Claudia Kestermann, Claudia Körmer,
Martin Langer, Arthur Hartmann

Konzernsicherheit in den **TOP100-Unternehmen**

Deutschland - Österreich - Schweiz

Fokus: Sicherheit im Ausland

Update 2017

Impressum

Diese Publikation wurde gemeinsam von der Hochschule für Öffentliche Verwaltung Bremen und der FH Campus Wien erstellt und herausgegeben.
AutorInnen und für den Inhalt verantwortlich: Prof. Dr. Claudia Kestermann (Hochschule für Öffentliche Verwaltung Bremen), FH-Prof. Mag. Claudia Körmer (FH Campus Wien), FH-Prof. DI Martin Langer (FH Campus Wien), Prof. Dr. Arthur Hartmann (Hochschule für Öffentliche Verwaltung Bremen)
Redaktion und Produktionsleitung: DI (FH) Mag. Thomas Goiser MA; Lektorat: Mag.a Verena Brinda www.verenabrinda.at; Grafik: Doris Grussmann (www.dggd.at): Druck: Druckerei Ferdinand Berger & Söhne GmbH

Wien/Bremen, Oktober 2017

Inhalt


LONDON
ANCHORAGE
TOKYO
GLOBAL IONETIK

Vorwort

FH Campus Wien

FH-Prof.in Dr.in Barbara Bittner
Rektorin der FH Campus Wien

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

Vorreiter in Unternehmens- bzw. Konzernsicherheit

Im Zentrum Europas sind wir seit einigen Jahrzehnten in der glücklichen Lage, dass in unseren Gemeinwesen die Demokratie und der Rechtsstaat grundsätzlich funktionieren und sozialer und politischer Friede herrscht. Sicherheit ist aber keine Selbstverständlichkeit. Das zeigt sich nicht nur vor den Toren Europas, sondern auch in unseren Gesellschaften, bei unserer kritischen Infrastruktur und – nicht zuletzt – im Cyberspace. Unsere hohen Sicherheitsstandards und ein hohes subjektives Sicherheitsgefühl sind die Folge der täglichen engagierten Arbeit von Behörden, couragierten Einzelpersonen, Zivilgesellschaft und Wirtschaft.

Große Unternehmen sind Leitsterne der wirtschaftlichen Entwicklung. Prozesse, Verfahren, die sich bei ihnen durchsetzen, sind beispielgebend für zahlreiche kleine Unternehmen. Als Vorreiter der Internationalisierung des Wirtschaftslebens sind sie auch in zahlreichen Ländern tätig, deren Sicherheitslage nicht unserer entspricht. Wie sie es schaffen, auch in diesen Umfeldern erfolgreich zu sein, welche Methoden und Verfahren sie anwenden, auf wessen Unterstützung sie zurückgreifen, ist entscheidend für ihre Wettbewerbsfähigkeit.

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 daher ein besonders wichtiges Forschungsthema.
Die Chief Security Officers in diesen Unternehmen sind besonders hoch qualifiziert und gut vernetzt. Vom Erfolg ihrer Arbeit hängt viel ab — in den Unternehmen selbst und in der Wirtschaft generell.

Die Ergebnisse der Umfrage unter den Unternehmen zeigen im großen Überblick: Das Bewusstsein für das Thema steigt, die Bedeutung nimmt zu, die Umsetzung nimmt an Professionalität zu. Das ist eine gute Nachricht. Gleichzeitig gibt es noch viel zu tun, dafür braucht es Experten und Expertinnen, die auch an unseren Hochschulen ausgebildet werden.

Nach der positiven Resonanz auf die Studienergebnisse von CSO TOP 100 aus dem Jahr 2014 liegt nun das Ergebnis der Nachfolgeuntersuchung vor, das hoffentlich ebenso viel Beachtung finden wird. Wenn diese Erkenntnisse die weitere Forschung anregen, den Dialog zwischen Wissenschaft und Wirtschaft stärken und/oder in den Unternehmen Impulse geben, sich bestimmten Sicherheitsfragen zu stellen, dann freut uns das sehr.

Barbara Bittner, Luise Greuel

Danksagung

Mit Profis arbeiten

Unsere beiden Hochschulen verbinden Wissenschaft, Sicherheit und Wirtschaft. Risiko- und Sicherheitsmanagement ist heute ein interdisziplinär vernetztes und globales Thema. Darauf sind die Curricula unserer Studiengänge ausgerichtet, unsere Kooperationen in Lehre und Forschung sowie nicht zuletzt unsere Forschungsthemen? Unsere Kooperation hat Tradition: Gemeinsam haben wir im Jahr 2009 das „Cooperation Network for Risk, Safety and Security Studies“ (CONRIS) mitbegründet.

Die gute Zusammenarbeit bei CSO TOP 100 im Jahr 2014 hat uns zur Fortsetzung und zum Ausbau unserer Studie motiviert. Die ersten Ergebnisse liegen mit dieser Veröffentlichung vor.
Wieder haben wir auf starke Partner zählen können, die zum Erfolg der Untersuchung einen wichtigen Beitrag geleistet haben, namentlich

- Holger Münch, Präsident des Bundeskriminalamtes der Bundesrepublik Deutschland, und
- General Franz Lang, Direktor des Bundeskriminalamtes im Bundesministerium für Inneres der Republik Österreich.

Für ihr Vertrauen und die Unterstützung möchten wir uns auf diesem Weg herzlich bedanken.

Ohne das Vertrauen, die Bereitschaft zur Mitwirkung und die Offenheit der „Chief Security Officers“ der jeweils größten Unternehmen aus Deutschland, Österreich und der Schweiz wäre ein solches Projekt nicht möglich gewesen. Daher sagen wir Ihnen ein herzliches Dankeschön und hoffen, dass die Studienergebnisse Sie in ihrer Arbeit unterstützen können.

Weiterhin wollen wir allen Beteiligten und allen am Thema Interessierten aktuelle Erkenntnisse sowie Denk- und Diskussionsansätze für ihr Tätigkeitsfeld bieten.
Wir hoffen, dass dies mit dieser Publikation wieder gelingt, und freuen uns auf den Dialog mit Ihnen!

Claudia Kestermann, Claudia Körmer, Martin Langer, Arthur Hartmann

1. Vorstellung der Studie

Im Winter 2013/2014 führten die Hochschule für Öffentliche Verwaltung in Bremen und die Fachhochschule Campus Wien erstmalig eine Befragung von besonders bedeutenden Wirtschaftsunternehmen in Deutschland, Österreich und der Schweiz (D-A-CH-Region) im Hinblick auf sicherheitsrelevante Aspekte durch. Mit der Studie „Unternehmenssicherheit CSO TOP 100“ wollten die beiden Partner länderübergreifend in Deutschland, Österreich und der Schweiz Informationen zu Aufbau und Struktur von Sicherheit ebenso wie zur Sicherheitskultur und Kriminalitätsbelastung in führenden Wirtschaftsunternehmen gewinnen.

Dem vorliegenden Bericht liegt eine erneute Befragung von LeiterInnen des Bereichs Konzernsicherheit und Sicherheitsverantwortlichen in der D-A-CH-Region im Winter 2016/2017 zugrunde. In dieser Untersuchung haben wir die Sicherheit im Ausland zum Schwerpunktthema gemacht.

Die Erkenntnisse zur Organisation von Sicherheit in Unternehmen und die vertiefende Analyse verschiedener interagierender Faktoren werden im Folgenden zunächst dargestellt und punktuell mit den Erkenntnissen aus 2014 in Verbindung gesetzt. Danach liegt das Hauptaugenmerk auf der Organisation und den Maßnahmen zur Sicherheit im Ausland, insbesondere in „high risk regions“.
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:

- Sicherheitsorganisation und Aufgabenfelder,
- Sicherheitskultur und Kriminalitätsbelastung sowie
- Sicherheit im Ausland.

Sicherheitsorganisation und Aufgabenfelder

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 bzw. die Geschäftsführung, inhaltliche Zuständigkeiten, mögliche Weisungsbefugnisse und strategische Einflussmöglichkeiten. Darüber hinaus wurden die Zuständigkeiten und Aufgabenbereiche erhoben.

Sicherheitskultur und Kriminalitätsbelastung

Unter dieses Themenfeld lassen sich verschiedene sicherheitsrelevante Haltungen, Verhaltensweisen und Maßnahmen subsumieren.[1] Zunächst wurde die Implementierung von Policys und Maßnahmen zur Security Awareness in den Unternehmen thematisiert, bevor Aspekte der jeweiligen Fehler- und Sicherheitskultur[2] adressiert wurden. Im Anschluss ging es um die Erfahrungen der befragten Unternehmen als Betroffene unterschiedlicher Delikte. Neben der Prävalenz (Betroffenheit innerhalb der vergangenen 24 Monate) wurde auch das Schadensausmaß erhoben. Außerdem war von Interesse, inwieweit die Unternehmen bekannt gewordene Vorfälle systematisch erfassen, worauf sich ggf. eine solche Erfassung erstreckt und in welcher Form und Häufigkeit die Meldung und Auswertung der gewonnenen Erkenntnisse erfolgen.

Sicherheit im Ausland

Zunächst wurden die Aktivitäten der Unternehmen im Ausland sowie die Organisation und der Stellenwert des Themas im Unternehmen erhoben. Es folgten Fragen zu Indikatoren zur Gefährdungseinschätzung und – im Eskalationsfall – zur Evakuierung von Unternehmensangehörigen aus dem Ausland. Im Mittelpunkt standen anschließend Maßnahmen der jeweiligen Unternehmen für Auslandsreisende oder Expatriates in „high risk regions". Den Abschluss der Erhebung bildeten die Einschätzungen zukünftiger Herausforderungen und der persönlichen Zufriedenheit mit den Arbeitsbedingungen.

2.2 Durchführung der Befragung und Anmerkungen zur Stichprobe

In den beteiligten Ländern – Deutschland, Österreich und der Schweiz – wurden in Abhängigkeit von der Bevölkerungszahl die jeweils umsatzstärksten Unternehmen ausgewählt. Zudem wurden die umsatzstärksten Versicherungsunternehmen und Banken separat adressiert. Grundlage für die Einbeziehung der Unternehmen waren deren veröffentlichte Umsatzzahlen. In Deutschland wurden insgesamt N=390 Fragebögen postalisch versandt, in Österreich N=155 und in der Schweiz ebenfalls N=155.

Insgesamt wurden n=60 Fragebögen zurückgesandt, was einer Rücklaufquote von rund 8,6 % entspricht. Eine solch geringe Quote mag sowohl der Besonderheit der Stichprobe vor dem Hintergrund der sicherheitsrelevanten Thematik der Befragung geschuldet sein als auch dem gewählten Schwerpunktthema „Sicherheit von Unter-

1 Aus methodischer Sicht ergeben sich im Hinblick auf einzelne Aspekte der 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 Sicherheitskultur wäre die Befragung einer größeren Stichprobe von Beschäftigten und Führungskräften in den einzelnen Unternehmen erforderlich.

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

nehmensangehörigen in Ländern mit hohem oder extremem Risiko“. Da im Sinne von good practice primär beispielhafte Erkenntnisse generiert werden sollen, die für die Praxis sowie für weitere Forschung handlungsleitend sein können, erscheint die Beteiligung tolerabel.

Die n=60 Teilnehmenden verteilen sich auf die beteiligten Länder wie folgt: n=39 Teilnehmende aus deutschen, n=12 aus österreichischen und n=9 aus schweizerischen Unternehmen. Angesichts der geringen Größe der Stichprobe haben die Ergebnisse (insbesondere auf Länderebene) primär heuristischen Charakter.
Die teilnehmenden Unternehmen sind in unterschiedlichen Branchen aktiv, vorrangig in der Industrie (n=27) gefolgt vom Dienstleistungsbereich sowie Banken/Versicherungen (jeweils n=8) und dem Handel (n=5). N=12 Unternehmen sind in anderen Bereichen aktiv.

3. Sicherheitsorganisation und Aufgabenfelder

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.

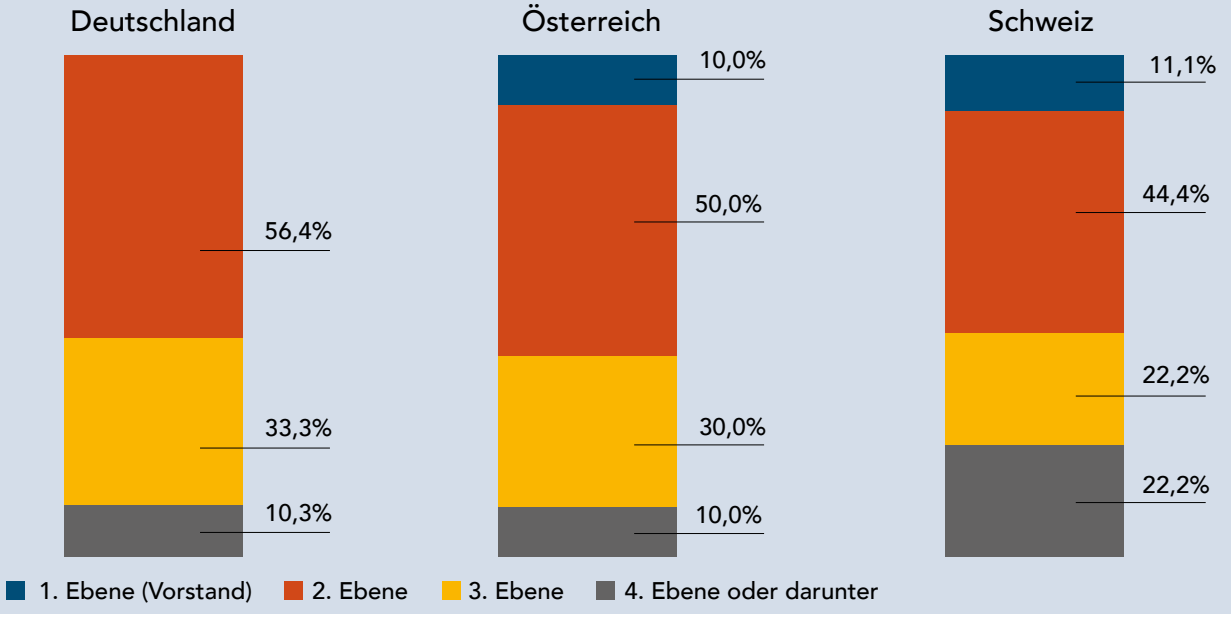
3.1 Organisation von Sicherheit und Zufriedenheit der Sicherheitsverantwortlichen

Drei von vier teilnehmenden Unternehmen (76,7 %) verfügen über eine Konzernsicherheitsabteilung. Bei den beteiligten deutschen Unternehmen liegt der Anteil mit 84,6 % (2014: 87,5 %) deutlich vor jenen aus der Schweiz (66,7 %; 2014: 66,7 %) und jenen aus Österreich (58,3 %; 2014: 46,2 %). Im Vergleich zur Befragung im Jahr 2014 weist der Anteil der Unternehmen mit Konzernsicherheitsabteilung in Österreich einen Anstieg auf.

Dass das Thema „Sicherheit" als Aufgabe explizit dem Vorstand zugeordnet ist, bejahen 62,7 % der Teilnehmenden. Während dies in der Schweiz von weniger als der Hälfte der Antwortenden angegeben wird (44,4 %; 2014: 50 %), sind es in Deutschland bereits 64,1 % (2014: 48,3 %), und in Österreich liegt der Anteil bei annähernd drei Viertel (72,7%; 2014: 76,9 %). Nur in Deutschland ist eine Zunahme im Vergleich zu 2014 festzustellen; der Anteil liegt allerdings immer noch auf moderatem Niveau.

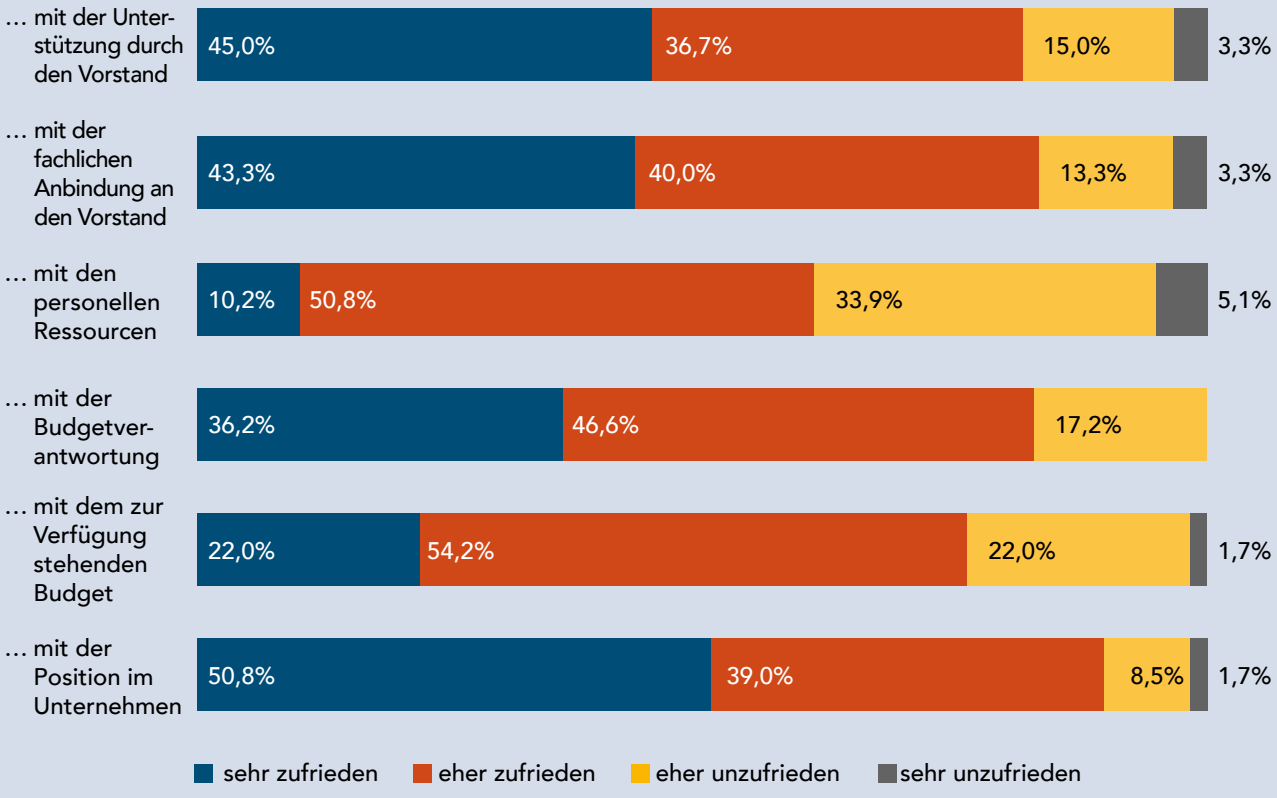
Wird die Position in der Hierarchie betrachtet, also die Ansiedlung der Stelle der Leiterin/des Leiters der Abteilung Konzernsicherheit bzw. der/des Sicherheitsverantwortlichen im Unternehmen, ergibt sich folgendes – relativ einheitliches – Bild: In Österreich sind 60 % der Stellen der Sicherheitsleitung organisatorisch in den ersten beiden Ebenen angesiedelt, in Deutschland 56,4 % und in der Schweiz 55,5 %. Die Hierarchie-Ebene, in der die Konzernsicherheitsabteilung angesiedelt ist, korreliert signifikant positiv mit der Ebene, auf der die eigene Stelle angesiedelt ist.[3]

Abbildung 1: Hierarchie-Ebene der Leitung der Abteilung Konzernsicherheit oder der/des Sicherheitsverantwortlichen



3 Spearman rho=.644, p<.001

Abbildung 2: Zufriedenheit der Befragten



Einige spezifische Fragen behandelten die Zufriedenheit der Sicherheitsverantwortlichen mit den Rahmenbedingungen im Unternehmen, ihrer Position und den zur Verfügung stehenden Ressourcen: Die Zufriedenheit mit der eigenen Position ist bei den Befragten sehr hoch ausgeprägt (89,8 %; 2014: 87,5 %: „trifft voll zu“ / „trifft eher zu“). Fast ebenso deutlich ist die positive Einschätzung der Unterstützung durch den Vorstand (81,7 %; 2014: 83,4 %) und der fachlichen Anbindung an den Vorstand (83,3 %; 2014: 73 %). Gerade der letzte Aspekt wird weitaus positiver bewertet als in der Befragung vor drei Jahren.

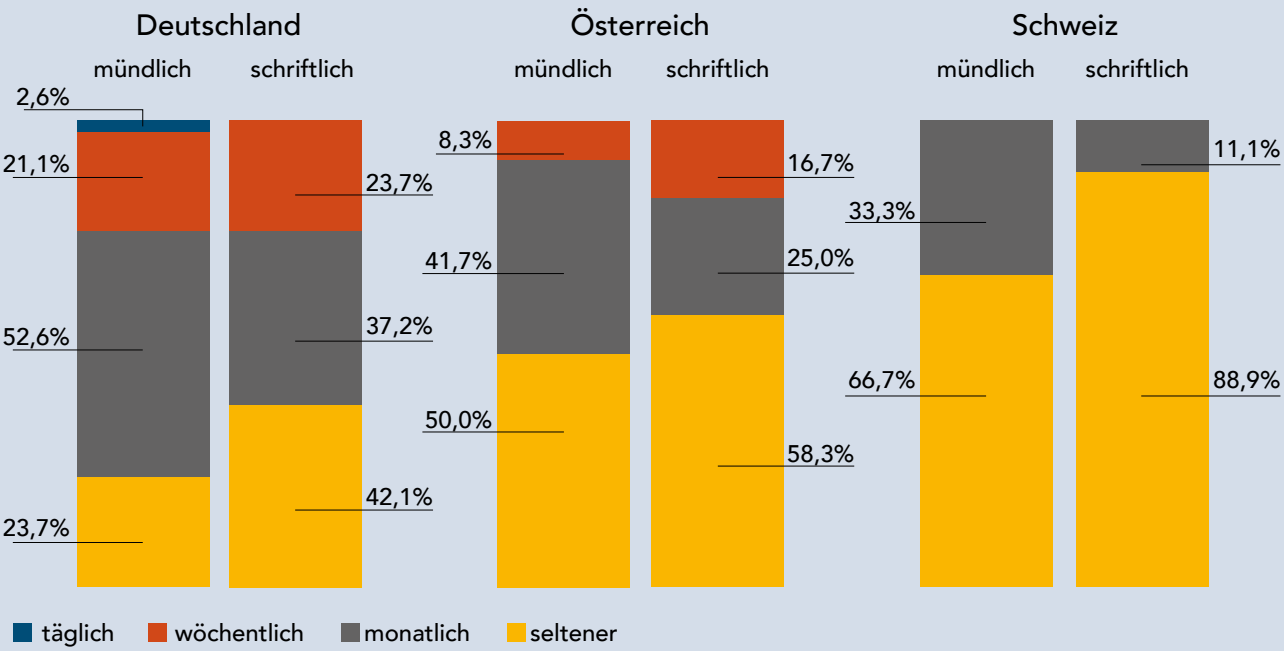
Mit der Verantwortung für das Budget ist ein sehr großer Teil der Befragten ebenfalls zufrieden. Auch im Hinblick auf die Höhe des zur Verfügung stehenden Budgets kann von einer relativen Zufriedenheit ausgegangen werden, wobei fast jede/r Vierte (23,7 %) angibt, „eher unzufrieden“ bzw. „sehr unzufrieden“ zu sein. Mit 39 % ist der Unmut über die personellen Ressourcen dagegen wesentlich höher ausgeprägt.

Mit einer durchschnittlichen Bewertung der Zufriedenheitsaspekte von 1,59 (Skala: 1=„sehr zufrieden“ bis 4=„sehr unzufrieden“) sind die schweizerischen Befragten deutlich zufriedener mit der aktuellen Situation als die deutschen (M=1,91) und österreichischen Teilnehmenden (M=1,92). Während im Hinblick auf Deutschland und Österreich keine Veränderungen zu 2014 festgestellt werden können, stellen sich die Zufriedenheitswerte aus der Schweiz deutlich positiver dar: Lag der Mittelwert im Jahr 2014 nur bei 2,5 und damit am Ende eines Zufriedenheitsrankings, so führen die schweizerischen Befragten dieses Ranking nun an.

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 erörtert werden. In Deutschland wird dem Vorstand weit häufiger als in den anderen Ländern regelmäßig mündlich und schriftlich berichtet (wöchentlich 23,7 %). In den österreichischen Unternehmen erfolgen wöchentliche Kontakte seltener, weitaus verbreiteter ist eine geringere Kontakt-

Abbildung 3: Häufigkeit, in der dem Vorstand berichtet wird



häufigkeit (weniger als monatlich). Für die Schweiz gilt dies in noch deutlicherem Ausmaß. Interessanterweise ist der Austausch mit dem Vorstand in den schweizerischen und österreichischen Unternehmen im Vergleich zu 2014 deutlich zurückgegangen, während für deutsche Unternehmen der Trend zu einer intensiveren Kommunikation geht.

Zudem geben 77,1 % der deutschen Antwortenden (2014: 80,6 %) und 75 % der österreichischen Antwortenden (2014: 69,2 %) an, bei Bedarf mit dem Vorstand in Kontakt treten zu können. Befragte aus der Schweiz haben nur zu 55,5 % (2014: 44,4 %) eine solche zusätzliche Kommunikationsmöglichkeit.

Die Häufigkeit der mündlichen Berichterstattung und damit des persönlichen Kontakts korreliert signifikant mit der Zufriedenheit mit der eigenen Position.[4] Ein ausgeprägter, häufiger Austausch insgesamt (schriftliche wie mündliche Berichte) korreliert zudem deutlich mit der Zufriedenheit der Sicherheitsverantwortlichen mit der fachlichen Anbindung und der Unterstützung durch den Vorstand.[5]

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, welche über ein eigenes Budget verfügen, ist mit 87,2 % (2014: 96,9 %) am höchsten, während dies in Österreich von 61,5 % (2014: 84,6 %) und in der Schweiz noch von 46,2 % (2014: 77,8 %) angegeben wird. Im Hinblick auf die Situation im Jahr 2014 wird deutlich, dass die Unternehmen zurückhaltender werden in Bezug auf die Übertragung von Budgets. Diejenigen, die über ein eigenes Budget verfügen können, zeigen im Hinblick auf die erhobenen Zufriedenheitsdimensionen in diesem Erhebungsjahr keine signifikant positiveren Werte als diejenigen, die keine Budgetverantwortung haben.

Eine Zunahme des zur Verfügung stehenden Budgets wird von jeweils 61 % der deutschen, 54,5 % der österreichischen und 50 % der schweizerischen Befragten bejaht und zeigt damit ein deutlich positiveres Bild als 2014. Im

4 Spearman rho=.262, p<.05
5 Spearman rho=.336 bis .466, p<.01

Abbildung 4: Finanzielle und personelle Ressourcen (2017)

Hinblick auf den Personalzuwachs ist zum Erhebungszeitpunkt 2014 ein leichter Rückgang zu verzeichnen; dabei gibt es keine deutlichen Unterschiede zwischen den Ländern.

Werden nun diejenigen, die eine Erhöhung des Budgets in den vergangenen zwei Jahren verzeichnen konnten, mit jenen 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[6]. Dieser Effekt zeigt sich nicht im Hinblick auf einen Anstieg des zur Verfügung stehenden Personals.

3.3 Strategische Entscheidungsmöglichkeiten im Unternehmen

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

Bei Entscheidungen mit unternehmensstrategischer Bedeutung sind lediglich 58,3 % der Befragten zumindest teilweise eingebunden (Antwortmöglichkeiten: „trifft voll zu“ und „trifft eher zu“). Im Hinblick auf die Gestaltung der Sicherheitsstrategie steigt der Anteil erwartungsgemäß an – auf 91,7 %.

Tabelle 1: Anstieg des Budgets 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	1,53
	Budget nicht gestiegen	2,08
Zufriedenheit mit der Unterstützung durch den Vorstand	Budget gestiegen	1,44
	Budget nicht gestiegen	2,13

Skala Zufriedenheit: 1=„sehr zufrieden“ bis 4=„sehr unzufrieden“

6 T=-2.736; p<.01; T=-3.564; p<.01

Als (mit)verantwortlich für die Konzeption und Planung des Krisenmanagements betrachten sich 85 %; ein noch etwas höherer Anteil von 88,3 % wird immer wieder von anderen Abteilungen aus dem Unternehmen in Anspruch genommen bzw. hinzugezogen, wodurch der Stellenwert im Unternehmen verdeutlicht wird.

Verantwortung und Einbindung ja, Anteil am Erfolg eher nein?

Wird allerdings die Einschätzung betrachtet, ob die Abteilung Konzernsicherheit bzw. der/die Sicherheitsverantwortliche und dessen/deren Arbeit als Bestandteil des Unternehmenserfolges gesehen werden, so ist diese deutlich weniger positiv ausgeprägt. Während 53,3 % zum Teil mit Einschränkungen annehmen, dass im Unternehmen diese Wahrnehmung vorherrscht, verbleibt ein nicht unerheblicher Anteil der Befragten, die eine mehr oder weniger deutliche pessimistische Position einnehmen. Dieser Wert ist im Vergleich zur Befragung 2014 unverändert (53,7 %). Hier wird die oft angeführte – und über die Jahre wenig veränderte – Diskrepanz zwischen der Bedeutung der eigenen Arbeit und des Themas „Sicherheit" einerseits und der Fremdeinschätzung bzw. des Images von „Sicherheit" im Unternehmen andererseits offensichtlich.[7]

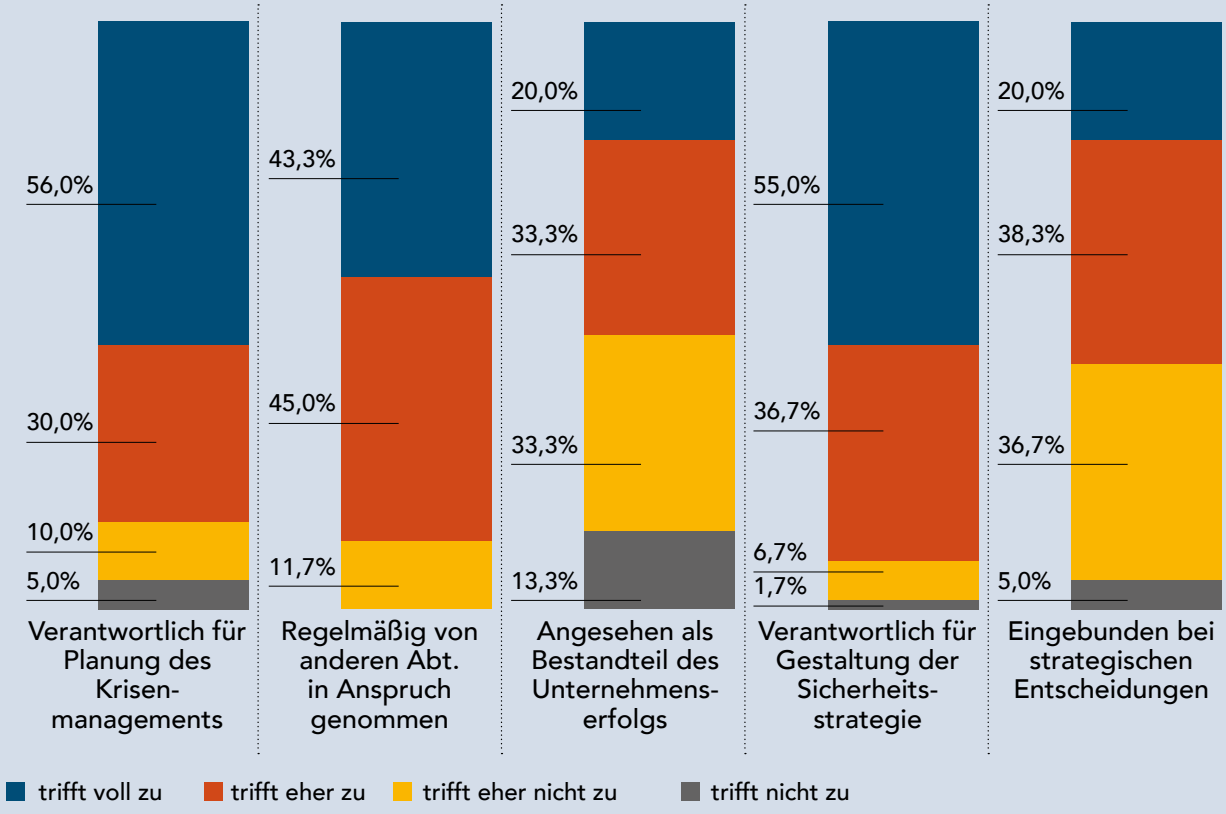
Kompetenzen: Governance-Funktion im Regelfall und Krisenstabsleitung im Sonderfall

Knapp drei Viertel (73,3 %) der Sicherheitsverantwortlichen sind gegenüber anderen Abteilungen in bestimmten Situationen weisungsbefugt (2014: 75,9 %). In Deutschland und der Schweiz liegt der Anteil bei jeweils etwa 80 %; in Österreich hingegen sind nur 41,7 % 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.

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 jede/r sechste Befragte aus Österreich (16,7 %; 2014: 50 %) gibt an, in bestimmten Situationen oder bei besonderen Ereignissen die Leitung des Krisenstabs zu übernehmen; in der Schweiz sind es dagegen 44,4 % (2014: 55,6 %) und in Deutschland sogar 3 von 4 Befragten (71,1 %; 2014: 78,1 %).

Abbildung 5: Bedeutung und strategische Einbindung der Abteilung Konzernsicherheit bzw. der Sicherheitsverantwortlichen (in %)



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")

Tabelle 2: Bedingungen für Weisungsbefugnisse

Grundsätzliche Befugnisse
• Governance in Form der „second line of defence“ • Policys/Standards in Safety & Security und Business Continuity (gelten für alle) • Fachliche Verantwortung, Richtlinienkompetenz und fachliches Weisungsrecht
Spezifische Befugnisse
• Notfall- und Krisensituationen (Incident & Crisis Management) • Auslands- und Reisesicherheit • Evakuierungen • Interne Ermittlungen, Incident Reporting • Informationsschutz • Veranstaltungsschutz • Einhaltung gesetzlicher Vorgaben

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 eine zu große Bedeutung beigemessen wird, erscheint es bedeutsamer, die Abteilungen Konzernsicherheit bzw. Corporate Security darzustellen. Im Folgenden erfolgt zunächst ein Überblick über jene Felder, die am häufigsten bzw. am wenigsten häufig in den Zuständigkeitsbereich der Befragten fallen.

Die Angaben zu den einzelnen – im Fragebogen vorgegebenen – Zuständigkeitsbereichen werden nun zuerst in den Abbildungen für die Gesamtstichprobe (über Organisationsformen und Länder hinweg) präsentiert. Danach werden jene Bereiche näher betrachtet, in denen die Länderergebnisse deutliche Unterschiede aufweisen.

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.

So geben 11,1 % der schweizerischen und 8,3 % der österreichischen Antwortenden an, dass „Know-how-Schutz“ in ihrem Unternehmen nicht relevant sei (DE 2,6 %). Damit wird das Thema bei einzelnen Unternehmen aus der Schweiz und Österreich als weniger wichtig eingestuft als in den Unternehmen aus Deutschland. 50 % der österreichischen und 44,4 % der schweizerischen Befragten erklären, dass sie für diesen Bereich nicht zuständig seien (DE 25 %).

Als weiteres interessantes Feld erweist sich die IT-Security: Während sich die Befragten aus schweizerischen Unternehmen mit 77,8 % als nicht zuständig beschreiben, trifft dies mit ca. 50 % nur auf die Hälfte der Teilnehmenden aus Österreich und Deutschland zu. Somit besteht bei der Hälfte der deutschen und österreichischen Unternehmen – und damit in einem weit größeren Ausmaß als in der Schweiz – für dieses Thema eine fachliche Zuständigkeit (zumindest teilweise).

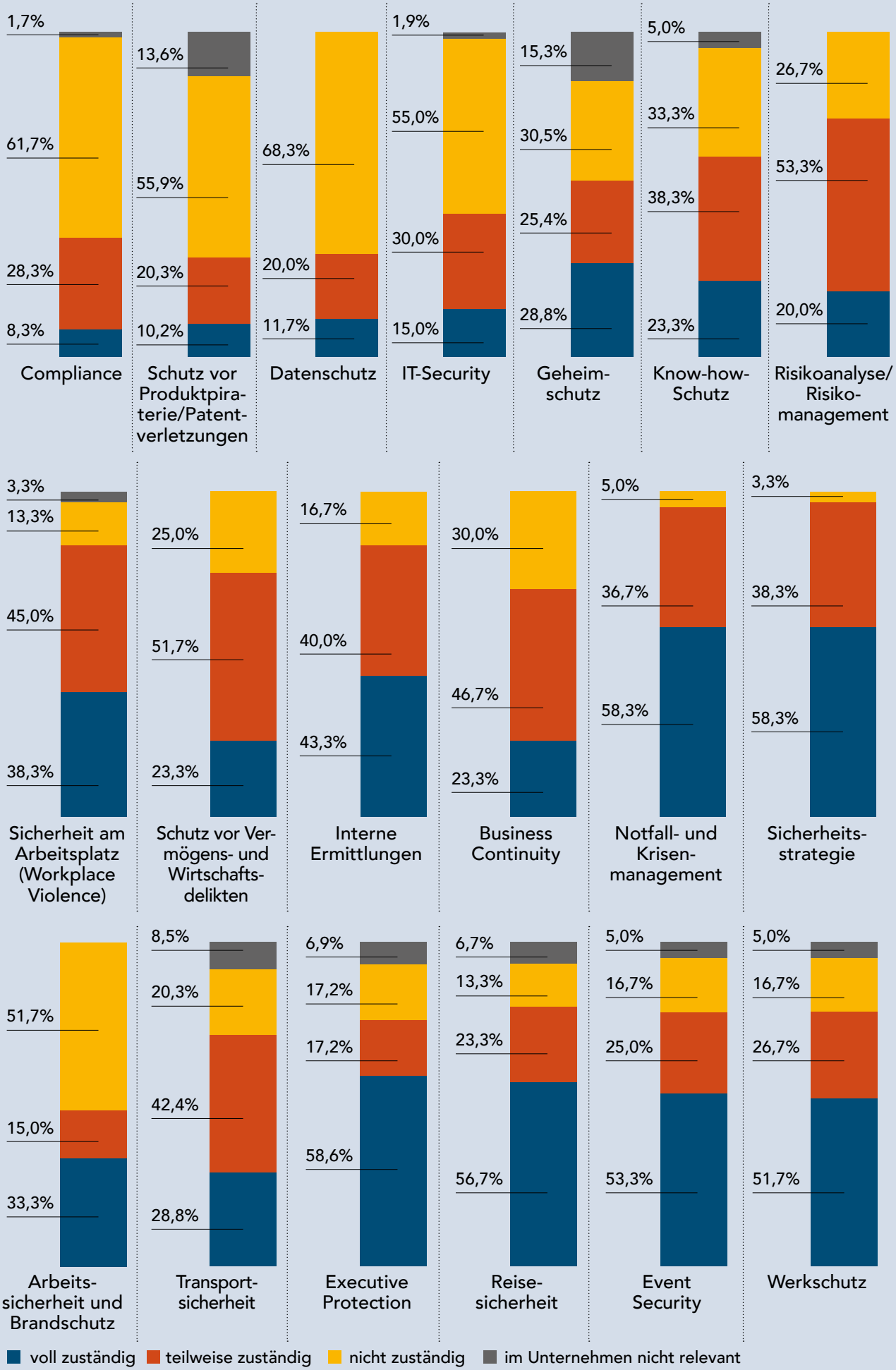
Bei der Betrachtung von Risikoanalyse und Risikomanagement überrascht das Ergebnis aus Österreich: Insgesamt erklärt sich nur die Hälfte der Befragten für diesen Bereich zuständig; in Deutschland sind es dagegen drei Viertel und in der Schweiz alle Teilnehmenden.
Ein interessantes Bild ergibt die länderspezifische Untersuchung der Aufgabenwahrnehmung im Bereich des Schutzes vor Vermögens- und Wirtschaftsdelikten. In den befragten deutschen Unternehmen liegt der Anteil der für diesen Bereich Zuständigen („voll zuständig“; „teilweise zuständig“) mit 84,6 % vergleichbar hoch, während sich in den Unternehmen aus Österreich und der Schweiz nur 58,3 % bzw. 55,6 % für zuständig erklären.

Unter Physical Security sind diverse Verantwortungsbereiche subsumiert; die Antworten lassen meist keine deutlichen Länderunterschiede erkennen (wohl aber Unterschiede in Abhängigkeit vom Aufbau der Sicherheitsstruktur im Unternehmen). In folgenden Bereichen wiederholt sich allerdings das zuletzt beschriebene Verantwortlichkeitsmuster mit einem geringen Anteil an Teilnehmenden aus schweizerischen und österreichischen Unternehmen, die für diese Bereiche zuständig sind (aufgelistet wird die Summe aus „voll zuständig“/„teilweise zuständig“): Event Security (CH 44,4 %, AT 75 %, DE 87,2 %,), Reisesicherheit (CH 55,6 %, AT 75 %, DE 87,2 %,), Executive Protection (AT 58,3 %, CH 62,5 %, DE 84,2 %,).

Tabelle 3: Hauptzuständigkeitsbereiche der Abteilungen Konzernsicherheit (n=46)
(Summe aus „voll zuständig"/„teilweise zuständig", in mind. 75% der Unternehmen)

	Zuständigkeitsbereiche	**2017**	**2014**
1.	Unternehmensweite Sicherheitsstrategie	**97,8%**	100%
2.	Notfall- und Krisenmanagement	**95,7%**	100%
3.	Interne Ermittlungen	**84,8%**	95,0%
4.	Risikoanalyse / Risikomanagement	**78,3%**	92,5%
5.	Werkschutz	**80,4%**	92,5%
6.	Event Security	**84,8%**	92,5%
7.	Reisesicherheit	**91,3%**	90,0%
8.	Know-how-Schutz/Geheimschutz	**67,4%/57,8%**	87,5%
9.	Schutz vor Vermögens- und Wirtschaftsdelikten	**78,3%**	87,5%
10.	Executive Protection	**84,4%**	87,5%
11.	Sicherheit am Arbeitsplatz (workplace violence)	**82,6%**	82,5%
12.	Business Continuity Management	**78,3%**	80,0%
13.	Transportsicherheit / Sicherheit der Lieferkette	**76,1%**	77,5%

Abbildung 6-8: Verantwortungs- und Zuständigkeitsbereiche



4. Sicherheitskultur und Kriminalitätsbelastung

4.1 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 Code of Conduct adressiert; 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.

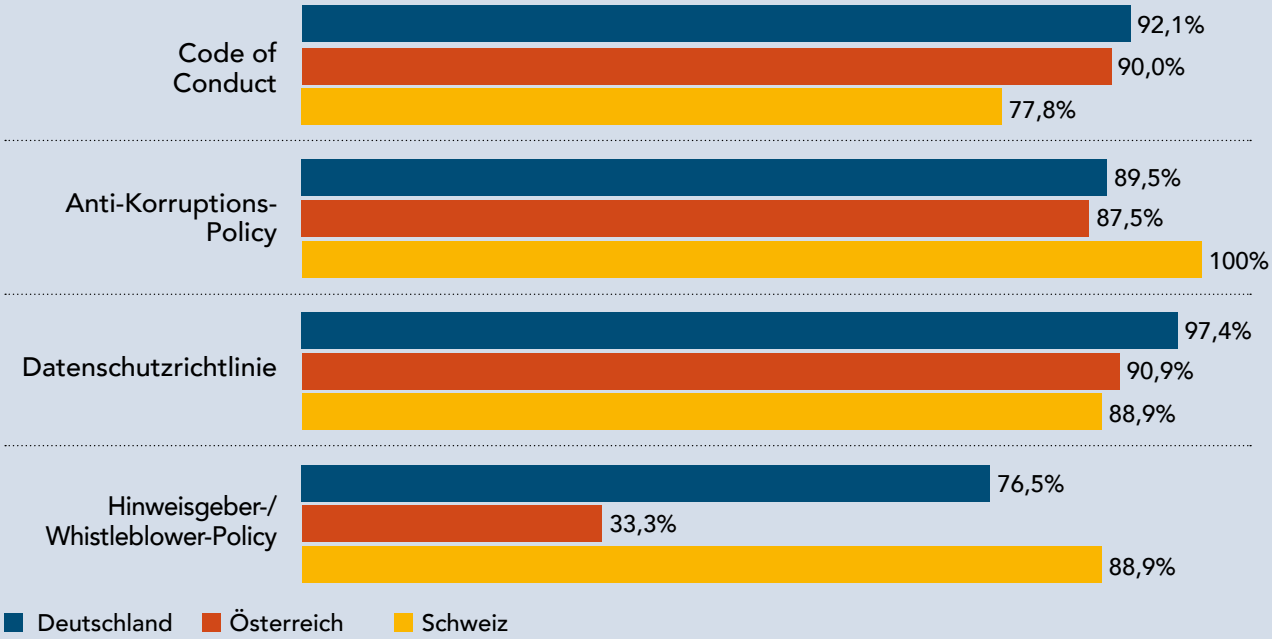
Insgesamt 89,5 % der Befragten geben an, dass in ihrem Unternehmen eine Verhaltensrichtlinie existiert, an der sich die Unternehmensangehörigen orientieren können. Unterschiede zwischen den Ländern illustriert die folgende Abbildung.

In der Befragung wurde auch das Vorhandensein weiterer Richtlinien bzw. Policys im Unternehmen erhoben: In über 90 % der Unternehmen, aus denen Antworten eingelangt sind, existieren eine Datenschutzrichtlinie sowie eine Anti-Korruptions-Policy. Sehr unterschiedlich ist die Situation in Bezug auf eine Hinweisgeber-/Whistleblower-Policy: Eine solche wurde in neun von zehn der deutschen, in drei von vier der schweizerischen, jedoch nur in einem Drittel der österreichischen Unternehmen eingeführt. In den Unternehmen aus Österreich, die sich an der Studie im Jahr 2014 beteiligten, lag der Anteil bei 53,8 %.

Hinweisgebersysteme: Nachholbedarf in Österreich

70 % aller befragten Unternehmen geben an, dass neben der Policy bei ihnen ein Hinweisgebersystem implementiert ist; bei weiteren 5 % befindet sich dieses aktuell im Aufbau. Auch in diesem Bereich sind die Unterschiede zwischen den einzelnen Ländern beträchtlich: Während von den schweizerischen nur 11,1 % und von den deutschen Unternehmen 15,4 % über kein (zumindest geplantes) Hinweisgebersystem verfügen, liegt der Anteil in Österreich mit 66,6 % deutlich höher. Diese Erkenntnis ähnelt dem Bild aus der Studie 2014, so dass weiterhin

Abbildung 9: Vorhandensein ausgewählter Policies



von einem gewissen Nachholbedarf in Österreich ausgegangen werden kann.

4.2 Maßnahmen zur Security Awareness

In den befragten Unternehmen spielen Maßnahmen zur Steigerung der Sensibilität für Sicherheitsfragen eine bedeutsame Rolle. 93,3 % aller Befragten der D-A-CH-Region setzen Maßnahmen oder Programme zur Security Awareness um. Die österreichischen Unternehmen liegen mit 83,3 % hinter den Unternehmen der anderen Länder (DE 94,9 %, CH 100 %).

Tabelle 4: Maßnahmen und Methoden

• Klassische Schulungen • Webbasierte Schulungen / Trainings • Regelmäßige Informationen und Neuigkeiten im Intranet • Regelmäßige Briefings zu aktuellen Entwicklungen • Regelmäßige Kommunikation über Bedrohungen
• Themenspezifische Kampagnen • Poster, Flyer, Broschüren • Kurzfilme und Video-Clips • „Gamification" • Fallschilderungen • Auseinandersetzung mit persönlicher Betroffenheit

Im Hinblick auf die Maßnahmen, die Unternehmen einsetzen, sind zunächst Schulungen zu nennen, die häufig für neue Beschäftigte angeboten werden. Neben Präsenzschulungen wird hier vermehrt auf e-learning und webbasierte Trainings gesetzt. Darüber hinaus spielt die Nachhaltigkeit der vermittelten Inhalte eine große Rolle: Unternehmen setzen dabei auf die wiederholte und regelmäßige Thematisierung spezifischer Inhalte auf unterschiedlichen Wegen. Auf neue Bedrohungsszenarien oder erneut aufzugreifende Phänomene wird mit besonderen Kampagnen reagiert. Neben klassischen Informationsmaterialien (Poster, Flyer, Broschüren) werden zunehmend bewegte Bilder in Form von Kurzfilmen und Video-Clips eingesetzt oder spielerische Varianten zur adressatengerechten Vermittlung gewählt („Gamification").

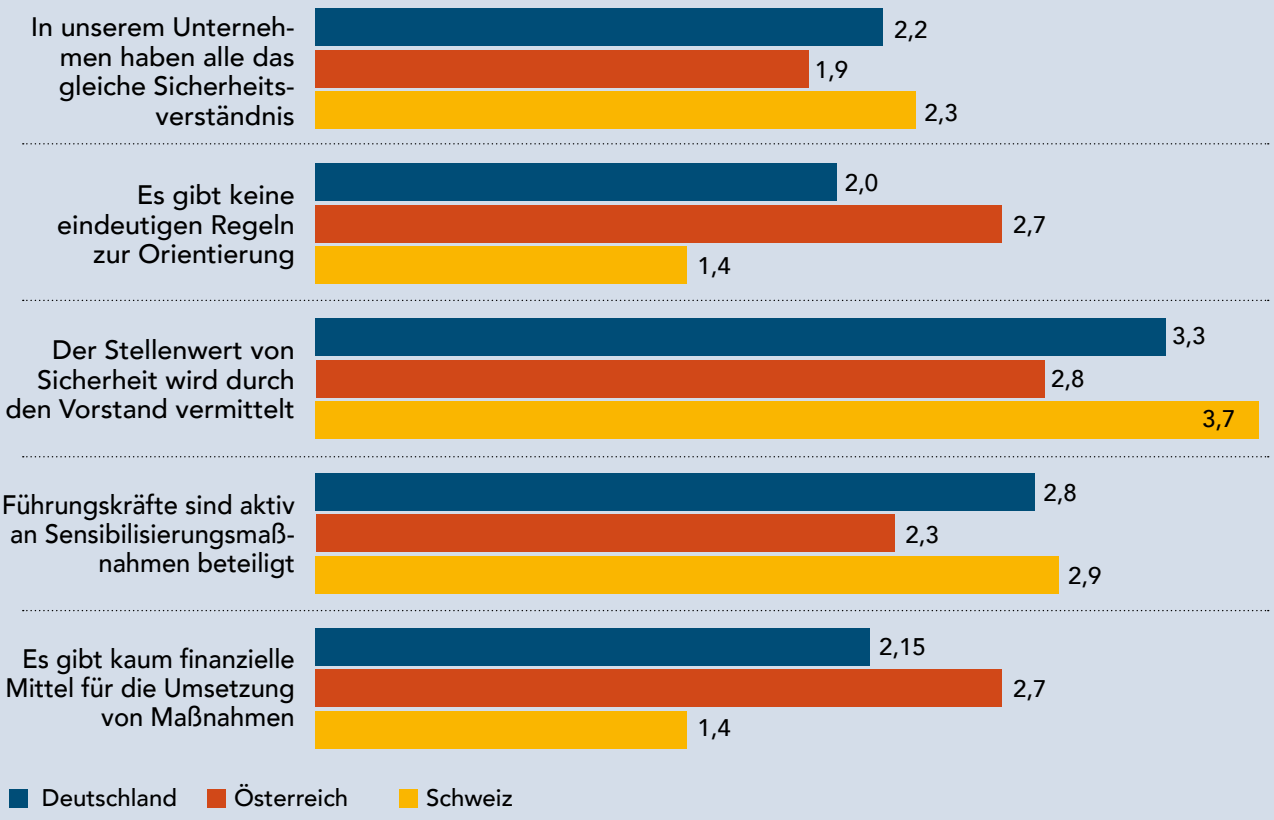
Tabelle 5: Themenbereiche und Kriminalitätsphänomene für Awareness-Maßnahmen

• CEO-Fraud • Betrugskriminalität • Umgang mit Bedrohungen, Gewaltkriminalität Cybersecurity • Know-how-Schutz / Informationsschutz • Social Engineering • Compliance • Korruption • Prävention • Reisesicherheit • Arbeitssicherheit (inkl. Evakuierungen)

Als wichtige Themenfelder für Awareness-Maßnahmen werden von den Befragten einerseits Basisthemen benannt, die wiederkehrend von Bedeutung sind, und andererseits Kriminalitätsphänomene mit aktueller Bedeutung oder Neuigkeitswert.

Interessant sind die Ergebnisse zum Sicherheitsverständnis in den Unternehmen. In der Gegenüberstellung der teilnehmenden Unternehmen nach Ländern wird deutlich, dass die schweizerischen Unternehmen zu den positivsten Einschätzungen gelangen: Der Stellenwert von Sicherheit wird vom Vorstand unterstrichen, und es beteiligen sich auch Führungskräfte an Awareness-Maßnahmen. Dagegen gibt es bei den kritischen Aspekten erhöhte Zustimmungswerte der österreichischen Befragten. So sind im Ländervergleich in diesen Unternehmen am wenigsten eindeutige Regeln zur Orientierung vorhanden, und es gibt die wenigsten finanziellen Mittel für Sensibilisierungsmaßnahmen.

Abbildung 10: Sicherheit und Sensibilisierung
(Skala: 1=„trifft nicht zu“ bis 4=„trifft völlig zu“; Mittelwert)

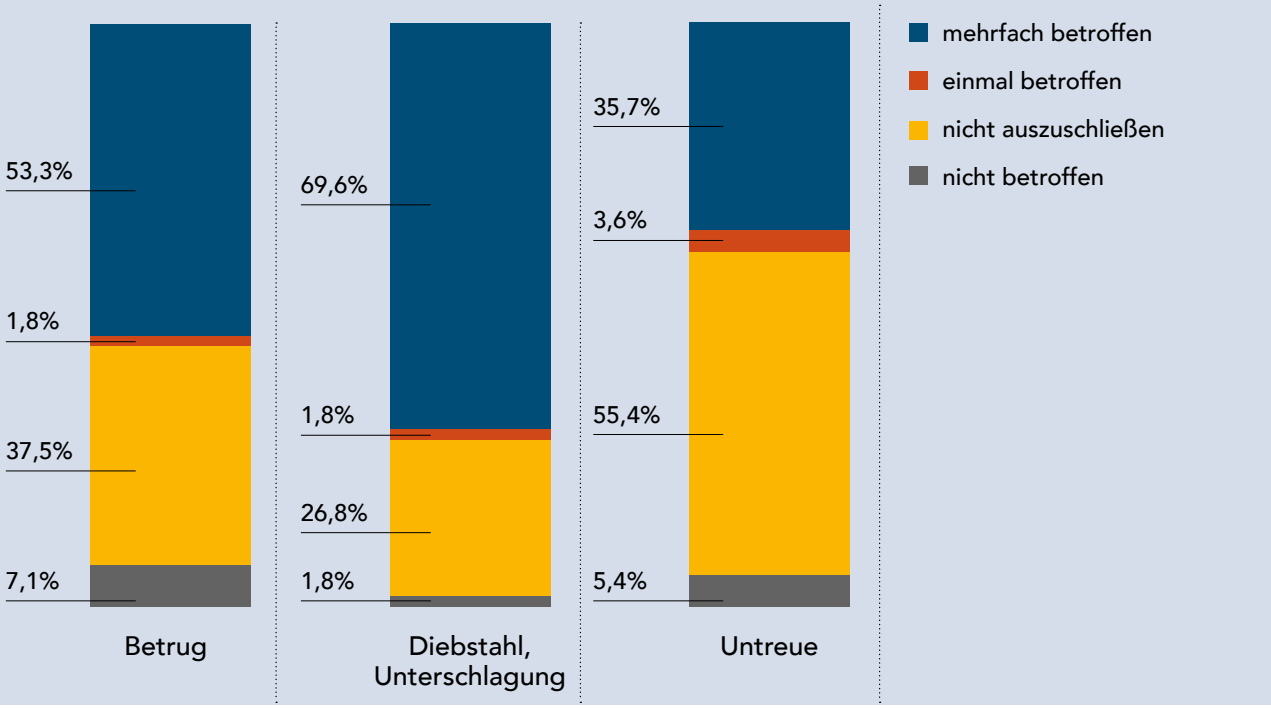


4.3 Kriminalitätsbelastung

Jedes Unternehmen kann von kriminellen Delikten betroffen sein. Gerade große Unternehmen geraten oft ins Visier. 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.

Abbildung 11: Vermögensdelikte – Betroffenheit der Unternehmen



Vermögensdelikte:
Von den vorgegebenen Delikten haben Vermögensdelikte die größte Auftretenshäufigkeit. Diebstahl und Unterschlagung hat in den befragten Unternehmen eine 2-Jahres-Prävalenz von 71,4 % (2014: 83 %). Das nächsthäufige Delikt ist Betrug mit einer Prävalenzrate von 55,1 % (2014: 58,3 %) gefolgt von Untreue mit 39,3 % (2014: 49 %).
Bei Betrachtung der Länder zeigt sich für Diebstahl und Unterschlagung eine besondere Situation. Schweizerische Unternehmen gaben in weit geringerem Ausmaß an, betroffen zu sein: bei Betrugsfällen lediglich 44,4 % (im Gegensatz zu DE 75 % und AT 72,7 %).

Wettbewerbsdelikte: Fälschung vor Datenverlust, hohe Unsicherheit über Betroffenheit
Bei den Wettbewerbsdelikten zeigt sich die höchste Betroffenheit bei Verstößen gegen das Patent- und Markenrecht mit 23,6 % gefolgt von Produktfälschungen mit 21,8 % (gleichzeitig eine hohe Nicht-Betroffenheit mit 49,1 %). Darüber hinaus existiert eine ausgeprägte Unsicherheit in Bezug auf die mögliche Betroffenheit („nicht auszuschließen") in den Bereichen Diebstahl von vertraulichen Unternehmensdaten (und damit Know-how-Verlust), Diebstahl von vertraulichen Kundendaten und Industrie- und/oder Wirtschaftsspionage.

Von 17,9 % der antwortenden Unternehmen wird ein Fall bzw. werden mehrere Fälle von Korruption und Bestechung in den vergangenen 24 Monaten angegeben (2014: 22,7 %). Zudem sind – in geringerem Ausmaß – Fälle von Kartellrechtsverstößen (12,5 %, 2014: 9 %) und Geldwäsche (7,4 %, 2014: 8,8 %) bekannt geworden. Die Angaben zu „nicht auszuschließen" sind jeweils Anzeichen für die Annahme eines gewissen Dunkelfelds an unentdeckt bleibenden Fällen. Bei Falschbilanzierung gab es keine Angaben zur festgestellten Betroffenheit.

Abbildung 12: Wettbewerbsdelikte – Betroffenheit des Unternehmens

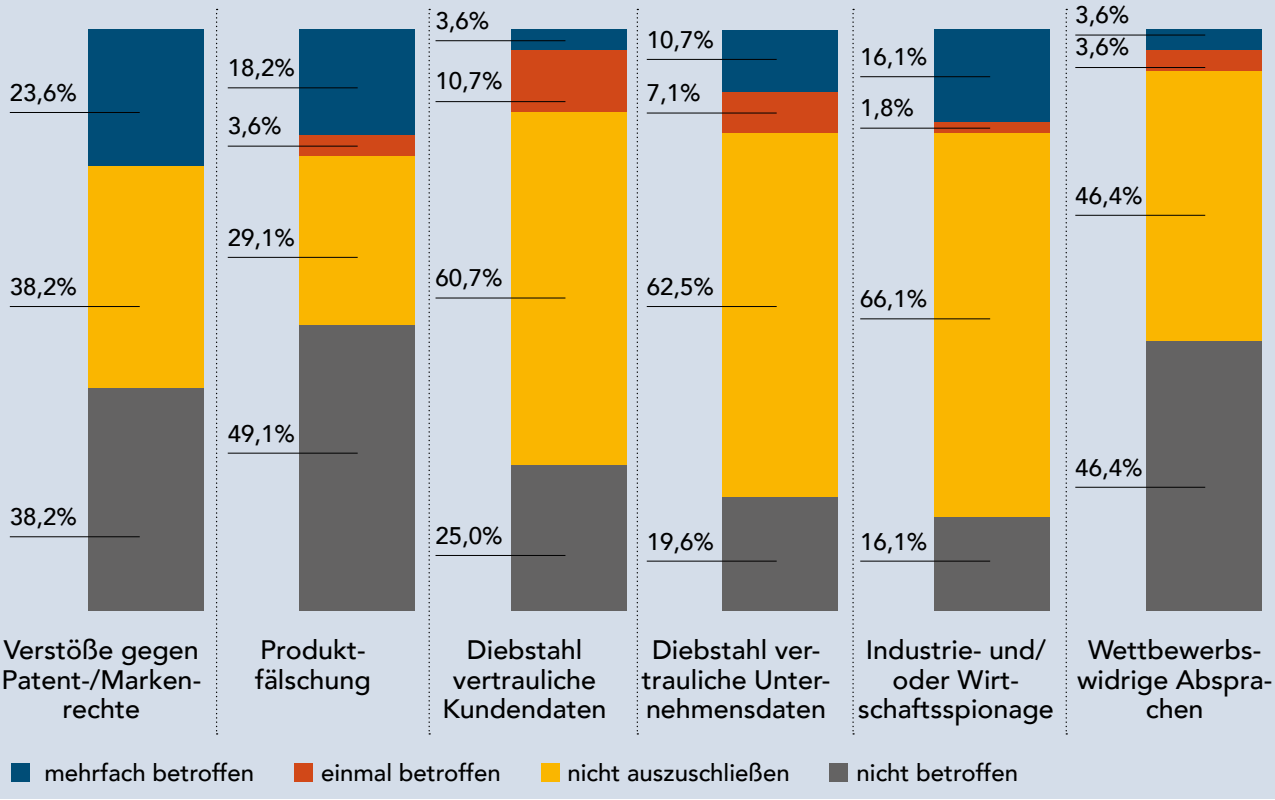
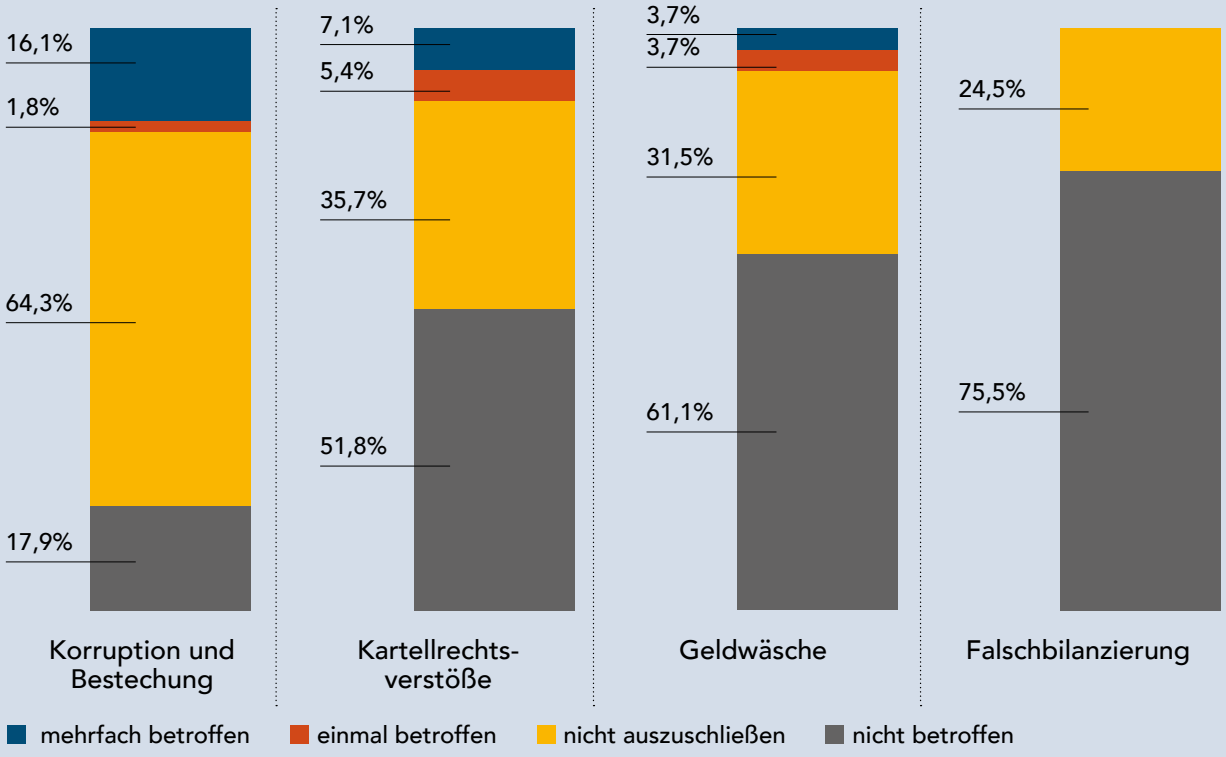


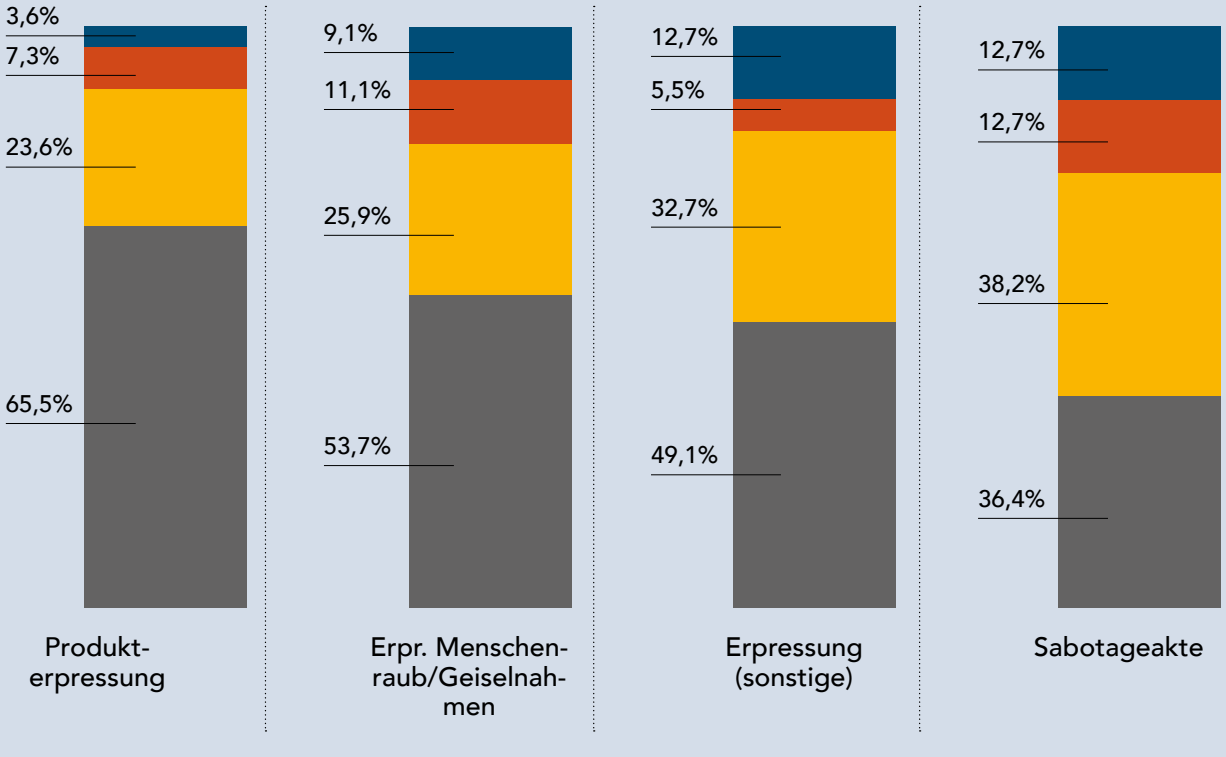
Abbildung 13: Andere Wirtschaftsdelikte – Betroffenheit des Unternehmens



Verbreitung von Erpressung und Sabotage

Eines von vier Unternehmen war in den vergangenen zwei Jahren Opfer von Sabotageakten. Unterschiedliche Formen der Erpressung dürften ebenfalls für einen nicht unerheblichen Anteil der Unternehmen von Bedeutung sein: 10,9 % waren von Fällen der Produkterpressung (2014: 6,5 %) und sogar 20,2 % von erpresserischem Menschenraub bzw. Geiselnahmen (2014: 10,5 %) betroffen. Weitere Formen der Erpressung wurden von 18,2 % der Befragten berichtet (2014: 21,3 %).

Abbildung 14: Erpressung und Sabotage – Betroffenheit des Unternehmens



Die Prävalenz soll nachfolgend für die Unternehmen mit Konzernsicherheitsabteilungen 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 Maße die teilnehmenden Konzerne von Delikten betroffen sind. Da sich die Angaben auf das unternehmensinterne Hellfeld beziehen, ist von weiteren – nicht bekannt gewordenen – Fällen auszugehen.

Im Vergleich zur Befragung 2014 ist ein Rückgang der berichteten Vermögensdelikte festzustellen. Bei den Wettbewerbsdelikten ist das Bild uneinheitlicher, wobei eine deutliche Zunahme im Bereich der Industrie- und/oder Wirtschaftsspionage zu verzeichnen ist. Andere Wirtschaftsdelikte wirken tendenziell rückläufig. Ein weiter zu untersuchendes Phänomen stellt die erhebliche Zunahme bei Produkterpressungen sowie auch – und insbesondere – bei erpresserischem Menschenraub / Geiselnahme dar.

4.4 Kriminalitätserfassung, Auswertung und Kommunikation von Delikten

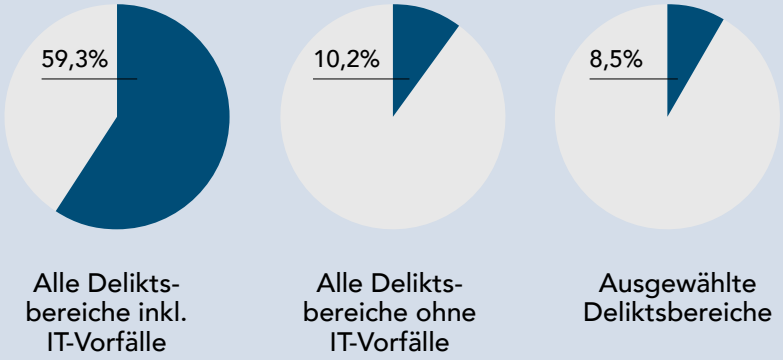
In welcher Form werden die Delikte erfasst, ausgewertet und im Unternehmen kommuniziert? Der folgende Abschnitt befasst sich mit der Erfassung und Aufbereitung von Vorfällen.
Insgesamt 69,5 % (2014: 72,3 %) aller befragten Unternehmen geben an, kriminelles Verhalten in allen Deliktsbereichen systematisch zu erfassen (mit oder ohne IT-Vorfälle). Weitere 8,5 % (2014: 6,4 %) beschränken die Erfassung auf spezifische Deliktfelder. Die Verbreitung der systematischen Erfassung variiert unter den Ländern: in Österreich 58,3 %, in Deutschland 68,4% und in der Schweiz 88,9 %.

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

Tabelle 6: Kriminalitätsbelastung der Unternehmen mit Konzernsicherheitsabteilung
2-Jahres-Prävalenz

Delikte	**Studie 2017 Abteilung Konzernsicherheit (n=46) im Unternehmen**	**Studie 2014 Abteilung Konzernsicherheit (n=40) im Unternehmen**
Betrug	59,5%	69,5%
Diebstahl / Unterschlagung	71,4%	97,2%
Untreue	45,3%	57,2%
Verstöße gegen Patent-/Markenrechte	26,2%	22,9%
Produktfälschung	22,8%	25,7%
Diebstahl vertraulicher Kundendaten	16,7%	14,3%
Diebstahl von Know-how, von vertraulichen Unternehmensdaten	21,4%	22,8%
Industrie- und/oder Wirtschaftsspionage	21,4%	14,3%
Wettbewerbswidrige Absprachen	4,8%	2,9%
Korruption und Bestechung	21,4%	30,3%
Kartellrechtsverstöße	11,9%	12,2%
Geldwäsche	7,3%	8,8%
Falschbilanzierung / Fälschung von Jahresabschlüssen	0,0%	0,0%
Sabotageakte	22,0%	29,7%
Produkterpressung	12,2%	5,8%
Erpresserischer Menschenraub / Geiselnahme	22,0%	13,5%
Erpressung (sonstige)	19,5%	25,0%

Abbildung 15: Systematische Erfassung bekannt gewordener Vorfälle/Taten



Wie bereits eingangs erwähnt sind die teilnehmenden Unternehmen, Banken und/oder Versicherungen überwiegend transnational tätig. Sie sind im Durchschnitt in 54 Ländern (2014: 42 Länder) vertreten. Auch hier gibt es deutliche Unterschiede zwischen den Herkunftsländern der Teilnehmenden: Die deutschen Unternehmen sind im Durchschnitt in 72 Ländern aktiv, die schweizerischen in 22 und die österreichischen in 7,5 Ländern.

In 69,6 % der Unternehmen, die Delikte zielgerichtet erfassen, bezieht sich dieses Vorgehen auf alle Standorte des Unternehmens weltweit (2014: 47,4 %), während sich 15,2 % der Unternehmen auf den Heimatstandort (2014: 26,3 %), 8,7 % auf den europäischen Raum (2014: 15,8 %) und 6,5 % auf nach anderen Kriterien ausgewählte Standorte (2014: 10,5 %) beschränken.

Berichtswesen unterschiedlich organisiert

Die erhobenen Daten zu den bekanntgewordenen Vorfällen werden von ca. 30 % dieser Unternehmen monatlich ausgewertet, von dem mit 40 % größten Teil halbjährlich und von ca. 30 % jährlich. In nahezu allen Fällen (93,2 %) werden die Ergebnisse an das Management berichtet.

Abbildung 16: Ausdehnung der systematischen Erfassung bekannt gewordener Vorfälle/Taten

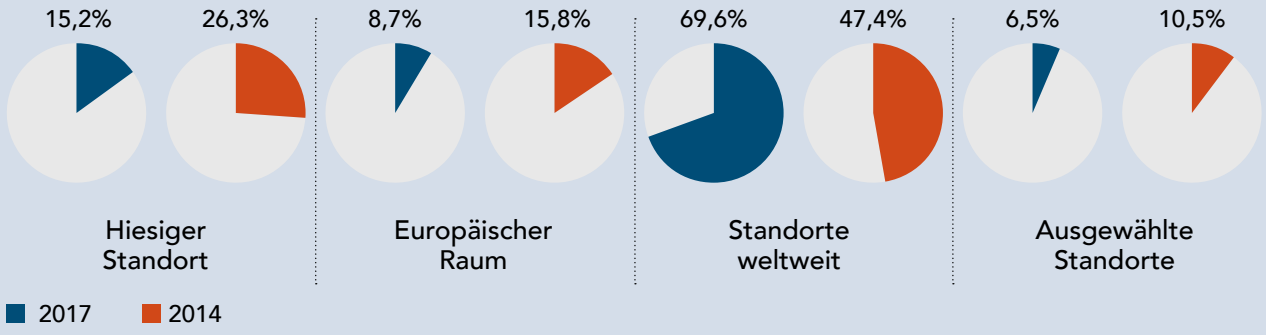
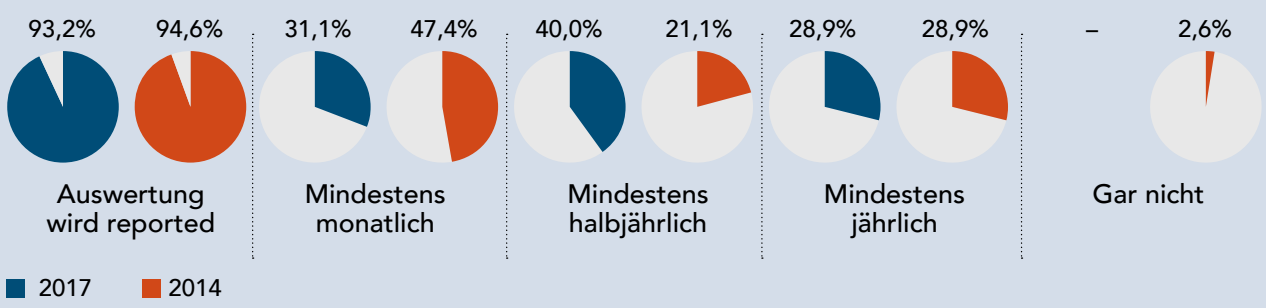


Abbildung 17: Häufigkeit und Kommunikation der Auswertung



5. Sicherheit im Ausland

5.1 Auslandsaktivitäten

Das Schwerpunktthema der vorliegenden Studie, die Sicherheit im Ausland, soll im Folgenden im Mittelpunkt der Ausführungen stehen. Zunächst erfolgt ein Überblick über den Einsatz von Mitarbeitenden und Unternehmensstandorte im Ausland.

Bis auf fünf Unternehmen sind alle befragten Unternehmen auf irgendeine Weise im Ausland aktiv.[8] Im Hinblick auf Mitarbeitende, die länger als ein Jahr im Ausland tätig sind, gibt es die deutlichsten Unterschiede zwischen den beteiligten Ländern.

Der Großteil der Aktivitäten findet in Ländern mit geringem oder mittlerem Risiko statt. Hier werden die meisten Auslandsreisen registriert und Expatriates eingesetzt. Dies gilt auch im Hinblick auf die Standorte im Ausland. Weniger als die Hälfte der Unternehmen ist in Ländern mit erhöhtem Risiko aktiv, wobei auch in diesen Unter-

Tabelle 7: Aktivitäten der Unternehmen im Ausland (nach Land)

	gesamt	Deutschland	Österreich	Schweiz
Auslandsreisende (< 1 Jahr im Ausland)	89,7%	92,1%	83,3%	87,5%
Expatriates (> 1 Jahr Ausland)	75,9%	84,2%	66,7%	50,0%
Unternehmensstandorte im Ausland	86,4%	89,5%	83,3%	77,8%

Tabelle 8: Aktivitäten der Unternehmen in Ländern mit hohem Gefährdungspotenzial

Hohes Risiko	**Anteil der Unternehmen, die in Ländern mit hohem Risiko aktiv sind (von N=60)**	**Anteil dieser Risikogruppe in den Unternehmen, die dort aktiv sind**
Auslandsreisende (< 1 Jahr im Ausland)	50,0%	1 % - 40% ($\bar{x}$=12,4%)
Expatriates (> 1 Jahr Ausland)	33,4%	1 % - 30% ($\bar{x}$=8,6%)
Unternehmensstandorte im Ausland	45,0%	1 % - 40% ($\bar{x}$=13,5%)
Extremes Risiko	**Anteil der Unternehmen, die in Ländern mit extremem Risiko aktiv sind (von N=60)**	**Anteil dieser Risikogruppe in den Unternehmen, die dort aktiv sind**
Auslandsreisenden (< 1 Jahr im Ausland)	33,3%	1 % - 20% ($\bar{x}$=5,5%)
Expatriates (> 1 Jahr Ausland)	11,7%	1 % - 20% ($\bar{x}$=6,9%)
Unternehmensstandorte im Ausland	15,0%	1 % - 20% ($\bar{x}$=9,8%)

8 Die weiteren Ausführungen und Prozentangaben beziehen sich – sofern nicht anders ausgewiesen – auf n=55 Unternehmen mit Auslandsaktivitäten.

nehmen diese Standorte nur einen geringen Anteil ausmachen.

Insgesamt gaben die Unternehmen, für die Beschäftigte ins Ausland reisen bzw. im Ausland länger tätig sind, für das Referenzjahr 2015 durchschnittlich 3.971 Personen pro Unternehmen als Auslandsreisende und/oder Expatriates an. Dieser Durchschnitt verzerrt das Bild erheblich, da die Varianz von einstelligen Reisezahlen bis zu 100.000 Personen reicht. Daher erfolgt eine sinnvolle Annäherung über den Median, der bei 400 Personen liegt.

Im Hinblick auf das Ausmaß der Mobilität der MitarbeiterInnen unterscheidet sich auch der Informationsweg, über den die Sicherheitsabteilung von der Planung von Reisen in kritische Länder erfährt. In 22 % der Unternehmen erfolgt keinerlei Meldung – auch nicht bei sicherheitsrelevanten Reisen, da in vielen Fällen keine Verpflichtung besteht und es keine geübte Praxis gibt, diese anzuzeigen. Unabhängig von einer möglichen Verpflichtung wird in anderen Unternehmen auf Freiwilligkeit und die Sensibilität der einzelnen Reisenden gesetzt. In 16 % der Unternehmen sind es explizit die Reisenden selbst, die der Sicherheitsabteilung ihr Vorhaben mitteilen. Darüber hinaus nennen weitere 16 % der Befragten eine ganze Reihe unterschiedlicher Verfahrensweisen: Anmeldung durch Vorgesetzte, betriebliche Abteilung, VISA-Abteilung oder HR.

Der verlässlichste Weg zur Meldung einer sicherheitskritischen Reise oder eines längeren Aufenthalts ist die Nutzung eines automatisierten Informationssystems. Ein solches System (Tracking Programm) wird von 54,5 % der Unternehmen verwendet.

5.2 Organisation und Stellenwert der Sicherheit im Ausland im Unternehmen

In einer Vielzahl der Unternehmen ist die Sicherheit im Ausland an die (Konzern-)Sicherheitsabteilung angebunden (76,9 %). Neben dem kompletten Outsourcing an externe Anbieter (9,6 %) existieren insbesondere Mischformen, bei denen die Abteilung für Konzernsicherheit mit externen Dienstleistungsunternehmen zusammenarbeitet (10,2 %).

Für die Standorte im Ausland werden vornehmlich die nachfolgend aufgeführten Lösungen gewählt.

Das vollständige Outsourcing wird nur von einem kleineren Anteil der Unternehmen angewandt (9,6 %), die Einbindung und Verantwortung des eigenen Unternehmens und seiner Sicherheitsverantwortlichen steht dagegen im Vordergrund.

Die Akzeptanz von Maßnahmen zur Sicherheit im Ausland wird insgesamt deutlich positiv eingeschätzt: Maßnahmen werden laut den Antwortenden weitgehend

Abbildung 18: Organisation von Sicherheit an den Standorten im Ausland (in %)

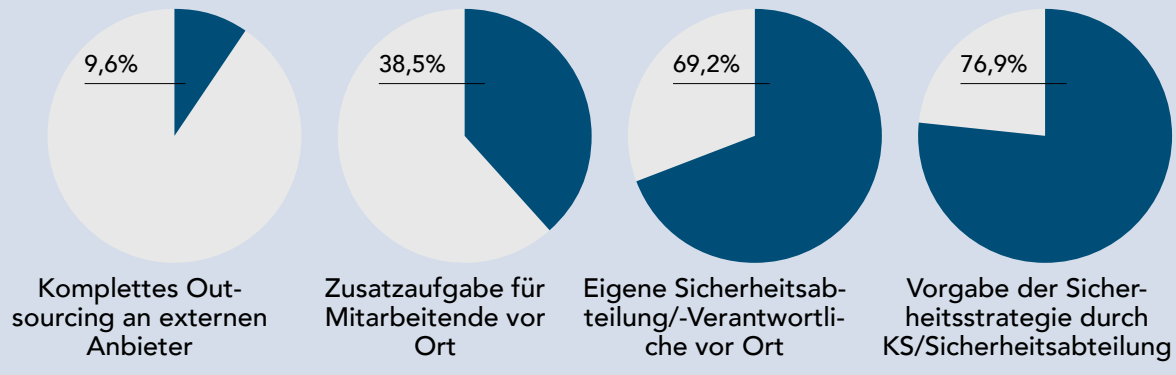
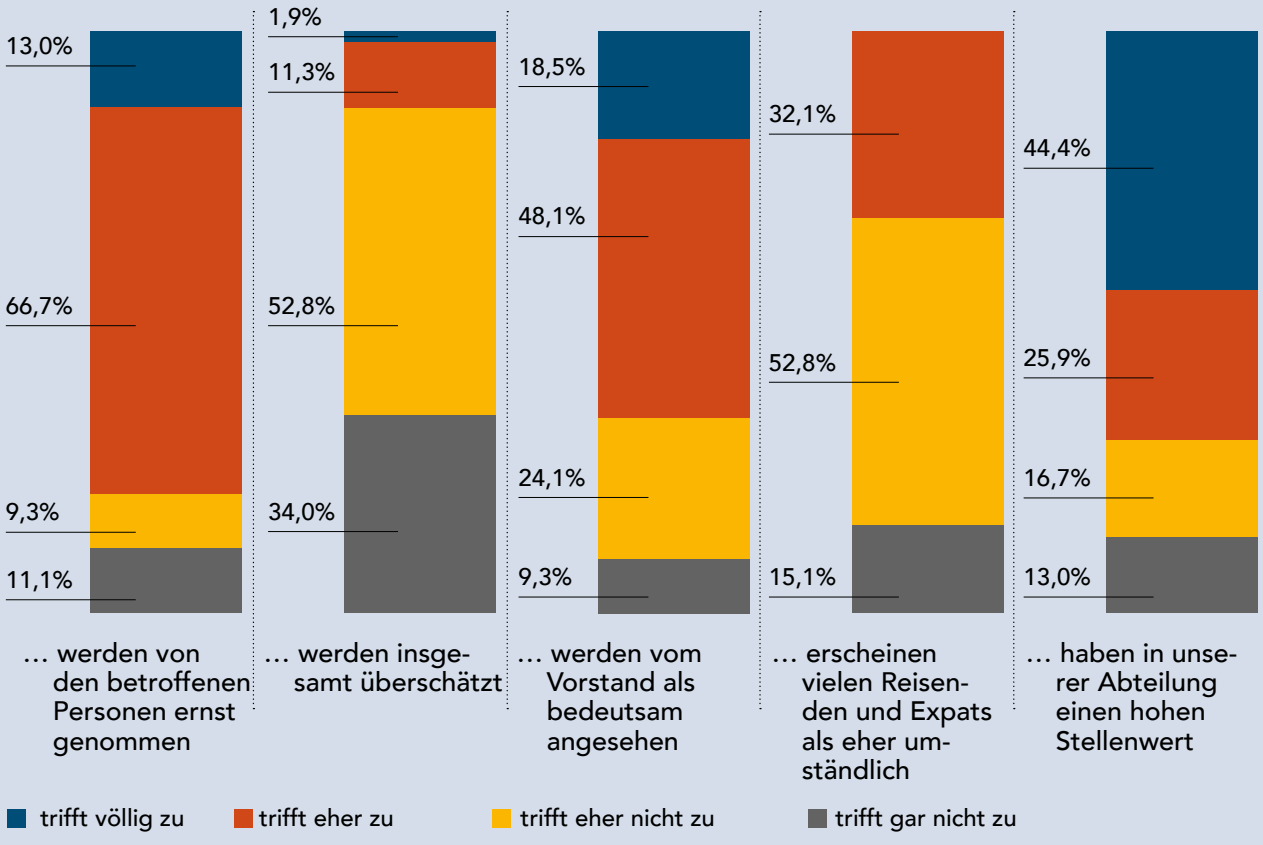


Abbildung 19: Maßnahmen zur Sicherheit im Ausland (in %)



ernst genommen (79,7 %) und haben einen hohen Stellenwert sowohl in der Abteilung (70,3 %) als auch beim Vorstand (66,6 %). Die Annahme, dass diese Maßnahmen überschätzt werden, lehnen 86,8 % der Befragten ab; jene, dass sie von der Zielgruppe als eher umständlich wahrgenommen werden, immerhin 67,9 %.

5.3 Beurteilung des Sicherheitsrisikos

Ein einheitliches Dokument zur Reisesicherheit, das Maßnahmen umschreibt und den Prozess der Risikobewertung abbildet, liegt in 58,2 % der befragten Unternehmen mit Auslandsaktivitäten vor. Zudem verfügen insgesamt 70,9 % über ein Klassifikationssystem für die Einstufung der Länder bzw. Landesteile in „low, medium, high or extreme risk".

Welche Grundlagen sind in den Unternehmen vorhanden, die der Einschätzung von Sicherheitsrisiken dienen? Anhand der Angaben der Sicherheitsverantwortlichen lassen sich verschiedene Strategien identifizieren. Im Sinne von „good practice" setzt der größte Anteil der Befragten hier auf eigene Expertise und Erfahrung kombiniert mit Einschätzungen externer Dienstleistungsunternehmen und Informationen von Behörden. Zu jeweils ungefähr gleichen, geringen Anteilen wird in den Unternehmen ausschließlich der eigenen Risikoeinschätzung vertraut oder ausschließlich auf externe Dienstleistungsunternehmen zurückgegriffen. Vereinzelt werden lediglich Behördeneinschätzungen herangezogen.

Insgesamt 69,2 % der Unternehmen stützen sich auf die Kategorisierung der Länder bzw. Regionen durch externe Anbieter oder beziehen diese mit ein; die übrigen Unternehmen bewerten das Risiko selbst und ziehen verschiedene Erkenntnisquellen heran, um eine fundierte Einschätzung zu erhalten.

Tabelle 9: Vorgehen bei der Bewertung des Siherheitsrisikos

Vorgehen	Quellen	
• Eigene Methodik • Analyse der Quellen • Lageauswertungen • Risikomatrix • Bewertung / Assessment	• OSINT (Open Source Intelligence) • Beurteilungen bzw. Reports externer Anbieter • Staatliche Informationen	• Security Management vor Ort • Lokale Quellen • Erfahrungen • Erkundungen / Länderbesuche

5.4 Einschätzung der Gefährdungslage, Evakuierungen und Frühwarnsystem

Die Auswertung der Ergebnisse zu diesen Themenfeldern bezieht sich auf eine Teilgruppe der Befragten, die sich intensiv mit diesen Fragen befasst und Freitextantworten formuliert hat. Einzelnen anderen Befragten waren die Fragen in diesem Komplex zu sicherheitssensibel.

Im Folgenden soll eine zusammenfassende Darstellung der Erkenntnisse im Sinne einer qualitativen, heuristischen Auswertung erfolgen und evtl. als Anregung oder Beispiel für „good practice" dienen.

Von den n=40 Sicherheitsverantwortlichen, die sich zur Einschätzung der Gefährdungslage und relevanten Indikatoren geäußert haben, haben n=12 Befragte zum Teil ausschließlich auf die herangezogenen Quellen bzw. das methodische Vorgehen Bezug genommen, während ins-

Tabelle 10: Indikatoren zur Einschätzung der Gefährdungslage (n=40)

Politische Lage (n=28)	
• Politische Stabilität / Instabilität • Geopolitische Lage • Rechtsstaatlichkeit, Zuverlässigkeit staatlicher Sicherheitsorgane	• Zivile Unruhen, soziale Spannungen • Bewaffnete Auseinandersetzungen, Bürgerkrieg • Politisch-militärische Situation • Einfluss von Nachbarregionen
Kriminalitätsphänomene/Kriminalitätsentwicklung (n=26)	
• Allgemeine Kriminalitätslage und Kriminalitätsentwicklung • Ausmaß an Schwerstkriminalität • Organisierte Kriminalität	• Präsenz extremistischer, krimineller Strukturen • Gefahr von Überfällen, Geiselnahmen • Korruption • Datenabfluss, Datendiebstahl
Gefahr von Naturereignissen/-katastrohen (n=9)	
Medizinische Versorgung/Gesundheitsrisiken (n=7)	
Sozio-ökonomische Situation (n=7)	
• Wirtschaftliche Situation / Stabilität	• Soziale Lage
Spezifische Aspekte der Reise/des Auftrags (n=3)	
• Profil der reisenden Person • Art der Tätigkeit	• Qualität der Unterbringung unter Sicherheitsgesichtspunkten

Quellen / Methodik (n=12)	
• Eigene Bewertungen, Erfahrungen und Analysen • Einschätzung von Dienstleistern • Reports, Benchmarks • Sicherheitsnetzwerke • Staatliche Informationen verschiedener Länder	• Kontakte im Zielland: externe Spezialisten, Mitarbeitende, Locals • Lageinformationen aus offenen Quellen • Medien

gesamt n=30 Personen Indikatoren benennen, die im Folgenden aufgeführt sind.

Die vielfältigen Faktoren, die zur Einschätzung der Gefährdungslage herangezogen werden, werden im besten Fall kontinuierlich analysiert und ausgewertet.

Zu welchem Zeitpunkt eine Entscheidung für eine Evakuierung von Unternehmensangehörigen fällt und welche Kriterien von den Unternehmen dafür als wesentlich erachtet werden, wird nachfolgend dargestellt.

Die Durchführung und Umsetzung einer Evakuierung ist abhängig von der jeweiligen Lage und dem Stadium der Entwicklungen.

Die in der konkreten Situation zur Verfügung stehenden Mittel bestimmen die Realisierung einer Evakuierung. Sofern es möglich ist, Linien- oder Charterflüge oder auch den Landweg zu nutzen, erfolgt eine Evakuierung häufig mit eigenen Ressourcen und gemäß der eigenen operativen Planung. Regelmäßig werden spezialisierte Dienstleistungsunternehmen hinzugezogen und weitere

Tabelle 11: Indikatoren zur Entscheidung für eine Evakuierung (n=44)

Gefahr für Leib und Leben	
Eine Gefahr für Leib und Leben ist allen Aussagen inhärent. Diese Gefahr / Bedrohung muss akut, konkret, unmittelbar oder wahrscheinlich sein und anders nicht abgewendet werden können.	
Ereignisse	
• Nachhaltige Beeinträchtigung der Sicherheitslage • Kriegerischer Konflikt • Erhebliche politische Unruhen • Erhebliche Terrorgefahr • Gezielte Angriffe gegen AusländerInnen	• Bevorstehende oder erfolgte Naturkatastrophe • Epidemie, Pandemie oder andere erhebliche Gesundheitsrisiken • Medizinische Versorgung ist nicht (mehr) gegeben • Infrastrukturelle Krise mit absehbar erheblichen Versorgungsengpässen
Weitere Anzeichen	
• Schließung der Landesgrenze möglich • Schließung von Flug-, See- und Landwegen / fehlende Logistik • Gefährdung der letzten Evakuierungsmöglichkeit durch drohende Besetzung des Flughafens • Botschaften geschlossen	• Hinweise / Empfehlungen von staatlichen Stellen • Einschätzungen von ExpertInnen, Sicherheitsberatungen • Einschätzung des Personals vor Ort, Hinweise von eigenen Standorten • Risikoempfinden des/der Mitarbeitenden

Tabelle 12: Bestandteile eines Frühwarnsystems (n=21)

Elemente	
• Einteilung/Kategorisierung sicherheitskritischer Ereignisse mit Beschreibungen und festgelegten Parametern • Definition von Triggern, Indikatoren; Intelligence; lokale und globale/generelle Information • Risk Warning System, Risk Infos, Expat-Listen, Duty Travel Listen • Info-Push via Travel-Tracker (bspw. bei Aufenthalt von Reisenden in/an „Incident Hotspots" oder bei „relevanten Ereignissen" in der Nähe von Unternehmensstandorten)	
Struktur	
• 24/7 Lagezentrum • Eigener Analysebereich, ständige eigene Risikobewertungen	• Lagebeurteilung durch Konzernsicherheit • ggf. Veränderung des Security-Levels mit den damit verbundenen Maßnahmen
Monitoring	
• Presse Monitoring • Event Analysen • Alerts externer Dienstleister	• (Tägliche) Auswertung von Risikodatenbanken • Situationsbeobachtungen der Landesvertretungen, staatliche Warnhinweise
Informationsaustausch	
• mit (verschiedenen) externen Dienstleistern (vor Ort) • mit Behörden, Auswärtigem Amt, Landesvertretungen	• mit lokalen Sicherheitsbeauftragten • mit Tochterunternehmen und/oder anderen Unternehmen • im nationalen/internationalen Netzwerk
Ereignisse (siehe Tabellen 10 und 11)	

Partner sowie die Behörden eingebunden (auch zur Koordination staatlicher und nicht-staatlicher Maßnahmen).

Unternehmen verfügen – im Sinne von „good practice" – für einen solchen Ernstfall über aktuelle Notfallpläne und Evakuierungspläne für die entsprechende Risikoregion. Diese sollten nach Angabe eines Befragten folgende Punkte adressieren: „Krisenstab, Landesgesellschaft, Werk, Mitarbeitende; Reisende separat; Evakuierung (Listen), Direktive, Sammelpunkt, Ausreise".

Wenn ein Monitoring der Situation und Entwicklung im Land erfolgt und nicht allein auf die Einschätzung von Dienstleistern und Behörden abgestellt werden soll, bedarf es spezifischer Kriterien zur Lageeinschätzung. Somit soll untersucht werden, inwiefern die befragten Unternehmen eigene Indikatoren entwickelt bzw. ein eigenes Frühwarnsystem etabliert haben, um eine krisenhafte Entwicklung vorzeitig erkennbar zu machen.

Insgesamt n=51 Antwortende haben sich zu diesem Aspekt geäußert: 41,2 % der befragten Unternehmen verfügen demnach über ein Frühwarnsystem oder haben spezifische Indikatoren entwickelt (DE 51,5 %, CH 25 %, AT 20 %). Von den n=21 Unternehmen mit Frühwarnsystem kommen n=17 aus Deutschland, n=2 aus der Schweiz und n=2 aus Österreich. In der folgenden Tabelle sind die jeweiligen Ausführungen zusammengefasst, wobei es sich bei den spezifischen Unterpunkten auch um Einzelaussagen handeln kann.

Deutlich wird, dass in einem Unternehmen die strukturellen Bedingungen zur federführenden Lagebeurteilung vorhanden sein oder geschaffen werden müssen. In diesem Analysebereich werden dann jene Informationen erhoben, gesammelt und analysiert, die die Identifikation vorher definierter Faktoren, Hinweise oder Auslöser ermöglichen, um sicherheitskritische Ereignisse frühzeitig zu detektieren.

5.5 Vorbereitungsmaßnahmen für Reisende oder Expatriates für „high risk regions"

Im Mittelpunkt der folgenden Ausführungen stehen Maßnahmen, die vor einem Aufenthalt von Unternehmensangehörigen in sogenannten „high risk regions" getroffen werden. Unter „high risk regions" werden dabei jene Länder und Regionen mit einem hohen oder extremen Gefährdungspotential subsumiert.

Im Hinblick auf sicherheitsrelevante Vorbereitungsmaßnahmen wird deutlich, dass keine der im Folgenden näher aufgeführten Maßnahmen in allen Unternehmen regelmäßig durchgeführt wird. Schulungen für Expatriates werden insgesamt deutlich häufiger angeboten als für Auslandsreisende.

Abbildung 20: Sicherheitsrelevante Vorbereitungsmaßnahmen für Auslandsreisende (n=42, in %)

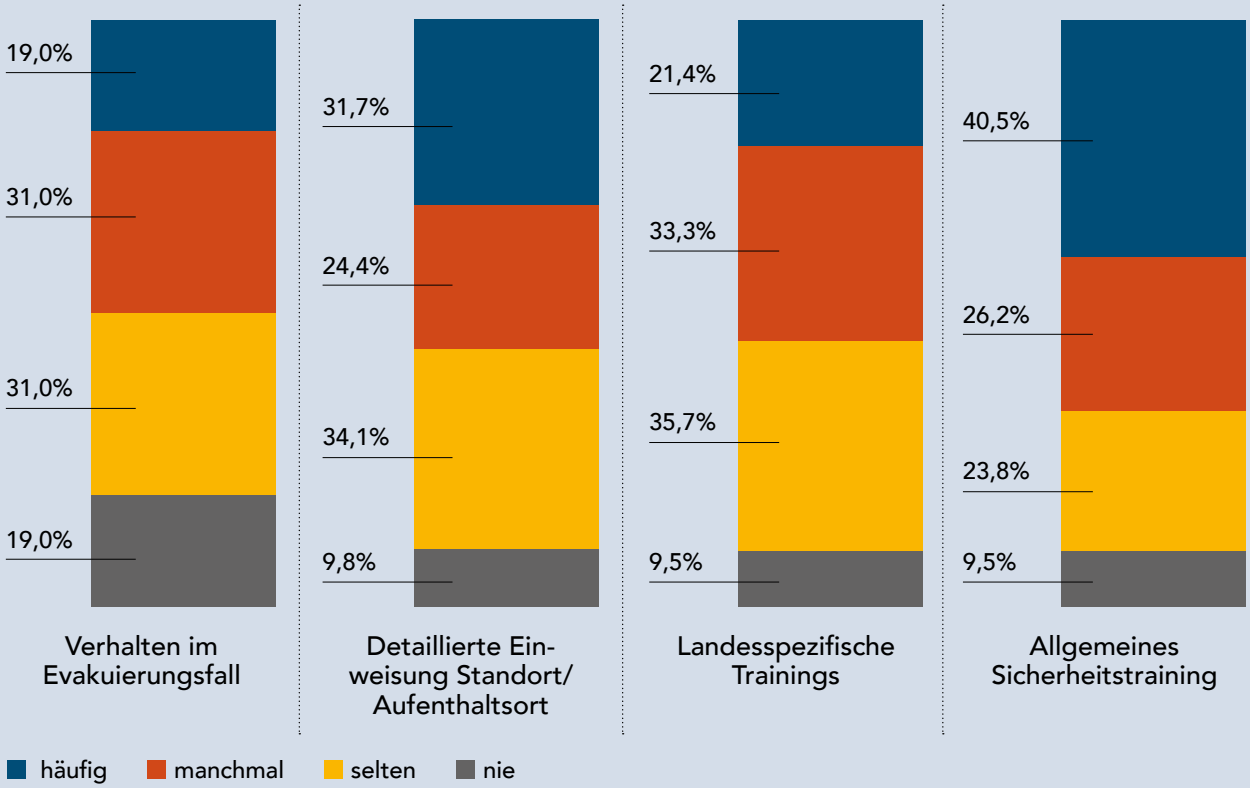
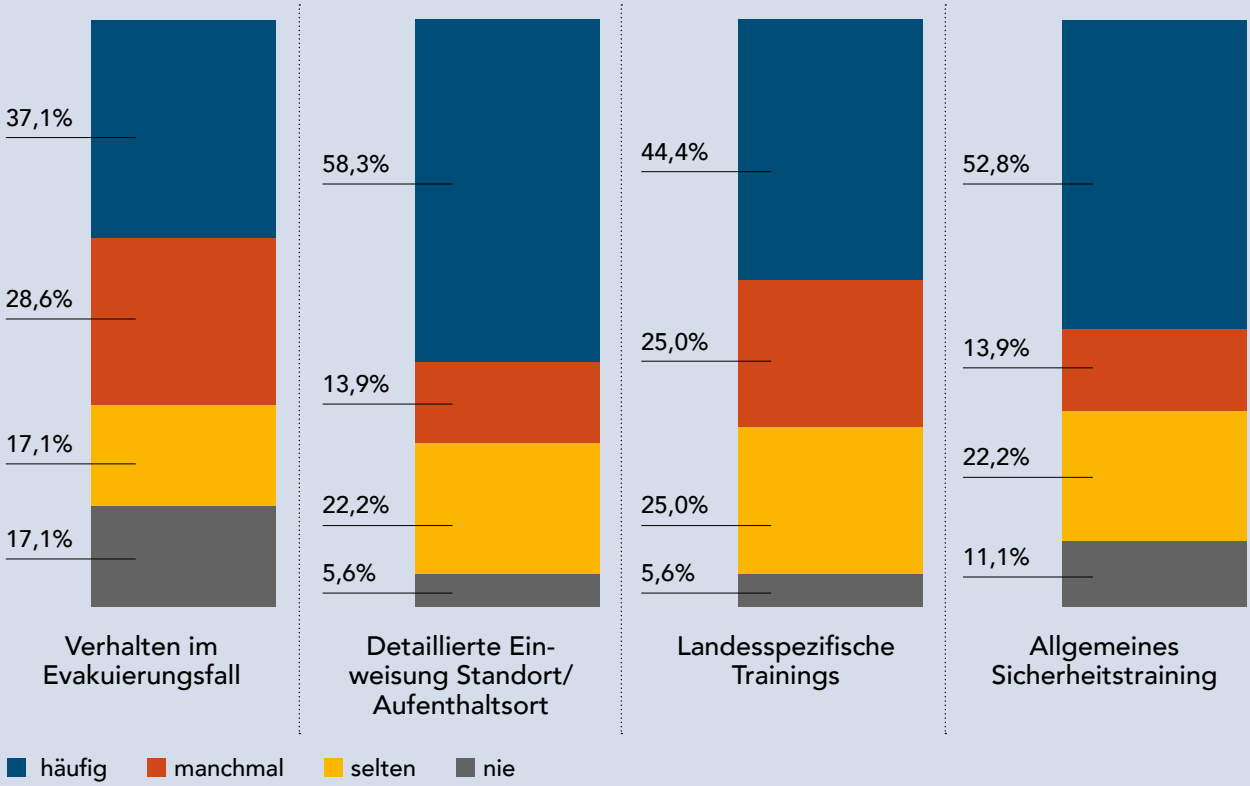


Abbildung 21: Sicherheitsrelevante Vorbereitungsmaßnahmen für Expatriates (n=36, in %)



Diejenigen Unternehmen, die Vorbereitungsmaßnahmen – wie oben und nachfolgend dargestellt – häufig durchführen, verfügen eher über automatisierte Meldeprozesse (Travel Tracking System) sowie auch und insbesondere über ein eigenes Frühwarnsystem. Es kann somit festgestellt werden, dass diese Unternehmen eine hohe Sensibilität für das Thema „Sicherheit im Ausland" aufweisen.

Abbildung 22: Sicherheitsrelevante Vorbereitungsmaßnahmen für Auslandsreisende (n=42, in %)

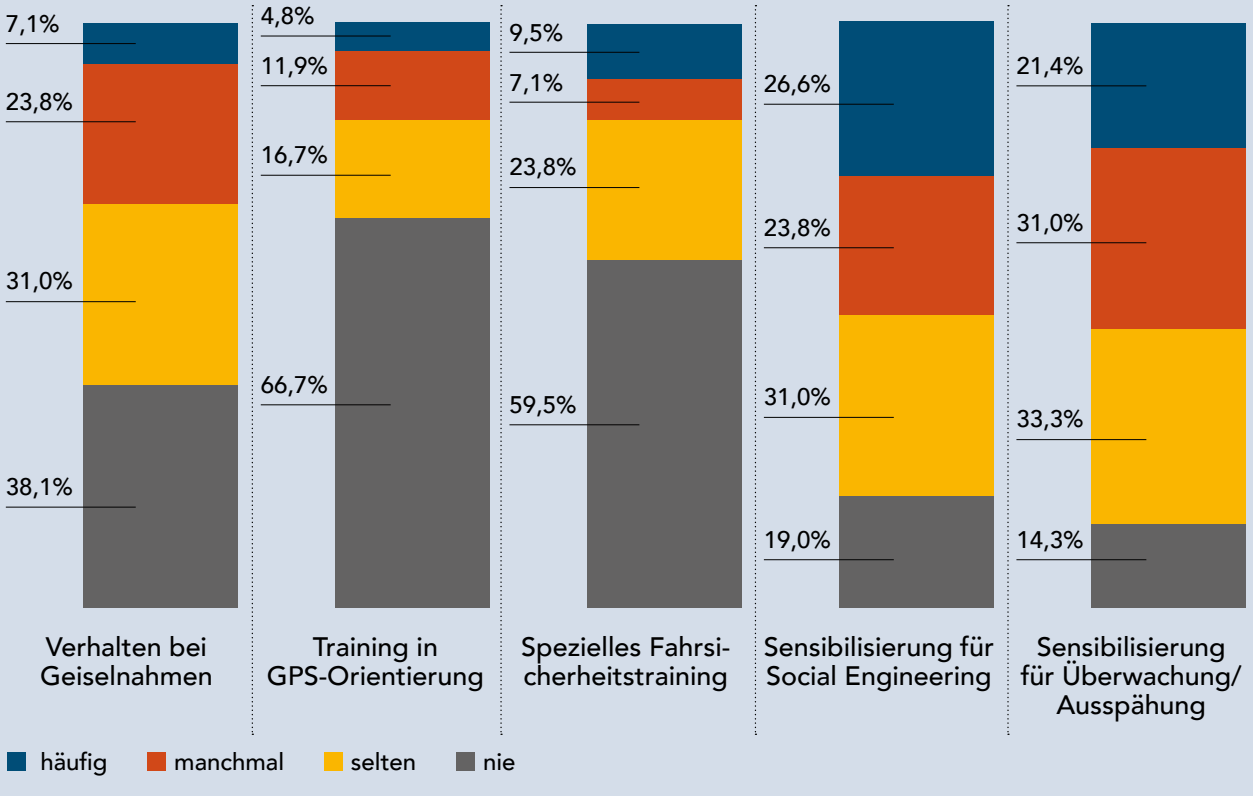


Abbildung 23: Sicherheitsrelevante Vorbereitungsmaßnahmen für Expatriates (n=36, in %)

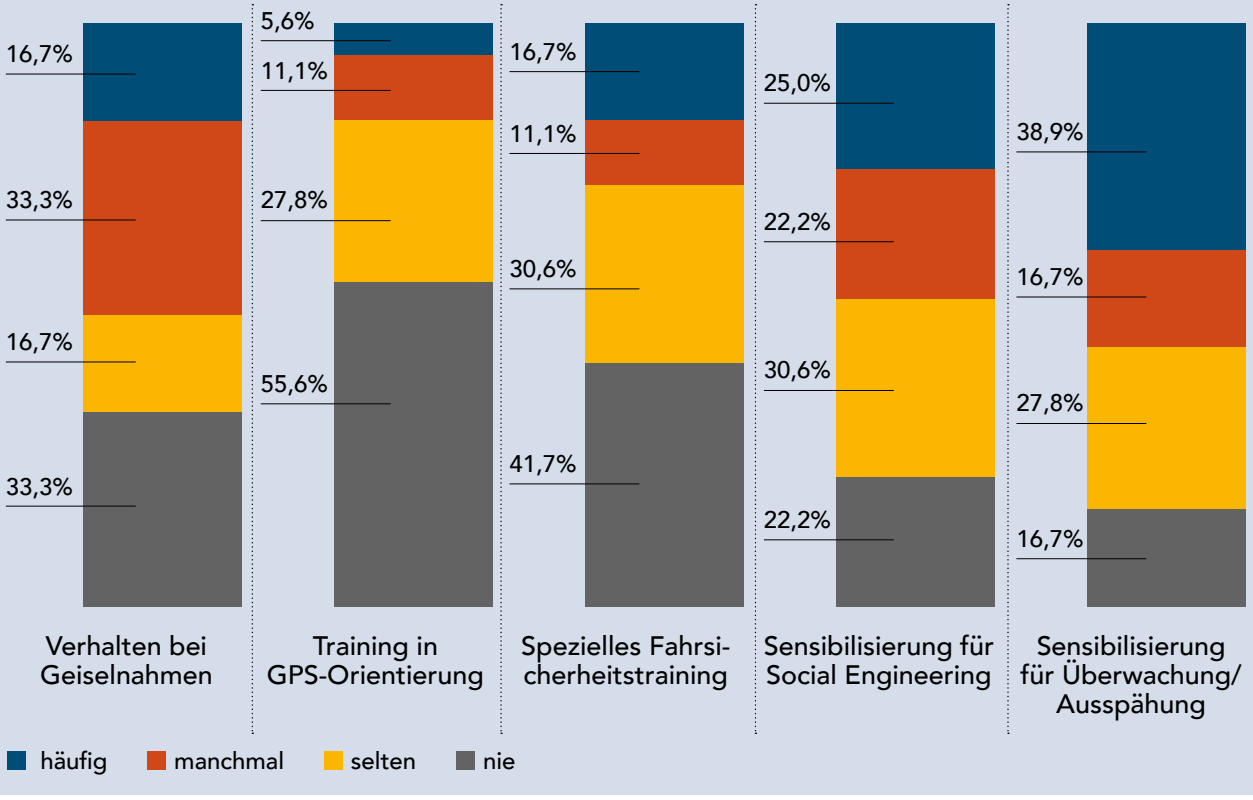


Tabelle 13: Dauer der sicherheitsrelevanten Maßnahmen

	keine Vorbereitung	< ½ Tag	½ bis 1 Tag	mind. 1 Tag	1 bis 3 Tage
Auslandsreisende	12,2 %	58,5 %	22,0 %	2,4 %	4,9 %
Expatriates	8,3 %	25,0 %	36,1 %	22,2 %	8,3 %

Bei den Expatriates korreliert die Häufigkeit der Durchführung aller Maßnahmen signifikant positiv mit der Dauer der Vorbereitungsmaßnahmen. Dies gilt auch für die Auslandsreisenden – abgesehen von der detaillierten Einweisung in den jeweiligen Aufenthaltsstandort/Aufenthaltsort.

Die jeweiligen Unterweisungen und Trainings werden in 38,5 % der Unternehmen als Einzeltrainings durchgeführt, in 20,5 % als Gruppentrainings. 41 % der Befragten geben an, dass in ihren Unternehmen diese Trainings in einer Kombination von Einzel- und Gruppentrainings angeboten werden.

Gesundheitsrelevante Vorbereitungs- bzw. Vorsorgemaßnahmen werden im überwiegenden Teil der Unternehmen vor einem Aufenthalt in „high risk regions“ durchgeführt. Dies gilt insbesondere für einen Gesundheitscheck, bei dem auch der Impfstatus geprüft wird. Auch eine arbeitsmedizinische Untersuchung nach dem Grundsatz G 35 der Deutschen Gesetzlichen Unfallversicherung für einen „Arbeitsaufenthalt im Ausland unter besonderen klimatischen oder gesundheitlichen Belastungen“ steht bei vielen Unternehmen auf der Agenda.

Abbildung 24: Gesundheitsrelevante Vorbereitungsmaßnahmen für Auslandsreisende (n=40, in %)

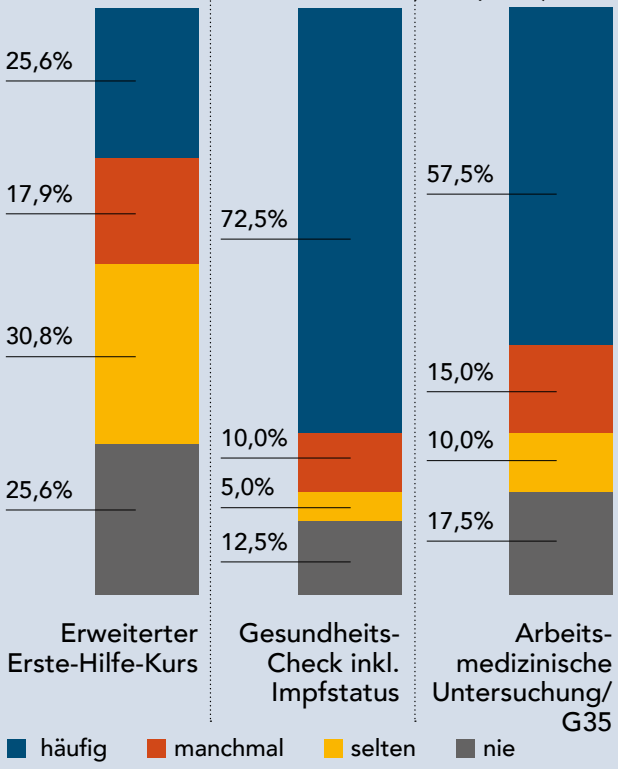


Abbildung 25: Gesundheitsrelevante Vorbereitungsmaßnahmen für Expatriates (n=33, in %)

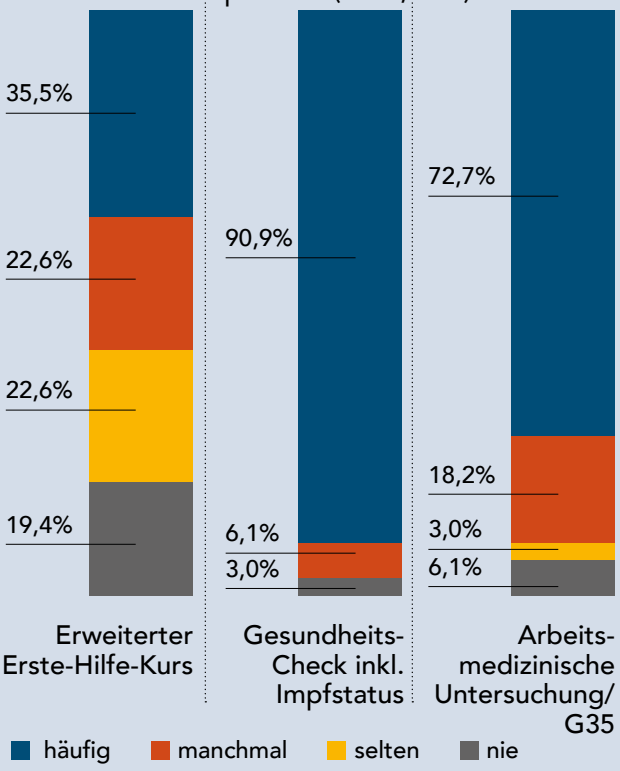


Tabelle 14: Vorbereitungsmaßnahmen für mitreisende (Ehe-)PartnerInnen

	keine	gesundheits-relevante Aspekte	ausgewählte sicherheits-relevante Unterrichtungen	alle sicherheits-relevanten Unterrichtungen
Angebote für (Ehe-)PartnerInnen	17,9 %	46,2 %	30,8 %	28,2 %

Diese gesundheitsrelevanten Maßnahmen werden in 46,2 % der Unternehmen auch den mitreisenden (Ehe-)PartnerInnen angeboten. Bei den sicherheitsrelevanten Maßnahmen ist der Anteil deutlich niedriger.

5.6 Maßnahmen während der Anreise oder des Aufenthalts

Abschließend zu diesem Themenfeld wurden Angaben dazu erhoben, inwiefern bestimmte Maßnahmen während der Anreise in das Zielland oder während des Aufenthalts durch das Unternehmen erfolgen.

Unter den oben angeführten Sicherheitsmaßnahmen wird die 24/7-Hotline am häufigsten angeführt, gefolgt von Tracking/Datenerfassung während der Anreise und Ankunft. Stichprobenartiges oder Echtzeit-Tracking wird dagegen zwar weniger häufig eingesetzt, hat aber im Bedarfsfall in fast der Hälfte der Unternehmen dennoch eine besondere Bedeutung.

Als wesentlich werden zudem aktuelle Informationen zur Sicherheitslage erachtet – insbesondere bei negativen Ereignissen oder einer problematischen Entwicklung. Weitere spezifische Sicherheitsmaßnahmen, die nachfolgend abgebildet sind, werden nicht in allen Unternehmen in dieser Häufigkeit durchgeführt.

Ein deutlicher Unterschied zwischen den Angeboten für Auslandsreisende und Expatriates ist nicht ersichtlich. Dies verwundert nicht, da sich die Maßnahmen weniger am Status, sondern primär am eingeschätzten Risiko orientieren.

Abbildung 26: Maßnahmen während Anreise und Aufenthalt für Auslandsreisende (n=39, in %)

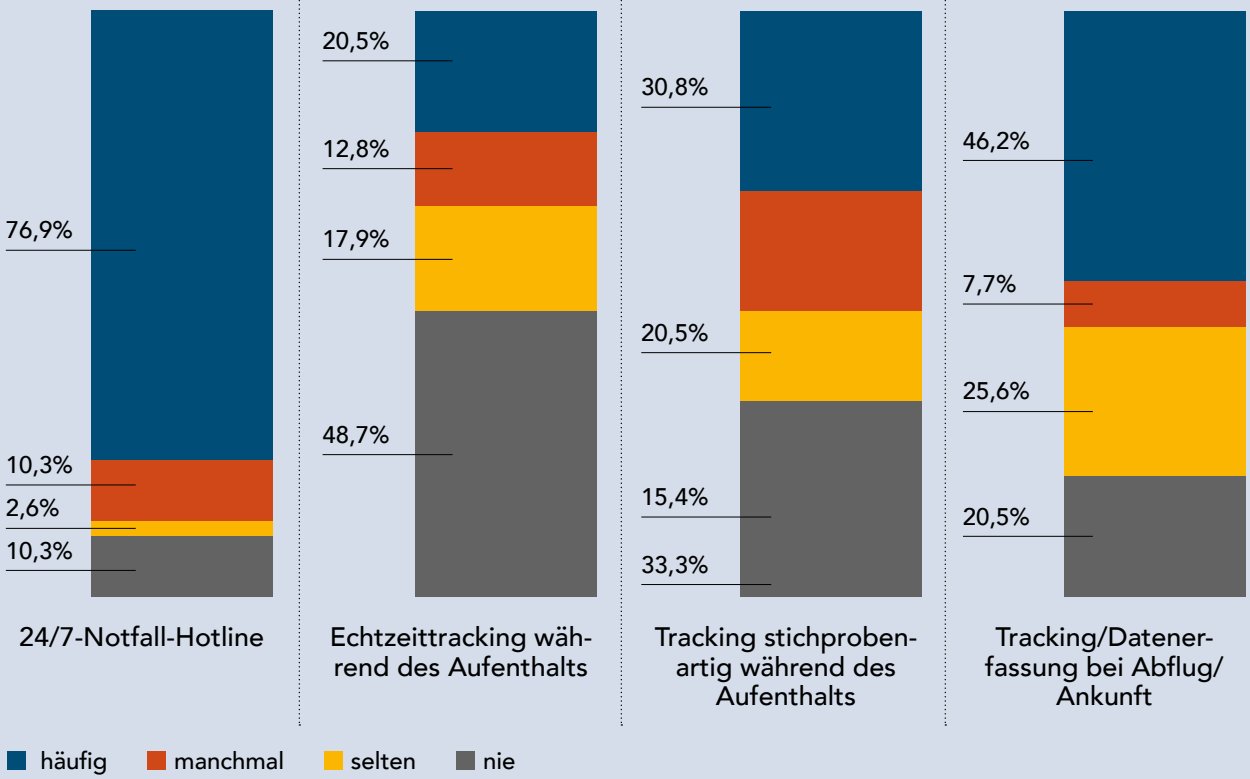


Abbildung 27: Maßnahmen während Anreise und Aufenthalt für Expatriates (n=32, in %)

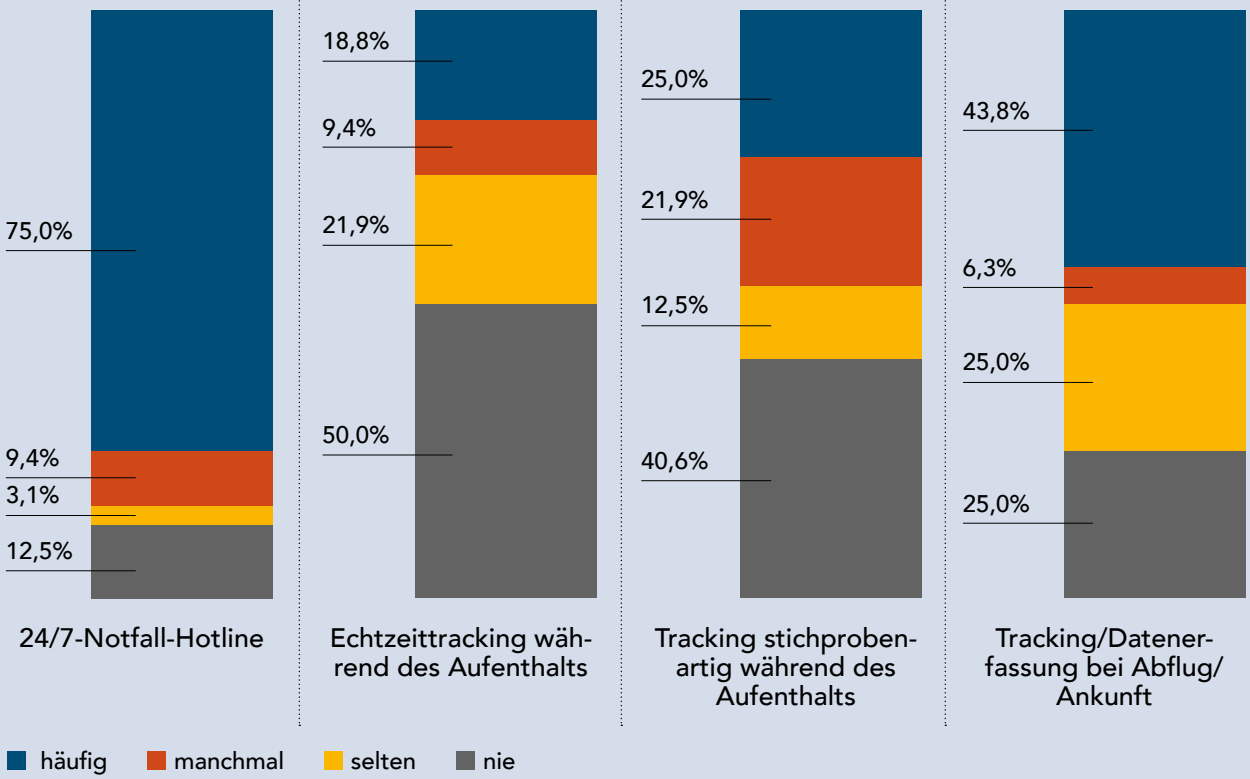


Abbildung 28: Maßnahmen während Anreise und Aufenthalt für Auslandsreisende (n=39, in %)

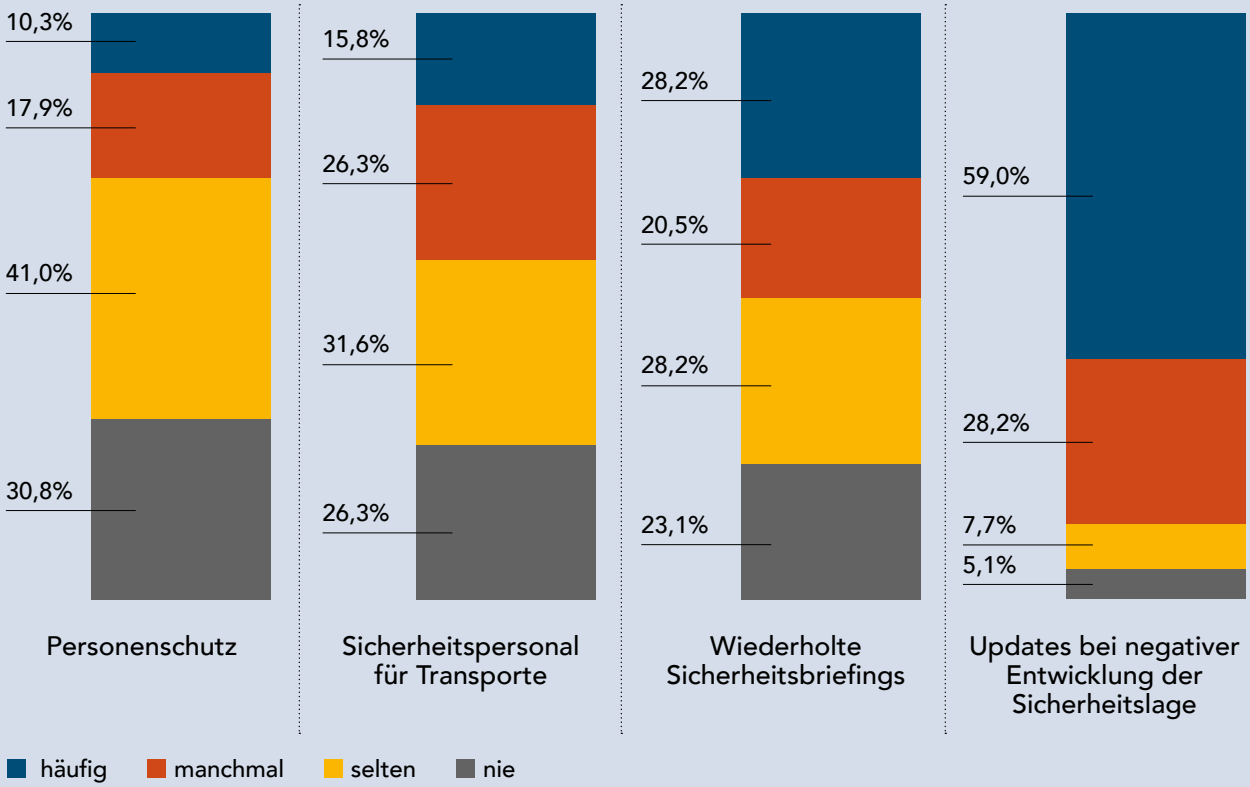
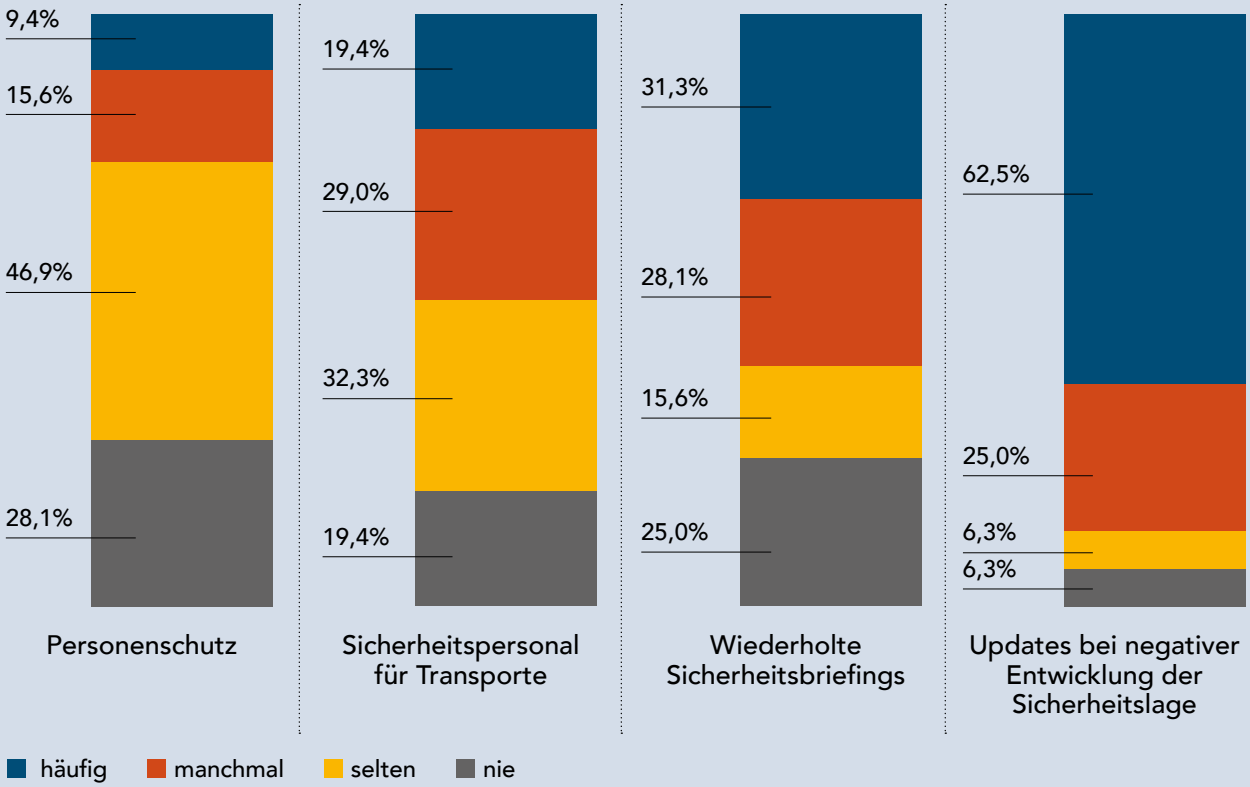


Abbildung 29: Maßnahmen während Anreise und Aufenthalt für Expatriates (n=32, in %)



6. Abschluss und Ausblick

6.1. Methodenkritische Anmerkungen

Wie bereits am Anfang des Berichts angemerkt haben die Befunde angesichts der geringen Größe der Stichprobe primär heuristischen Charakter. Insbesondere im Hinblick auf den Themenschwerpunkt „Sicherheit im Ausland“ ging es in der vorliegenden Untersuchung in erster Linie nicht darum, einen allgemeinen Überblick über die Struktur, das Ausmaß und die sicherheitsrelevanten Maßnahmen von Unternehmen abzubilden, sondern beispielhafte Erkenntnisse von good practice zu präsentieren. Das Transparentmachen des Vorgehens großer Wirtschaftsunternehmen, die im Ausland und insbesondere in „high-risk-regions“ aktiv sind, soll anderen Unternehmen Ansatzpunkte bieten, die eigenen Maßnahmen und Strategien zu reflektieren. In diesem Sinne hoffen wir, mit dem Bericht zu einer Diskussion und zu einer etwaigen Implementierung oder Optimierung von Maßnahmen und Prozessen in anderen Unternehmen beizutragen.

6.2. Diskussion einzelner Befunde

Arbeitszufriedenheit und Wertschätzung 2014 und 2017
Wie in der Studie von 2014 kann auch 2017 eine relativ hoch ausgeprägte Zufriedenheit der Befragten konstatiert werden, insbesondere im Hinblick auf die eigene Position und die wahrgenommene Unterstützung durch den Vorstand. Gleichwohl fühlen sich auch im Jahr 2017 46,6 % der Sicherheitsverantwortlichen (eher) nicht als Bestandteil des Unternehmenserfolgs angesehen (2014: 46,3 %).

Sicherheitsverantwortliche werden auch heute in vielen Fällen noch immer nicht als Prozessoptimierer oder „Business Enabler“ angesehen. Die Unternehmen würden mit einer Veränderung dieser Perspektive und mit zunehmender Wertschätzung einen positiven Effekt erzielen – im Hinblick auf die (Arbeits-)Zufriedenheit der Sicherheitsverantwortlichen und damit letztlich auch auf deren Leistungsbereitschaft und -fähigkeit.

Kriminalitätsbelastung - Betroffenheit der Unternehmen
Die Prävalenzraten zeigen, in welchem Maße die befragten Unternehmen insgesamt sowie auch und insbesondere diejenigen mit Konzernsicherheitsabteilungen von Delikten betroffen sind.

Ein besonders erklärungsbedürftiges Phänomen stellt die erhebliche Zunahme bei erpresserischem Menschenraub/Geiselnahme dar. Es gibt wenige Anhaltspunkte, weitere Erkenntnisse oder gesicherte Informationen für einen Anstieg von – im Ernstfall länger andauernden – Entführungen oder Geiselnahmen. Es kann mit Erdweg (2016/2017) die Hypothese aufgestellt werden, dass dieses erhöhte Fallaufkommen auf Express Kidnapping zurückzuführen ist, d.h. auf die „kurzfristige Entführung einer oder mehrerer Personen mit dem Ziel, in einem äußerst kurzen Zeitraum das Maximum an Werten“ (Leidel 2007) zu erlangen. Um diese Frage abschließend zu klären, bedarf es weiterer zielgerichteter Studien.

Sicherheit im Ausland
Ein Dokument zur Reisesicherheit, das Maßnahmen umschreibt und den Prozess der Risikobewertung abbildet, liegt in ca. 40 % der befragten Unternehmen mit Auslandsaktivitäten nicht vor. Erdweg (2016/2017) konstatiert, dass es für einen Konzern wesentlich sein sollte, zumindest ein einheitliches Grundverständnis zu haben, was Reisesicherheit bedeutet und welche Komponenten und Schnittstellen hierbei wichtig sind (Betriebsarzt, Expat Management, Travel Management, Human Resources, Versicherungen etc.).

Es geben rund 70 % der Unternehmen an, über ein Klassifikationssystem für die Einstufung der Länder bzw. Landesteile in „low, medium, high or extreme risk“ zu verfügen. Wird allerdings keine Einschätzung vorgenommen bzw. für alle Standorte vorgegeben und wird die Bewertung von Risiken nicht einheitlich geregelt, gibt Erdweg (2016/2017) zu bedenken, dass Teile eines Konzerns, die z.B. in Pakistan ansässig sind, das Risiko in einem Dritt-

land eventuell deutlich anders bewerten, als Teile, die in den USA ansässig sind.

Im Hinblick auf krisenhafte Entwicklungen in einem Land und potentielle Evakuierungen, haben 80 % der befragten Unternehmen mit Auslandsaktivitäten Indikatoren festgelegt, die für die Entscheidung zur Evakuierung besondere Relevanz haben. Notfall- und Evakuierungspläne sollten aber vorhanden und entsprechende Maßnahmen implementiert sein, da auch im Falle von vertraglich vereinbarten Evakuierungsleistungen externer Sicherheitsdienstleister diese häufig nur eine Evakuierung vom nächsten internationalen Flughafen anbieten (Erdweg 2016/2017).

Dieser Abschnitt soll dazu dienen, die Ergebnisse in den Kontext anderer Untersuchungen einzuordnen. Einerseits werden hier Umfragen zur konkreten Kriminalitätsbelastung, andererseits solche zur Einschätzung von Herausforderungen und Risiken kurz vorgestellt.

In der in Deutschland durchgeführten Studie zur „Wirtschaftskriminalität in der analogen und digitalen Wirtschaft" verzeichnet PwC einen Anstieg gegenüber 2013: 51 % der Unternehmen gaben an, von Wirtschaftskriminalität betroffen gewesen zu sein. Vermögensdelikte führen mit 37 % die Liste an, gefolgt von Verstößen gegen Patent- und Markenrechte (13 %), Diebstahl vertraulicher Kunden- und Unternehmensdaten und Geldwäsche (je 5 %), Industrie- und Wirtschaftsspionage mit 3 % und Falschbilanzierung mit 2 %. Die Zahl der Verdachtsfälle hat sich grundsätzlich gleichartig entwickelt, liegt aber bei Geldwäsche, Spionage und Datendiebstahl erheblich höher.

34 % der Unternehmen gaben an, von „E-Crime" (also Kriminalität unter gezielter Ausnutzung elektronischer Systeme und Kommunikationsmittel) betroffen gewesen zu sein. Bei forschungsintensiven Unternehmen gehen 70 % von einem höheren E-Crime-Risiko infolge von Industrie 4.0 aus (48 % der Unternehmen ohne bzw. mit geringer Forschung).

Die weltweite Untersuchung „Global State of Information Security" von PwC beschäftigt sich spezifisch mit Informationssicherheit, die durch die Entwicklungen hin zu einem „Internet of Things" (IOT) immer bedeutender wird. IOT-spezifische Sicherheitsstrategien können sich als Herkulesaufgabe herausstellen: Nur 35 % der befragten Unternehmen erheben die Kommunikation der Geräte und Systeme in ihrer Geschäftsumgebung und wissen über mögliche Verwundbarkeiten Bescheid. Beim Zugang zu den Ressourcen eines Unternehmens (insb. Daten) wird künftig Identity-and-Access-Management als kritische Fähigkeit eingeschätzt.

Eine Umfrage von Deloitte unter Führungskräften zu aktuellen Herausforderungen (Director 360) liefert ebenfalls einen Ländervergleich. Im Themenfeld Corporate Governance zählen in Österreich Risikomanagement und Cybersicherheit, in Deutschland Digitalisierung generell sowie Cybersicherheit und in der Schweiz ebenfalls Cybersicherheit zu den Prioritäten.

Im Allianz Risk Barometer identifiziert der Versicherungskonzern die wichtigsten Risiken für Unternehmen in den einzelnen Ländern. Betriebsunterbrechungen können unterschiedliche Auslöser haben; dabei werden die Nicht-Sachschaden-Ereignisse wichtiger. In Deutschland werden Cybervorfälle als Top-Risiko für Unternehmen genannt vor Betriebsunterbrechung generell und Marktentwicklungen. Für die Schweiz identifiziert die Allianz Betriebsunterbrechung als wichtigstes Risiko vor Marktentwicklungen und Cybervorfällen. In Österreich gelten Betriebsunterbrechungen, Cybervorfälle und Naturkatastrophen als die drei Top-Risiken.

6.3Fazit Hohe Bedeutung der CSO für den Unternehmenserfolg

CSO TOP 100 liefert durch den Fokus auf eine sehr spezifische Zielgruppe einen Überblick über die Arbeitsweise der führenden Unternehmen der Länder in der D-A-CH-Region. Vor allem die Verknüpfung der Informationen zwischen internen Organisationsfragen (Policy, Awareness, Systeme), der Belastung der Unternehmen durch kriminelle Vorfälle und dem Umgang damit liefert Ergebnisse, die in dieser Form einzigartig sind. In Bezug auf die Kriminalitätsbelastung ist auch der Hinweis auf das (wahrscheinlich erhebliche) Dunkelfeld zu nennen, das von anderen Umfragen nicht umfasst wird. Dies kann vor allem an der Auswahl der Befragten liegen: Während andere Studien auf die Geschäftsleitung (Board, Vorstand, Geschäftsführung) abzielen, wurden für CSO TOP 100 die Chief Security Officers direkt befragt.

Dabei zeigt sich, dass vor allem in Österreich deutlich mehr Unternehmen über eine eigene Konzernsicherheitsabteilung verfügen als 2014 (mittlerweile nahezu 6 von 10). Die Unternehmen aus Deutschland und der Schweiz sind nahezu unverändert strukturiert (8 von 10 bzw. rund zwei Drittel haben eine Konzernsicherheitsabteilung). Die Zuständigkeit für Risikomanagement steigt an; auch Weisungsbefugnisse sind bereits weit verbreitet. Höhere Budgets und mehr Arbeitszufriedenheit führen dazu, dass die Arbeit als Sicherheitsverantwortliche/r in Konzernen auch künftig ein interessantes Tätigkeitsfeld bleibt. Die Bedeutung der Sicherheitsverantwortlichen für den Unternehmenserfolg scheint dennoch weiterhin unterschätzt zu werden.

Das ebenfalls hier zum ersten Mal vorgestellte Fokusthema Sicherheit im Ausland wurde bisher in keiner relevanten Studie, die einerseits eine derartig umfassende Beschreibung der Praxis, andererseits einen Vergleich der Länder der D-A-CH Region bietet, behandelt. Dieses Aufgabenfeld für CSOs wird in der globalisierten Wirtschaft weiter an Bedeutung gewinnen und verdient daher auch mehr wissenschaftliche Beachtung.

Literaturverzeichnis

Allianz (2017). Allianz Risk Barometer. Die 10 wichtigsten Geschäftsrisiken 2017.
Allianz Global Corporate & Specialty SE, München

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.

Deloitte (2016). EMEA 360 Boardroom survey.
Agenda priorities across the region. Deloitte University EMEA CVBA,

Erdweg, St. (2016/2017). Sicherheit im Ausland – Diskussion von Fragestellung und Erkenntnissen.
Juli 2016 – September 2017. HfÖV Bremen.

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.

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

Leidel, S. (2007). Express Kidnappings in Südamerika.
www.sicherheitsmelder.de

PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft AG und Martin Luther Universität Halle-Wittenberg:
Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016, 2016. Halle-Wittenberg.

PwC (2017). Uncovering the Potential of the Internet of Things.
Key Findings from The Global State of Information Security® Survey 2017.

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

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. Mag.a Claudia Körmer lehrt und forscht seit 2014 im Fachbereich Risiko- und Sicherheitsmanagement der FH Campus Wien. In dieser Position war sie bereits für Studienprojekte wie z. B. „Konzernsicherheit in der D-A-CH Region 2016“ und „Wirtschafts- und Industriespionage in österreichischen Unternehmen 2015“ verantwortlich. Die Absolventin der Universität Wien (Soziologie und Philosophie) war davor als Projektleiterin im Kuratorium für Verkehrssicherheit tätig.

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

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

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

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

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

HfÖV
Hochschule für
Öffentliche Verwaltung Bremen