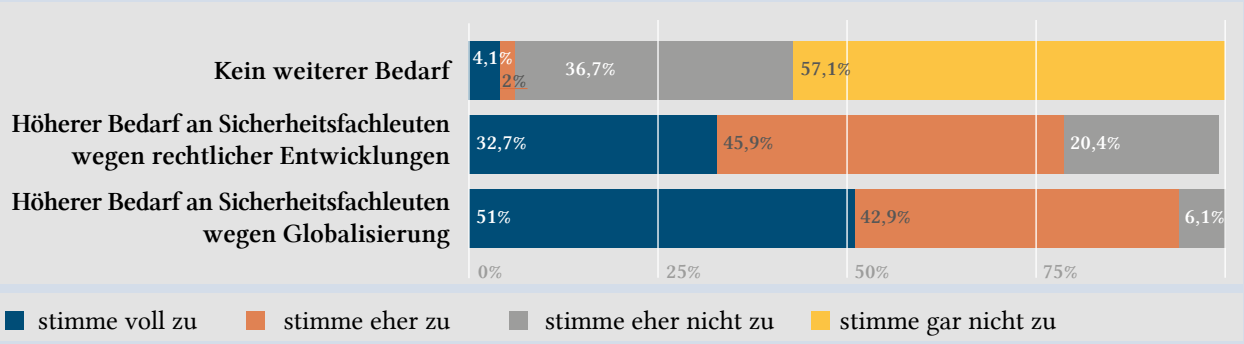
Erwartungen: Höherer Bedarf an Sicherheitsfachleuten

Bereits heute bestimmen zahlreiche rechtliche Rahmenbedingungen das Arbeitsfeld der Sicherheitsverantwortlichen. Der Aussage, dass es wegen der rechtlichen Entwicklung künftig einen höheren Bedarf an Sicherheitsfachleuten geben werde, stimmten 32,7 % voll und 46,9 % eher zu. Diese Erwartung teilten 20,4 % nicht („stimme eher nicht zu“).

Gerade die TOP100-Unternehmen agieren global vernetzt, was besondere Herausforderungen für die Sicherheitsverantwortlichen bedeutet. Eindeutig wird die fortschreitende Globalisierung als noch stärkerer Grund für einen höheren Bedarf an Fachleuten für Sicherheitsthemen eingeschätzt: Hier stimmten 51,0 % „voll“ und 42,9 % “eher“ zu, im Gegensatz zu 6,1 % der Antwortenden, die „eher nicht“ zustimmten.

Keinen weiteren Bedarf an Sicherheitsfachleuten dagegen sehen 4,1 % bzw. 2,0 % der Antwortenden (Zustimmung „voll“ oder „eher“). 36,7 % stimmten hier „eher nicht“ zu, eine deutliche Mehrheit von 57,1 % stimmte gar nicht zu.

Abbildung 26: Bedarf an Fachleuten im Sicherheitsbereich



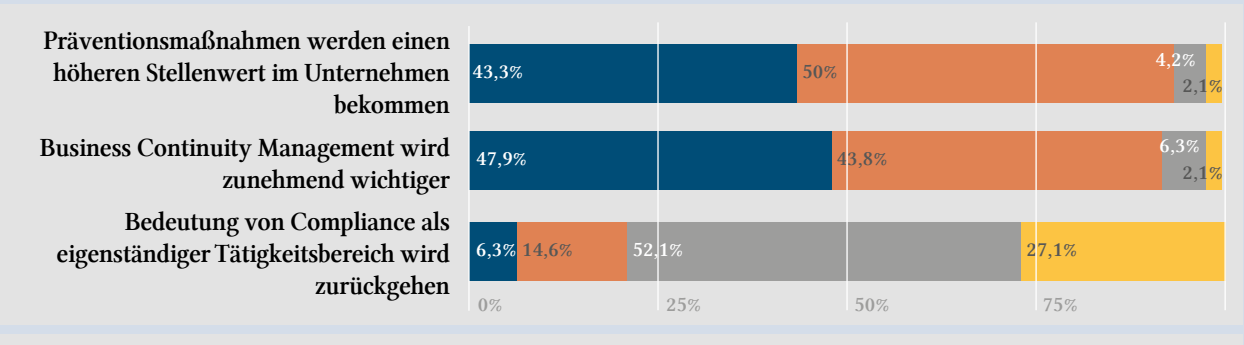
Zukünftige Bedeutung von Compliance, BCM und Prävention

Compliance wird nach Einschätzung der Sicherheitsverantwortlichen der TOP100 auch künftig ein eigenständiges Arbeitsfeld bleiben: Dass die Bedeutung von Compliance zurückgehen wird, nimmt nur jeder Fünfte an („stimme voll zu“ / „stimme eher zu“), fast 80 % der Befragten glauben dies nicht.

Eindeutig als Zukunftsthema wurde Business Continuity Management identifiziert: Der Aussage „Business Continuity Management wird zunehmend wichtiger“ stimmten 47,9 % der Antwortenden voll und weitere 43,8 % eher zu. 6,3 % stimmten „eher nicht“ und 2,1 %, „gar nicht“ zu. Hier können unternehmens- oder brancheninterne Besonderheiten ausschlaggebend sein.

Präventionsmaßnahmen bekommen nach Meinung der Befragten ebenfalls einen höheren Stellenwert. Volle Zustimmung kommt hier von 43,8 % der Antwortenden, 50,0 % stimmten eher zu. Ablehnung kommt hier nur von 3,7 % (eher) bzw. 1,9 % (voll).

Abbildung 27: Zukünftige Entwicklungen



4. Diskussion der bisherigen Ergebnisse

Bevor ausgewählte Erkenntnisse in einem größeren Zusammenhang diskutiert werden, soll noch einmal darauf hingewiesen werden, dass angesichts der Größe und der Besonderheiten der Stichprobe – die Teilnehmenden gehören zu den umsatzstärksten Unternehmen sowie den größten Banken und Versicherungen der beteiligten Länder – eine Generalisierung auf alle Wirtschaftsunternehmen der beteiligten Länder selbstverständlich nicht möglich ist.

Während einige Ergebnisse im Bereich der Erwartungen liegen und die bisherigen Erfahrungswerte bestätigen, bedürfen andere einer näheren Betrachtung.

Unternehmensstruktur, Kriminalitätsbelastung und internationale Präsenz

Bedeutsam ist etwa die unterschiedliche Strukturierung der Aufbauorganisation, die in den untersuchten Unternehmen zwischen Deutschland, Österreich und der Schweiz stark differiert: In nahezu 90 % der Unternehmen aus Deutschland existieren Konzernsicherheitsabteilungen, in der Schweiz dagegen etwa in zwei Dritteln und in Österreich überhaupt nur mehr in 50 % der Unternehmen. Deutliche Unterschiede bestehen im Hinblick auf die internationale Präsenz der Unternehmen mit Konzernsicherheitsabteilungen im Vergleich zu jenen, die Sicherheit anders organisieren. Erstere sind im Durchschnitt in wesentlich mehr Ländern vertreten (M=52,2 im Vergleich zu M=8,4).

Die ausgeprägte internationale Unternehmenstätigkeit dürfte sehr eng mit der unternehmensweiten Kriminalitätsbelastung zusammenhängen: Bei Vorhandensein einer Konzernsicherheitsabteilung wurde eine bis zu drei Mal höhere Betroffenheit angegeben.

Zudem liegt die Vermutung nahe, dass im Rahmen einer eigenen Abteilung für Konzernsicherheit ein stärkerer Fokus auf ein Monitoring und Lagebild gelegt wird. Ein weiterer Umstand ist, dass ein weltweites Monitoring der Kriminalitätsbelastung in Deutschland in mehr als der Hälfte der Unternehmen erfolgt, in Österreich und der Schweiz lediglich bei einem Drittel.

Kriminalitätsbelastung – Einordnung der Erkenntnisse

Vergleicht man die vorliegende Studie mit anderen Untersuchungen zu dieser Thematik, so ist fast durchgehend eine weit größere Kriminalitätsbelastung festzustellen. Hier sei nochmals hervorgehoben, dass sich die vorliegende Studie ausschließlich auf Großunternehmen bezieht, während ansonsten durchaus auch die klein- und mittelständischen Unternehmen mitbetrachtet werden. So steigt bereits rein statistisch mit zunehmender Unternehmensgröße das Risiko, von (wirtschafts-)kriminellen Handlungen betroffen zu sein.

Dass Diebstahl/Unterschlagung sowie Betrug und Untreue die häufigsten Delikte sind, von denen große Unternehmen betroffen sind, wird durch andere Studien bestätigt. So waren bspw. in der jüngsten Studie der KPMG (2014), die sich auf N=32 Großunternehmen in Deutschland und N=31 in Österreich bezieht, diese am häufigsten von dem Delikt Diebstahl/Unterschlagung betroffen, gefolgt von Betrug und Untreue, während allerdings in der Schweiz (N=30) Datendiebstahl/Datenmissbrauch an erster Stelle stand.

Diebstahl führt die Liste der häufigsten Delikte auch in weniger großen Unternehmen an, wie die Ergebnisse der „WIK/ASW-Sicherheits-Enquête 2012/2013“ nahelegen, welche ebenfalls eine hohe Belastung (84,8 %) ausweisen.

In der vorliegenden Studie fällt die im Bereich des Betrugs und auch der Untreue außergewöhnlich niedrige Betroffenheit der teilnehmenden österreichischen Unternehmen (im Vergleich zu den deutschen und schweizerischen Unternehmen) auf. Dieser Befund mag mit spezifischen österreichischen Bedingungen zusammenhängen, kann allerdings zum

Teil auf den Aufbau der Sicherheit zurückgeführt werden und damit einhergehend auf die Größe und die internationalen Geschäftsaktivitäten der österreichischen Unternehmen. In den befragten Unternehmen lag der Anteil derer mit einer Konzernsicherheitsabteilung bei 46 % (DE 87,5 %, CH 66,7 %).

Sehr deutlich zeigte die Untersuchung den Einfluss der Unternehmensorganisation auf das Erkennen von Kriminalitätsbelastungen. Unternehmen mit einer Abteilung für Konzernsicherheit weisen im Hellfeld deutlich höhere Prävalenzraten auf als Unternehmen ohne eine solche Abteilung. Dies kann damit zusammenhängen, dass es sich um die - im Spektrum dieser Studie – besonders großen Unternehmen handelt, die allein deshalb hohe Prävalenzraten bei der Betroffenheit von Kriminalität erreichen. Größe könnte aber auch den Überblick erschweren und dazu führen, dass weniger Delikte erkannt werden. Dies kann für die vorliegende Studie aber deshalb ausgeschlossen werden, weil über 72 % der hier befragten Unternehmen, ihre Kriminalitätsbelastung systematisch erfassen und auswerten. Dieser Befund hat eine hohe Bedeutung für die Interpretation einschlägiger Untersuchungen und die Anlage künftiger Studien. Untersuchungen, die die Kriminalitätsbelastung von Unternehmen erheben, sollten überprüfen, ob eine systematische Erfassung der Kriminalitätsbelastung vorliegt, denn die Befunde von Unternehmen mit und ohne systematische Kriminalitätserfassung lassen sich nicht ohne weiteres vergleichen. Für künftige Untersuchungen zeigt dieser Befund die Möglichkeit auf, sich von dem groben Instrument der Prävalenz zu lösen und nicht nur danach zu fragen, ob ein Unternehmen in einem bestimmten Zeitraum überhaupt Opfer bestimmter Straftaten geworden ist, sondern auch deren Häufigkeit/Inzidenz zu erheben. Damit erschließen sich weitere Möglichkeiten, z.B. kann die Wirksamkeit und Bedeutung von Präventionsmaßnahmen näher beleuchtet werden und es verwundert nicht, dass über 90 % der Befragten von einem Bedeutungszuwachs der Prävention ausgehen.

Unterschiedliche Zuständigkeiten – mögliche Gründe

Erhebliche Unterschiede im Aufgabenspektrum zeigten sich zwischen Deutschland einerseits und Österreich und der Schweiz andererseits. Dies kann auf ein unterschiedliches Verständnis von Sicherheit auf Konzernebene hindeuten, aber möglicherweise auch damit zusammenhängen, dass die Größe der jeweils zu den „TOP100“ zählenden Unternehmen sehr unterschiedlich ist. Hinsichtlich der fachlichen Zuständigkeit der Sicherheitsabteilungen zeigt die Studie einerseits einen Kernbestand an Verantwortungsbereichen, der oben auf der Grundlage einer sogenannten Clusteranalyse in Cluster 1 zusammengefasst ist. Andererseits ergaben sich auch hier interessante Unterschiede zwischen den beteiligten Ländern. Auffallend waren die hohen Anteile von österreichischen Befragten, die Know-how-Schutz als

für ihr Unternehmen nicht oder wenig relevant einstuften und die Risikoanalysen und Risikomanagement sowie den Schutz vor Vermögens- und Wirtschaftsdelikten nicht zu ihrem Zuständigkeitsbereich zählten. Sicherheitsabteilungen bzw. -verantwortliche in Österreich und der Schweiz sind in deutlich höherem Maß als in Deutschland für Datenschutz, workplace violence, Arbeitssicherheit und Brandschutz zuständig. Dies führte in der Analyse zur Ausprägung der Cluster 2 und 3.

Diese Unterschiede können einen besonderen historischen, gesellschaftlichen oder auch juristischen Hintergrund haben; sie beruhen möglicherweise auf der organisatorischen Strukturierung; sie könnten aber auch mit einer unterschiedlichen Zusammensetzung der befragten TOP100-Unternehmen hinsichtlich Branche und Größe zusammenhängen. Auf eine Erhebung der zuletzt genannten Aspekte wurde in dieser Studie zur Wahrung der Anonymität der Befragten verzichtet. Da sich bei dieser und anderen Analysen wiederholt die Bedeutung dieser Aspekte für die Interpretation der Befunde gezeigt hat, wird man über diese Entscheidung bei nachfolgenden Erhebungen neu diskutieren müssen. Unabhängig davon geben die Befunde Anlass, sich in der Praxis über die Erfahrungen mit den unterschiedlichen Zuständigkeiten der Sicherheitsabteilungen bzw. -verantwortlichen auszutauschen und die Zuständigkeiten auf dieser Grundlage eventuell neu zu justieren.

Ein weiteres interessantes Faktum ist das Thema Hinweisgebersysteme, das sich in Deutschland und der Schweiz bereits etabliert hat, während in Österreich noch die Hälfte der Unternehmen über kein entsprechendes System verfügt oder die Einführung andenkt.

Zukunftsthema: Arbeitszufriedenheit und Wertschätzung

Abschließend soll noch ein Befund hervorgehoben werden: die Bedeutung von Zufriedenheit und ihr Zusammenhang mit der Wertschätzung.

Grundsätzlich kann eine relativ hoch ausgeprägte Zufriedenheit der Befragten konstatiert werden, insbesondere im Hinblick auf die eigene Position sowie im Hinblick auf die wahrgenommene Unterstützung durch den Vorstand. Gleichwohl fühlen sich 46,3 % der Sicherheitsverantwortlichen (eher) nicht als Bestandteil des Unternehmenserfolgs angesehen.

Die eigene Einschätzung, ob jemand sich als „Business Enabler“ angesehen fühlt, korreliert signifikant mit fast allen erhobenen Zufriedenheitswerten: mit der fachlichen Anbindung an den Vorstand (Spearman-rho=.582; p<.001) und seiner Unterstützung (rho=.424; p<.01), mit dem zur Verfügung stehenden Budget (rho=.459; p<.01) und nicht zuletzt der Position im Unternehmen (rho=.408; p<.01).

Sicherheit wird in einigen Unternehmen möglicherweise eher als Cost Center und als „Business Disabler“ verstanden anstatt als „Business Enabler“. Die vorliegenden Ergebnisse legen nahe, dass eine Veränderung dieser Perspektive einen positiven Effekt auf die (Arbeits-)Zufriedenheit der Sicherheitsverantwortlichen und ihrer Mitarbeitenden haben könnte, was sich aus arbeitspsychologischer Sicht ebenfalls auf Leistungsbereitschaft und -fähigkeit – von der wiederum das Unternehmen profitiert – auswirken dürfte.

5. Ausblick

Die Weiterentwicklung der Rolle von CSOs: Vielfältige Herausforderungen

Die vorliegende Untersuchung in Bezug auf Verantwortliche für Konzernsicherheit umfasste einen gemeinsamen Sprachraum, der gleichzeitig ein sehr weit entwickelter und verzahnter Wirtschaftsraum ist. Wegen der besonderen Eigenschaften der TOP100-Unternehmen – Komplexität der Organisation, globale Vernetzung, Vorreiterrolle bzw. Vorbildwirkung und volkswirtschaftliche Bedeutung – wird es besonders interessant sein, sich in Zukunft noch intensiver mit der Lage der Konzernsicherheit in diesen Unternehmen zu beschäftigen. Die Auswertungen der weiteren Daten aus der vorliegenden Untersuchung werden noch interessante Aspekte beleuchten.

Als Ausblick sollen einzelne übergeordnete Themen und Herausforderungen skizziert werden.

Business Continuity: Krisen nahe Europa als neue Normalität?

Versicherungsfachleute in großen Unternehmen haben im „Allianz Business Barometer on Business Risks 2014“ das Thema „Business Interruption“ wiederholt als bedeutendstes Risiko für Unternehmen identifiziert. CSOs leisten mit ihren Teams Tag für Tag einen wichtigen Beitrag dazu, dass Wertschöpfungsketten intakt bleiben. Kaum ein Jahr zeigt deutlicher als 2014, wie rasch sich die sicherheitspolitische Situation ändern kann: Die Europäische Union ist in ihren südlichen, südöstlichen und östlichen Nachbarregionen mit Konflikten konfrontiert, die neben dem menschlichen Leid auch wirtschaftliche Auswirkungen haben. Weiterhin instabile Länder mit ungeklärter politischer Situation in Nordafrika, Flüchtlingsströme, ein Bürgerkrieg in Syrien und – damit einhergehend – der IS-Terror auch im Nordirak sowie die Kampfhandlungen in der Ukraine beeinträchtigen auch Wirtschaftsbeziehungen. Täglich kann sich für CSOs das Lagebild ändern, und die Akteure auf den Finanzmärkten beobachten das Agieren betroffener globaler Unternehmen besonders genau. Aufgrund der großen Bedeutung der Ukraine für den Transport von Energie sind das Ausmaß der internationalen Vernetzung und die Abhängigkeit von Lieferanten noch stärker ins allgemeine Bewusstsein gerückt.

Die Zukunft: Vernetzte globale Risiken im Fokus

Diese Netze wiederum sind gerade seit 2013 im Zentrum des öffentlichen Diskurses und auch in anderer Hinsicht von größter Relevanz für die Sicherheit von Unternehmen: Mit Edward Snowdens Enthüllungen zur Tätigkeit von Geheimdiensten ist Cyber-Sicherheit ins Bewusstsein der Gesellschaft gerückt. Diese Enthüllungen ziehen indirekt auch Diskussionen über rechtliche Regelungen nach sich. Das bestätigt der aktuelle „Global Risk Report“ des World Economic Forum, den dieses gemeinsam mit Universitäten und maßgeblichen Vertretern der Versicherungswirtschaft erstellt: Neben dem Ranking der aktuell als am stärksten wahrgenommenen Risiken, das von „Finanzkrisen in wichtigen Volkswirtschaften“ vor „hoher struktureller Arbeitslosigkeit“ und „Wasserkrisen“ (Versorgung mit Wasser und extreme Wetterereignisse) angeführt wurde, wurden drei zusammenhängende Risikokonstellationen näher beschrieben. Diese werden für die Arbeit von Verantwortlichen für Konzernsicherheit in global tätigen Unternehmen besondere Bedeutung bekommen:

- Mehr Instabilitäten in einer zunehmend multipolaren Welt (demographischer Wandel in unterschiedlicher Form, eine wachsende Mittelklasse in Schwellenländern, knappe staatliche Budgets sowie eine Entwicklung hin zu eingeschränkter wirtschaftlicher Vernetzung)

- Eine „verlorene Generation“ von jungen Arbeitslosen oder prekär Beschäftigten, die das Bildungssystem, die Arbeitsmärkte und die Gesellschaft selbst herausfordert.

- Die Desintegration der digitalen Wirtschaft/Gesellschaft, wenn durch fortgesetzte Angriffe aufgrund der Verwundbarkeit der Netzwerke das Vertrauen in das Internet als Basis für Kommunikation und wirtschaftliche Tätigkeit erodiert wird.

Mehr Fokus auf Wirtschaftskriminalität, Compliance und IT-Security

Im Bereich Compliance laufende rechtliche Entwicklungen und die Vernetzung mit möglichen Wirtschaftsdelikten sind ein Ansatzpunkt für eine stete wissenschaftliche Begleitung. Vergleichbare Befragungen wie jene von KPMG (2012, 2014) und PWC (2014) konzentrieren sich vor allem auf Mitglieder des Top-Managements als Adressaten und inhaltlich auf unterschiedliche Aspekte von Wirtschaftskriminalität und Compliance. Dabei zeigt sich über die Jahre ein stetiger Anstieg des Ausmaßes und der Bedeutung von „Cyber Crime“ in seinen verschiedenen Ausprägungen.

Ein wichtiges Indiz dafür, dass das Thema an Bedeutung gewinnt, ist die Beachtung durch die Versicherungswirtschaft, wie wieder das „Allianz Business Barometer“ zeigt: In allen drei untersuchten Regionen („Americas“, „Europe, Middle East and Africa - EMEA“ und „Asia Pacific“) ist „cyber cri-

mes, IT failures, espionage“ in das Ranking der Top-10-Risiken aufgestiegen – wohl eine Folge der Diskussionen um die Enthüllungen von Edward Snowden. „Theft, fraud & corruption“ befinden sich in den „Americas“ und EMEA ebenfalls unter den Top 10. Die unterschiedliche Wahrnehmung von Risiken ist einerseits eine Folge der unterschiedlichen Betroffenheit aufgrund von wirtschaftlichen Strukturen und Entwicklungen. Andererseits lässt sich daraus auch die Frage nach der Ausprägung unterschiedlicher Sicherheitskulturen ableiten.

Gegenstand künftiger Untersuchungen könnten etwa mögliche Unterschiede in den Zugängen und Haltungen von CSOs sein – wie stark setzt man etwa auf technische, organisatorische oder bauliche Lösungen? Welche Methoden und Werkzeuge werden wie kombiniert? Gibt es eine spezifische europäische Sicherheitskultur in Unternehmen; wie grenzt sie sich etwa von einer angloamerikanischen ab?

Darüber hinaus ergibt sich aus dem hier erhobenen Befund, dass bereits ein großer Teil der TOP100-Unternehmen die Betroffenheit der Unternehmen von Kriminalität systematisch und differenziert auch in ihrem quantitativen Ausmaß erhebt, dass sich künftige Studien nicht auf die derzeit verbreitete Erhebung bloßer Prävalenzen beschränken müssen. Vielmehr kann zumindest für die TOP100-Unternehmen anhand von Häufigkeiten/Inzidenzen ein erheblich differenzierteres Bild der aktuellen Lage abgebildet werden, und damit können auch die Grundlagen für künftige Trendanalysen und „Impact-Analysen“ von Präventionsmaßnahmen geschaffen werden.

Aufschwung für Sicherheitsfachkräfte, neue Schnittstellen

Insgesamt ist zu erwarten, dass sich die Rolle und der Aufgabenbereich von CSOs noch stärker um die analytische und strategische Komponente erweitern werden. Wurden früher zahlreiche Risiken noch weniger beachtet, so findet nach unserer Einschätzung eine Professionalisierung in Unternehmen aller Größenklassen statt. Ein systematisches Unterschätzen bzw. Ignorieren und mangelhafte Prävention kann sich mittelfristig kein Unternehmen leisten. Es ergeben sich damit auch mehr Anknüpfungspunkte für die Kooperation mit Behörden.

Die Einstellungen von Verantwortlichen für Konzernsicherheit und ihre wichtigste Schnittstelle im Unternehmen – die Anbindung an das Top-Management – wurden vor den vorliegenden Studienergebnissen in dieser Form noch nicht untersucht. Eine Fortsetzung bzw. Wiederholung dieser Untersuchung könnte Veränderungen im Zeitverlauf sichtbar machen und frühzeitige Reaktionen ermöglichen. Über Fragen nach Erwartungen an künftige Mitarbeiterinnen und Mitarbeiter lässt sich auch wertvolles Feedback für die Aus- und Weiterbildung generieren.

Literaturverzeichnis

ALLIANZ (2014). Allianz Risk Barometer on Business Risks 2014. URL: www.agcs.allianz.com

Buerschaper, C. (2008). Organisationen – Kommunikationssystem und Sicherheit. In P. Badke-Schaub, G. Hofinger & K. Lauche (Hrsg.), Human Factors – Psychologie sicheren Handelns in Risikobranchen (Kap. 9). Heidelberg: Springer Medizin Verlag.

Erwin P. M. (2011). Corporate Codes of Conduct: the effects of code content and quality on ethical performances. Journal of Business Ethics, 99(4), 535 – 548.

Fahlbruch, B., Schöbel, M. & Domeinski, J. (2008). Sicherheit. In P. Badke-Schaub, G. Hofinger & K. Lauche (Hrsg.), Human Factors – Psychologie sicheren Handelns in Risikobranchen (Kap. 2). Heidelberg: Springer Medizin Verlag.

Hofmann, S. (2008). Anti-Fraud-Management: Bilanzbetrug erkennen - vorbeugen – bekämpfen. Berlin: Erich Schmidt.

Hudson, P. (2007). Implementing a safety culture in a major multi-national. Safety Science, 45(6), 697-722.

Jöns, I., Hodapp, M. & Weiss, K. (2006). Kurzskala zur Erfassung der Unternehmenskultur. Mannheimer Beiträge 01/06. Mannheim: Universität Mannheim.

Kaptein M. & Schwartz, M. (2008) The effectiveness of business codes: A critical examination of existing studies and the development of an integrated research model, Journal of Business Ethics, 77, 111-127.

KPMG (2012). Wirtschaftskriminalität. Deutschland – Eine empirische Studie zur Wirtschaftskriminalität im Mittelstand und in den 100 größten Unternehmen. URL: www.kpmg.com.

KPMG (2013). Wirtschaftskriminalität. Deutschland, Österreich, Schweiz im Vergleich – Wirtschaftskriminalität in Grossunternehmen und dem Mittelstand. URL: www.kpmg.com.

PWC (2014). Economic Crime: A Threat to Business Globally. URL: www.pwc.com/crimesurvey.

Wecker, G. & Van Laak, H. (2009) (Hrsg). Compliance in der Unternehmenspraxis – Grundlagen, Organisation und Umsetzung. Wiesbaden: Gabler.

Weick, K.E. & Sutcliffe, K.M. (2003). Das Unerwartete managen. Wie Unternehmen aus Extremsituationen lernen. Stuttgart: Klett-Cotta.

WIK/ASW-Sicherheits-Enquête 2012/2013 (2013). Ergebnisse der WIK/ASW-Sicherheits-Enquête 2012/2013. Gau-Algesheim: SecuMedia.

World Economic Forum (2014). Global Risks 2014, Ninth Edition. Genf: World Economic Forum. URL: www3.weforum.org.

Die Partner

FH Campus Wien

Mit mehr als 4.600 Studierenden (Stand: November 2014) ist die FH Campus Wien die größte akkreditierte Fachhochschule Österreichs. In den Departments Applied Life Sciences, Bauen und Gestalten, Gesundheit, Public Sector, Soziales und Technik steht den Studierenden ein Angebot von mehr als 50 Bachelor- und Masterstudiengängen sowie Masterlehrgängen zur Verfügung. Die FH Campus Wien ist mit Unternehmen, Verbänden, Schulen und öffentlichen Einrichtungen vernetzt. Zahlreiche F&E-Projekte der Studiengänge und externe Auftragsforschungsarbeiten werden über eigene Forschungsgesellschaften abgewickelt.
Der Fachbereich „Risiko- und Sicherheitsmanagement“ ist im Department Public Sector angesiedelt. Die beiden Studiengänge – das Bachelorstudium „Integriertes Sicherheitsmanagement“ und das Masterstudium „Risk Management and Corporate Security“ – sind berufsbegleitend organisiert und in Österreich einzigartig.

www.fh-campuswien.ac.at

Hochschule für Öffentliche Verwaltung Bremen

Die Hochschule für Öffentliche Verwaltung Bremen wurde 1979 als interne Fachhochschule für den Öffentlichen Dienst gegründet. Sie hat sich in den vergangenen Jahren für weitere Studiengänge geöffnet mit dem Fokus auf Recht, Sicherheit und Polizei. Das Studienangebot umfasst aktuell die drei Bachelorstudiengänge „Polizeivollzugsdienst”, „Risiko- und Sicherheitsmanagement” und „Steuer und Recht”.

Die Hochschule für Öffentliche Verwaltung unterhält mit dem Institut für Polizei- und Sicherheitsforschung (IPoS) sowie dem Fortbildungsinstitut für die Polizeien im Lande Bremen zwei eigenständige Institute. Das Fortbildungsinstitut für die Polizei gewährleistet die gesamte berufliche Fortbildung für die Bremer Polizei und beteiligt sich in Kooperation mit der Deutschen Hochschule der Polizei und weiteren Länderpolizeien an der Führungskräfteausbildung.

Das Institut für Polizei- und Sicherheitsforschung (IPoS) besteht seit 2002 an der Hochschule. Die Forschungsteams verbinden die Disziplinen Rechtswissenschaften, Psychologie, Soziologie, Kriminologie und Kriminalistik. Das IPoS beschäftigt sich mit polizeilichen und anderen sicherheitsrelevanten Forschungsfeldern, verfolgt einen interdisziplinären und praxisorientierten Ansatz und führt neben EU-Projekten insbesondere drittmittelfinanzierte Studien und F&E-Projekte auf nationaler und lokaler Ebene durch.

www.hfoev.bremen.de – www.ipos.bremen.de

Autorenbiographien

Prof. Dr. jur. habil. Arthur Hartmann leitet seit 2009 das Institut für Polizei- und Sicherheitsforschung (IPOS) der Hochschule für Öffentliche Verwaltung Bremen.
Nach dem Studium der Rechtswissenschaften und der Soziologie an der Ludwig-Maximilians-Universität München war er als Universitätsassistent tätig und forschte im Rahmen des Modellversuchs Täter-Opfer-Ausgleich im Jugendstrafrecht. Ab 1992 arbeitete er als wissenschaftlicher Assistent am Institut für Kriminologie der Universität Heidelberg, wo er 2001 für die Fächer Kriminologie, Strafrecht und Strafverfahrensrecht mit einer Arbeit über die organisierte Kriminalität habilitierte. Nach einer Vertretungsprofessur an der Humboldt-Universität Berlin und der Tätigkeit als stellvertretender Leiter des Instituts für Kriminologie der Universität Tübingen wurde er 2002 an die HfÖV Bremen berufen.

Kontakt:
Tel.: +49 421 36159-519
E-Mail: arthur.hartmann@hfoev.bremen.de

Prof. Dr. phil. Claudia Kestermann ist Professorin für Rechts- und Kriminalpsychologie an der Hochschule für Öffentliche Verwaltung Bremen sowie stellvertretende Leiterin des Instituts für Polizei- und Sicherheitsforschung (IPOS). Ihre Schwerpunkte in Forschung und Entwicklung liegen im Bereich der Kriminalitätsforschung und der angewandten Sicherheitsforschung.
Nach dem Studium von Psychologie, Kriminologie und Strafrecht an den Universitäten Bochum und Bonn promovierte die Diplom-Psychologin im Jahr 2001 an der Universität Bremen. Der mehrjährigen Tätigkeit als wissenschaftliche Mitarbeiterin an den Universitäten von Bremen und Greifswald folgte der Wechsel an die HfÖV Bremen. Dort war sie an der Entwicklung und Implementierung des Bachelorstudiengangs „Risiko- und Sicherheitsmanagement“ maßgeblich beteiligt, dessen Leiterin sie heute ist.

Kontakt:
Tel.: +49 421 36159-446
E-Mail: claudia.kestermann@hfoev.bremen.de

FH-Prof. DI Martin Langer ist Leiter des Fachbereichs Risiko- und Sicherheitsmanagement der FH Campus Wien und leitet dort den Bachelorstudiengang „Integriertes Sicherheitsmanagement“ sowie den Masterstudiengang „Risk Management and Corporate Security“.
Davor war Langer als Berater für Sicherheits- und Krisenmanagement bei zahlreichen börsennotierten Unternehmen in Österreich und Deutschland tätig. Zusätzlich war er leitend im Rahmen internationaler Einsätze für das Rote Kreuz, das österreichische Bundesheer und die UNO nach Naturkatastrophen in der Türkei, Mosambik, Honduras und dem Iran tätig. Langer ist Absolvent des Strategischen Führungslehrganges der österreichischen Bundesregierung und beschäftigt sich aktuell mit dem Thema Wirtschaftsschutz.

Kontakt:
Tel.: +43 1 606 68 77-2151
E-Mail: martin.langer@fh-campuswien.ac.at

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

www.fh-campuswien.ac.at
www.hfoev.bremen.de

HfÖV
Hochschule für
Öffentliche Verwaltung Bremen