KPMG
cutting through complexity

Ergebnispapier

GOVERNANCE & ASSURANCE SERVICES

Ausgestaltung von Security Management-Systemen

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

INHALT

1 DESIGN DER STUDIE 4

1.1 Überblick 4

1.2 Ausgestaltung eines Security Management-Systems gemäß IDW PS 980 5

2 MANAGEMENT SUMMARY 6

3 ERGEBNISSE DER STUDIE 8

3.1 Mandatierung und Bedeutung im Unternehmen 8

3.2 Schnittstellen- und Expertenfunktionen 9

3.3 Konzernweite Sicherheitsorganisation und definierte Verantwortungsbereiche 10

3.4 Security-Risiken – Wesentliche Studienergebnisse 11

3.4.1 Identifizierung, Bewertung und Akzeptanz von Risiken 12

3.4.2 Risikobereiche 13

3.5 Security-Programm – Wesentliche Studienergebnisse 14

3.5.1 Schwerpunkte 15

3.5.2 Access Control 17

3.5.3 Physical/Technical Security 18

3.5.4 Travel Security 19

3.5.5 Information Security 20

3.5.6 Crisis Management 21

3.5.7 Investigations 22

3.5.8 Protective Intelligence 23

3.6 Unsere Empfehlungen 24

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

1 DESIGN DER STUDIE

1.1 Überblick

Naturkatastrophen, verschärfter Wettbewerb, Marktschwankungen, Datenflut, Internetkriminalität – Unternehmen sind heute zahlreichen internen und externen Risiken ausgesetzt. Um diesen vorzubeugen und potenzielle – schlimmstenfalls sogar existenzgefährdende – Fallstricke zu vermeiden, empfiehlt sich die Entwicklung und Implementierung eines nachhaltigen Sicherheitskonzepts, das sowohl aktuelle Gesetze, Sorgfalts- und Überwachungspflichten und ISO-Standards als auch interne Richtlinien, Prozesse und Maßnahmen berücksichtigt.

Um herauszufinden, welche Risiken für die Unternehmen besonders im Fokus stehen und wie sie den zahlreichen Gefährdungen begegnen, haben wir eine Studie zum aktuellen Stand der Ausgestaltung von Security Management-Systemen durchgeführt. Hierfür wurden Security-Verantwortliche aus wesentlichen Wirtschaftsbranchen – unter anderem aus den Sektoren Versicherung, Luftfahrt, Nahrungsmittel und Industrie – befragt. Die Erhebung erfolgte anhand eines strukturierten, teilstandardisierten Fragebogens mit 21 Fragen. Alle Informationen wurden anonymisiert und unter Beachtung hoher Datenschutzanforderungen ausgewertet.

Wie die Untersuchung zeigt, messen die Befragten dem Thema Sicherheit insgesamt hohe Bedeutung bei und haben größtenteils entsprechende Verfahren im Unternehmen implementiert. Der überwiegende Teil von ihnen hat eine explizite Mandatierung der Sicherheitsprozesse vorgenommen und den Risk Owner definiert. Das Hauptaugenmerk liegt dabei insbesondere auf den Bereichen Access Control, Informationssicherheit sowie physische Sicherheit.

Auf den folgenden Seiten stellen wir Ihnen die Kernergebnisse der Befragung vor. Wir freuen uns darauf, diese mit Ihnen zu diskutieren.

Vorteile durch externes Benchmarking

Um die Wirksamkeit eines Security Management-Systems sicherzustellen, kann neben der Einrichtung interner Maßnahmen auch ein externes Benchmarking hilfreich sein. So dient es beispielsweise als Orientierungshilfe hinsichtlich gängiger Marktpraktiken, trägt zur angemessenen Information im Sinne der Business Judgement Rule (§ 93 Abs. 1 AktG) bei und unterstützt bei der effektiven Ausgestaltung des Security Management-Systems. Zugleich liefert der Vergleich mit anderen Unternehmen Anhaltspunkte für Verbesserungen und unterstützt bei der Identifikation von Optimierungspotenzialen.

Gerne nehmen wir eine individuelle Einordnung Ihres Unternehmens in einem für Sie relevanten Benchmark vor. Sprechen Sie uns an.

Komplexe Sicherheitsrisiken

Ein Sicherheitsereignis tritt in den meisten Fällen unerwartet ein. Dann ist schnelles, durchdachtes und zielgerichtetes Handeln gefragt. Wenn sich die Unternehmensleitung in solchen Situationen nicht auf ein erprobtes und höchsten Sicherheitsstandards entsprechendes Krisenmanagement verlassen kann, sind unter Umständen Leben und Gesundheit der Mitarbeiter sowie die Anlagen und Vermögensgegenstände des Unternehmens akut gefährdet.

Zusätzlich kann ungewollter Informationsabfluss zur existenziellen Gefährdung der Wettbewerbsfähigkeit eines Unternehmens führen. Vor allem innovative Unternehmen sind hier besonders großen Risiken ausgesetzt. Den vielfältigen Gefahren durch illoyale Mitarbeiter, kriminelle Organisationen oder fremde Nachrichtendienste lässt sich nicht mit Einzelmaßnahmen begegnen.

Auch die Erzielung der Reisesicherheit für Mitarbeiter und Entsandte (Expatriates) wird in Zeiten globaler Geschäftstätigkeit zunehmend komplexer. Für die Unternehmensleitung bedeutet dies ein hohes Maß an Verantwortung für das Leben und die Gesundheit ihrer Mitarbeiter.

Risken erkennen und bewältigen

Um bereits präventiv sicherheitsrelevanten Risiken vorzubeugen und das mögliche Schadensausmaß zu kontrollieren, gilt es Gesetze, interne Richtlinien, Prozesse, Maßnahmen und Standards einzuhalten. Darüber hinaus können so auch potenzielle Reputations-, Haftungs- und Bußgeldrisiken reduziert werden. Die Implementierung eines Security Management-Systems trägt wesentlich dazu bei,

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

ein Unternehmensumfeld zu schaffen, in dem Risiken laufend erfasst, systematisiert und bewertet sowie risikoreduzierende Maßnahmen implementiert werden.

Bescheinigung nach IDW PS 980

Grundlage für die Prüfung und Bewertung eines Management-Systems ist der Prüfungsstandard IDW PS 980 des Instituts der Wirtschaftsprüfer (IDW). Dieser definiert die Grundsätze ordnungsgemäßer Prüfung von Compliance Management-Systemen. In analoger Anwendung des IDW PS 980 können auf dieser Grundlage auch die Konzeption, Angemessenheit und Implementierung sowie die Wirksamkeit eines Management-Systems von Wirtschaftsprüfern bestätigt werden.

1.2 Ausgestaltung eines Security Management-Systems gemäß IDW PS 980

Security-Überwachung und -Verbesserung

- Kontinuierliche Überwachung der Sicherheitsprozesse sowie Incident Reporting und Evaluation von unternehmensspezifischen Standards

Security-Kultur

- Förderung des Sicherheitsbewusstseins der Mitarbeiter und Akzeptanz der internen und externen Sicherheitsvorgaben

Security-Ziele

- Definierte Sicherheitsziele auf Grundlage der allgemeinen Unternehmensziele

Security Management-System

Security-Programm

- Maßnahmen und Prozesse zur Reduzierung der identifizierten Sicherheitsrisiken

Security-Risiken

- Prozess zum Verfahren der Risikoerkennung und -berichterstattung relevanter Sicherheitsbereiche

Security-Kommunikation

- Definierte Berichtswege für Sicherheitsrisiken sowie sicherheitsrelevante Schulungen und Sensibilisierungsmaßnahmen

Security-Organisation

- Definition der unternehmensweiten Aufbau- und Ablauforganisation von Sicherheitsmaßnahmen

© 2015 KPMG, Deutschland

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

2 MANAGEMENT SUMMARY

Das vorliegende KPMG-Ergebnispapier informiert über den aktuellen Stand der Ausgestaltung von Security Management-Systemen. Nachfolgend finden Sie einen Überblick über die wesentlichen Umfrageergebnisse.

- Die Befragung zeigt, dass 70 Prozent der Unternehmen über eine explizite **Mandatierung** ihrer Sicherheitsprozesse verfügen.
- Etwa zwei Drittel der Befragten (70 Prozent) definieren den **Risk Owner**, das heißt den Träger der Hauptverantwortung für ein identifiziertes Risiko.
- Die Hälfte der Unternehmen definiert **Kriterien zur Akzeptanz eines Risikoniveaus**.

Allgemeine Entwicklungen

- Die befragten Unternehmen legen ihren Fokus insbesondere auf die folgenden Sicherheitsbereiche: **Zugangskontrolle** (68 Prozent), **Informationssicherheit** (63 Prozent), **Krisenmanagement** (54 Prozent) sowie **physische Sicherheit** (52 Prozent).

Security-Programm

- Hinsichtlich der Themenfelder **Reisesicherheit** und **Ermittlungen** sieht etwa die Hälfte der Befragten Optimierungsbedarf (jeweils 48 Prozent).
- Mehr als jedes dritte Unternehmen verfügt über Maßnahmen zur präventiven Früherkennung von Sicherheitsrisiken: 39 Prozent der Befragten geben an, in Bezug auf **Protective Intelligence** aktiv zu sein.

© 2015 KPMG, Deutschland

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

3 ERGEBNISSE DER STUDIE

3.1 Mandatierung und Bedeutung im Unternehmen

Die Befragung zeigt, dass das Thema Security-Management insgesamt einen hohen Stellenwert für die mittlere Führungs- sowie für die Leitungsebene hat.

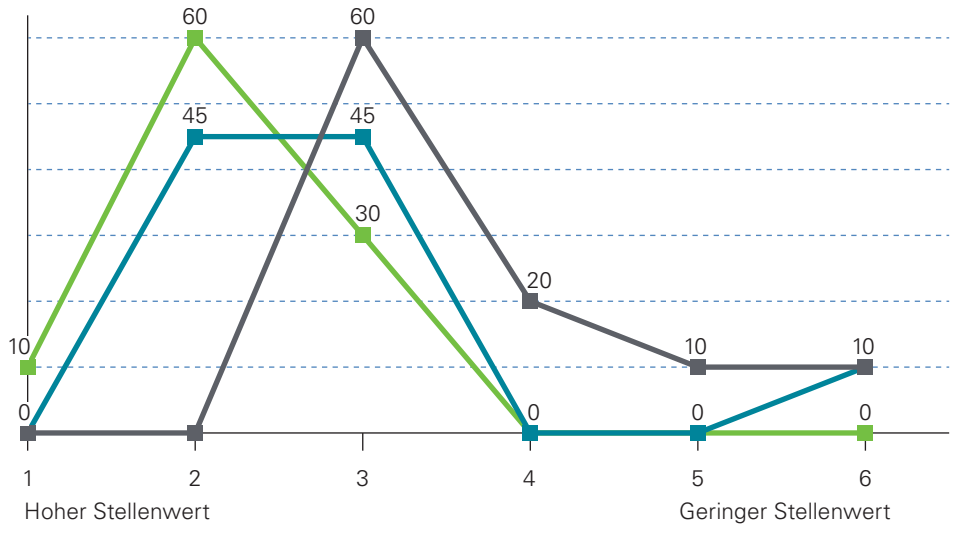
Er verringert sich bezogen auf die Gesamtheit aller Mitarbeiter – sie messen diesem Thema eher geringere Bedeutung bei.

„Inwiefern ist der Aufgabenbereich von Security bei Ihnen im Unternehmen explizit mandatiert? Wie weit wird Sicherheit gefasst?“

Bei 30 Prozent der Unternehmen erfolgt keine explizite Mandatierung des Security-Aufgabenbereichs. Stattdessen wird dieser in der Regel über einzelne Prozesse oder Notfallpläne abgedeckt.

Abb. 1 Mit steigender Verantwortung erhöht sich der Stellenwert von Security-Management: Thema für Mehrheit der Unternehmensleitung und mittleren Führungsebene relevant

„Welchen Stellenwert hat das Security-Management nach Ihrer Einschätzung gegenwärtig in Ihrem Unternehmen?“



© 2015 KPMG, Deutschland

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.

3.2 Schnittstellen- und Expertenfunktionen

Für eine möglichst umfassende Einschätzung und Bewertung der Sicherheitsrisiken eines Unternehmens müssen verschiedenste Bereiche eingebunden werden. Im Rahmen der Studie wurde daher untersucht, welche internen und externen Partner die Befragten bei der Risikoevaluierung vorwiegend miteinbeziehen.

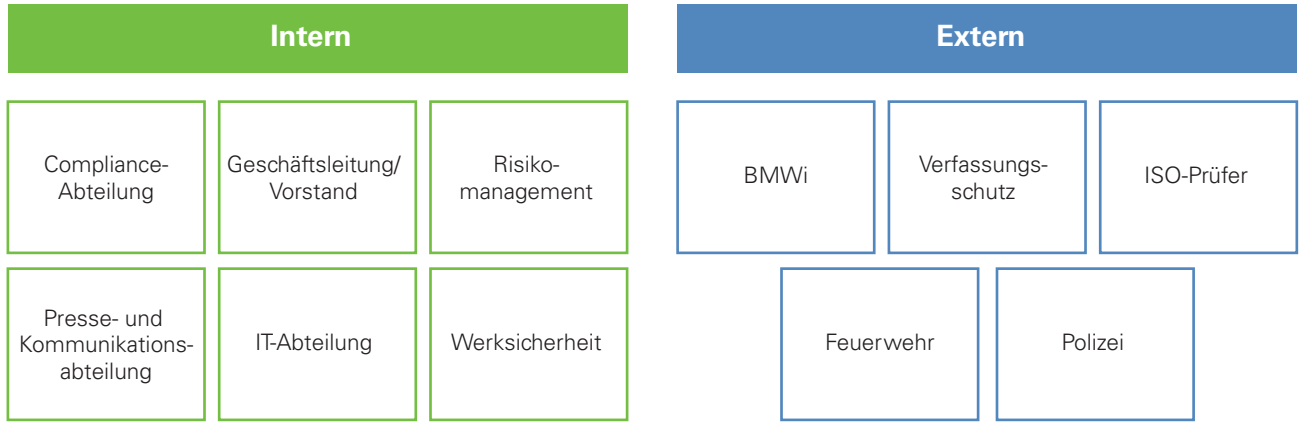
Da es sich bei der Konzernsicherheit/Sicherheitsabteilung um eine Querschnittsfunktion handelt, die für alle Mitarbeiter und eine Vielzahl von Unternehmensprozessen (etwa in der Forschung und Entwicklung, in der Produktion oder auch in der Außenkommunikation) Sicherheitsdienstleistungen erbringt, ist es umso wichtiger, eine umfassende, systemimmanente Betrachtung aller relevanten Risiken einzubeziehen. Nur daraus lassen sich, siehe IDW PS 980, wirksame Maßnahmen ableiten.

IDW PS 980

„Merkmal einer […] Organisation (ist) unter anderem die Bereitstellung von im Hinblick auf die […] Ziele und […] Risiken ausreichenden Ressourcen zur Konzeption, Einführung, Durchsetzung und Überwachung sowie kontinuierlichen Verbesserung des […] Management-Systems. (Tz. A18)“

Abb. 2 Fundierte Risikobewertung erfordert Einbindung sowohl unternehmensinterner als auch externer Expertise

„Bitte geben Sie an, welche Abteilungen beziehungsweise Fachleute Ihres Unternehmens oder gegebenenfalls externen Partner in der Risikoevaluation involviert sind.“



© 2015 KPMG, Deutschland

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.

3.3 Konzernweite Sicherheitsorganisation und definierte Verantwortungsbereiche

„Wie wird die Umsetzung der auf Konzernebene entwickelten Konzepte und Programme in den Tochtergesellschaften sichergestellt?“

Die meisten Befragten haben einen Prozess im Unternehmen implementiert, um die Umsetzung der Sicherheitskonzepte und -programme in den Tochtergesellschaften zu überwachen. Immerhin noch ein Fünftel der Befragten verfügt jedoch über keine diesbezüglichen Vorgehensweisen oder überträgt die Konzepte nicht auf die Tochtergesellschaften.

Bei denjenigen Unternehmen, die die Umsetzung der Sicherheitskonzepte in ihren Tochtergesellschaften kontrollieren, erfolgt dies mehrheitlich durch

- die Interne Revision,
- das Interne Kontrollsystem (IKS).

IDW PS 980

„Bei der […] Überwachung handelt es sich um Überwachungsmaßnahmen durch prozessunabhängige Stellen, zum Beispiel die Interne Revision. Die […] Überwachung zielt darauf ab, festzustellen, ob das […] Management-System unter Beachtung der angewandten […] Grundsätze angemessen ausgestaltet und wirksam ist. Dies beinhaltet auch, ob die prozessintegrierten Kontrollen (vgl. Tz. A17) wirksam sind. (Tz. A20)“

„Wird der Risk Owner der einzelnen Risiken bei Ihnen klar definiert? Inwieweit wird dabei darauf eingegangen, wer der Risk Owner und wer der Process Owner ist?“

Im ISO 27000:2014 wird der Risk Owner als die Person oder Einheit definiert, die die Autorität und die Verantwortung innehat, ein Risiko zu managen. Dabei handelt es sich üblicherweise um eine Person, die daran interessiert ist, ein Risiko zu mitigieren. Zugleich nimmt sie eine Position im Unternehmen ein, die es ihr ermöglicht, entsprechende Maßnahmen anzustoßen. Der Process Owner hingegen ist auf operativer Ebene verantwortlich für den Prozess.

Mehr als zwei Drittel der Befragten definieren einen Risk Owner. Lediglich 30 Prozent nehmen diesbezüglich keine Zuordnung vor. Jedes fünfte Unternehmen trennt nicht eindeutig zwischen Risk Owner und Process Owner.

IDW PS 980

„Festlegung der Berichtspflichten (Anlässe) und der Berichtswege für die Kommunikation von […] Risiken und festgestellten beziehungsweise vermuteten Regelverstößen. (Tz. A19)“

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.

3.4 Security-Risiken – Wesentliche Studienergebnisse

Aufbauend auf den wesentlichen Bestandteilen eines Security Management-Systems werden nachfolgend die verschiedenen Sicherheitsrisiken untersucht. Typische Bereiche, in denen für Unternehmen Sicherheitsrisiken auftreten können, und und entsprechende potenzielle Maßnahmen sind zum Beispiel:

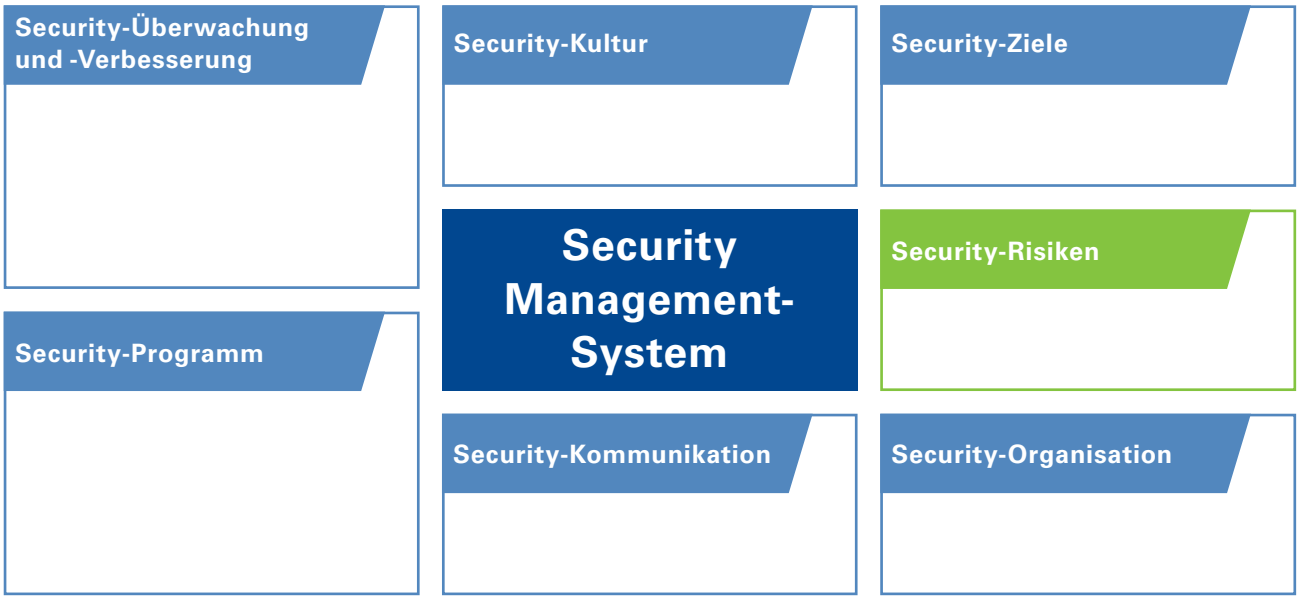
Personenschutz
Schutzkonzept zur Wahrung der Privatsphäre und der spürbaren Sicherheit

Informationsschutz und Spionageabwehr
Präventivkonzept zur Verhinderung ungewollten Informationsabflusses

Krisenmanagement
Maßnahmen zur Schadensbegrenzung vor und während Ereignissen, die das Unternehmen in seinem Bestand gefährden können

Reisesicherheit
Gewährleistung der schnellen Unterstützung von Mitarbeitern im Ausland (bei kritischen Ereignissen – von plötzlicher Erkrankung bis hin zu gewaltsamen Übergriffen)

Physische Sicherheit
Konzept zur Sicherung von Bürogebäuden und Produktionsstätten



© 2015 KPMG, Deutschland

IDW PS 980, Tz. 23

> Unter Berücksichtigung der […] Ziele werden die […] Risiken festgestellt, die Verstöße gegen einzuhaltende Regeln und damit eine Verfehlung der […] Ziele zur Folge haben können. Hierzu wird ein Verfahren zur systematischen Risikoerkennung und -berichterstattung eingeführt. Die festgestellten Risiken werden im Hinblick auf Eintrittswahrscheinlichkeit und mögliche Folgen analysiert.

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

3.4.1 Identifizierung, Bewertung und Akzeptanz von Risiken

„Inwieweit erfassen und bewerten Sie die Sicherheitsrisiken Ihres Unternehmens in einem standardisierten Verfahren?“

Die Befragung zeigt, dass bei den meisten Unternehmen standardisierte Verfahren eher die Ausnahme sind. Tendenziell lässt sich beobachten, dass ihr Umfang mit der Größe des Unternehmens zunimmt. Dabei werden die Verfahren sowohl anhand der Unternehmensrichtlinien als auch auf Grundlage externer Quellen festgelegt.

Viele Unternehmen beschränken sich lediglich auf die Erfassung der Risiken und nehmen diese einzelfallbezogen auf.

IDW PS 980

„Bei der Risikoanalyse werden die grundsätzlichen Entscheidungen der gesetzlichen Vertreter zur Risikosteuerung (Risikovermeidung, Risikoreduktion, Risikoüberwälzung oder Risikoakzeptanz) berücksichtigt. (Tz. A16)“

„Inwieweit existiert bei Ihnen ein Prozess, der Risk Acceptance definiert und dokumentiert?“

Die Hälfte der Unternehmen hat einen Prozess zur Definition und Dokumentation von Risk Acceptance eingerichtet.

Die übrigen 50 Prozent der Befragten nutzen einzelfallbezogene Prozesse oder wenden branchenspezifische Vorgehensweisen an.

In der Regel sind es vor allem Großunternehmen, die Prozesse zur Risk Acceptance in ihren Guidelines verankert haben.

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.

3.4.2 Risikobereiche

Um die Sicherheit des Unternehmens und der Mitarbeiter zu gewährleisten und den umfänglichen Security-Anforderungen zu entsprechen, ist es erforderlich, die wesentlichen Risikobereiche zu definieren und kontinuierlich zu überprüfen. Im Rahmen der Studie wurde daher untersucht, bei welchen Themen die Unternehmen diesbezüglich Schwerpunkte setzen.

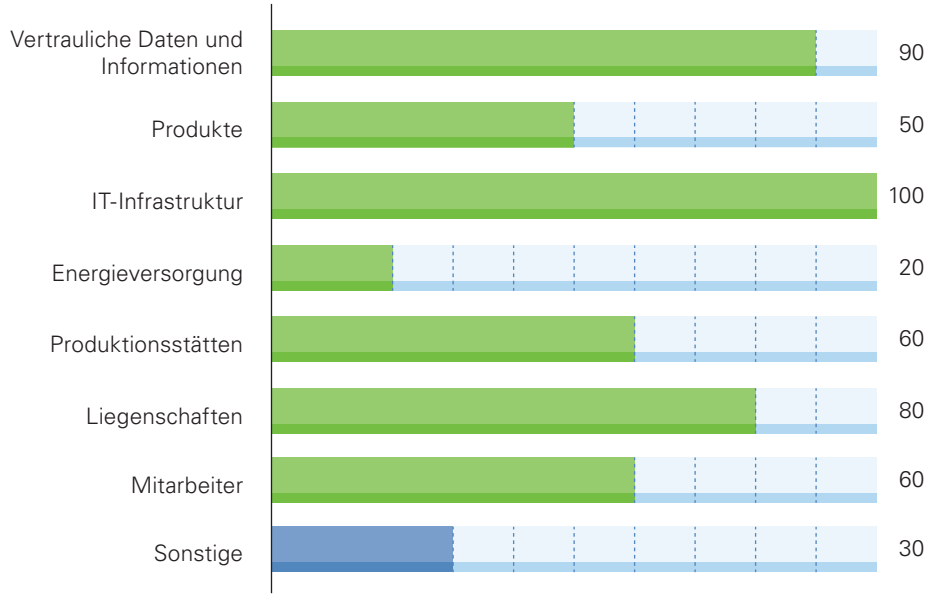
Dabei zeigte sich, dass die Befragten ihr Hauptaugenmerk auf IT-Sicherheit und Datenschutz legen – beide Bereiche werden von fast allen in ihrer Risikoanalyse berücksichtigt. Die Sicherheit ihrer Liegenschaften und Produktionsstätten sowie die physische Sicherheit ihrer Mitarbeiter steht bei mehr als der Hälfte der Unternehmen im Fokus. Weniger Aufmerksamkeit richten die Befragten auf eine sichere Energieversorgung: Sie ist lediglich bei einem Fünftel Bestandteil der Risikoanalyse.

IDW PS 980

„Unter Berücksichtigung der […] Ziele werden die […] Risiken festgestellt, die Verstöße gegen einzuhaltende Regeln und damit eine Verfehlung der […] Ziele zur Folge haben können. (Tz. 23)“

Abb. 3 Unternehmen messen IT-Sicherheit und Datenschutz hohe Bedeutung bei – beide Bereiche in fast allen Risikoanalysen enthalten

„Welche der folgenden Bereiche werden in der Risikoanalyse berücksichtigt?“



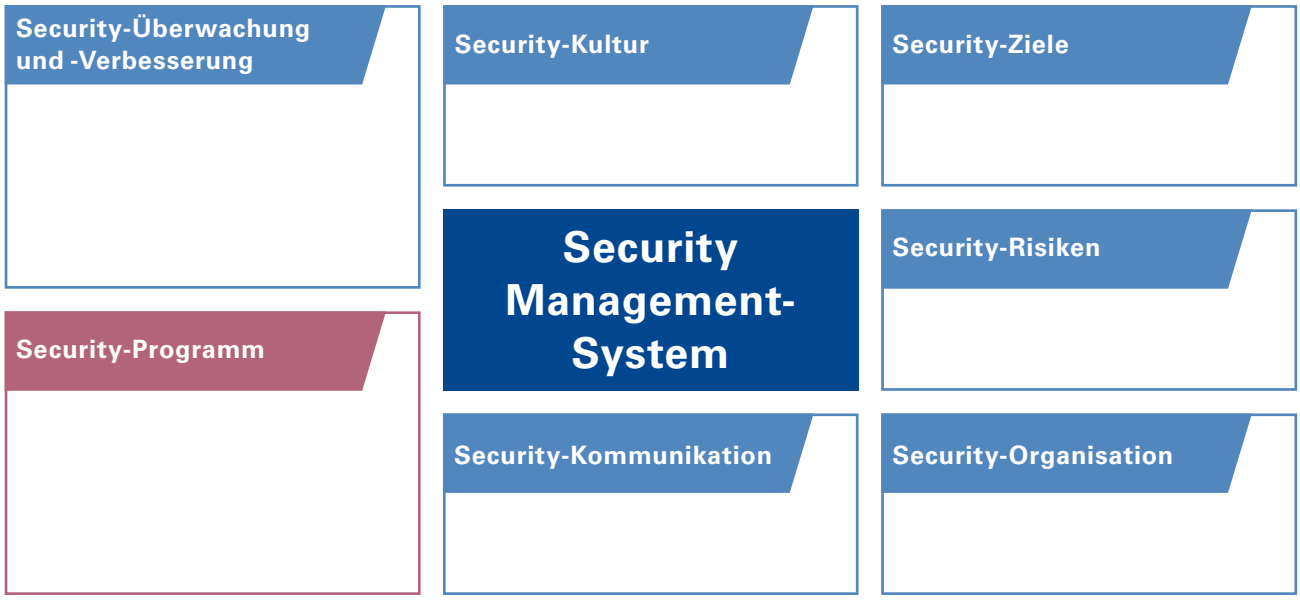
Mehrfachnennungen möglich, Angaben in Prozent

© 2015 KPMG, Deutschland

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.

3.5 Security-Programm – Wesentliche Studienergebnisse

Unter Berücksichtigung der wesentlichen Bestandteile eines Security Management-Systems wird untersucht, welche Schwerpunkte die Unternehmen bei ihren Security-Programmen setzen.



© 2015 KPMG, Deutschland

IDW PS 980, Tz. 23

> Auf der Grundlage der Beurteilung der […] Risiken werden Grundsätze und Maßnahmen eingeführt, die auf die Begrenzung der […] Risiken und damit auf die Vermeidung von […] Verstößen ausgerichtet sind. Das […] Programm umfasst auch die bei festgestellten […] Verstößen zu ergreifenden Maßnahmen. Das […] Programm wird zur Sicherstellung einer personenunabhängigen Funktion des […] Management-Systems dokumentiert.

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

3.5.1 Schwerpunkte

Der Schutz von spezifischem Know-how und wertvollen Daten rangiert bei den Befragten an erster Stelle. Im Mittelpunkt ihres Security-Programms steht für die Unternehmen vor allem Zugangskontrolle: 90 Prozent der Befragten haben eine risikoorientierte Festlegung der Zugangsberechtigungen und -kontrollen vorgenommen. Der Geheimhaltung und dem Schutz geistigen Eigentums messen die meisten Unternehmen ebenfalls große Bedeutung bei. Auch Maßnahmen zur physischen Sicherheit haben 80 Prozent der Befragten in ihren Sicherheitsprogrammen integriert. Vorbeugende Schritte treffen jedoch nur die wenigsten Unternehmen: Lediglich 10 Prozent geben an, über proaktive Strategien zur präventiven Risikomitigierung zu verfügen.

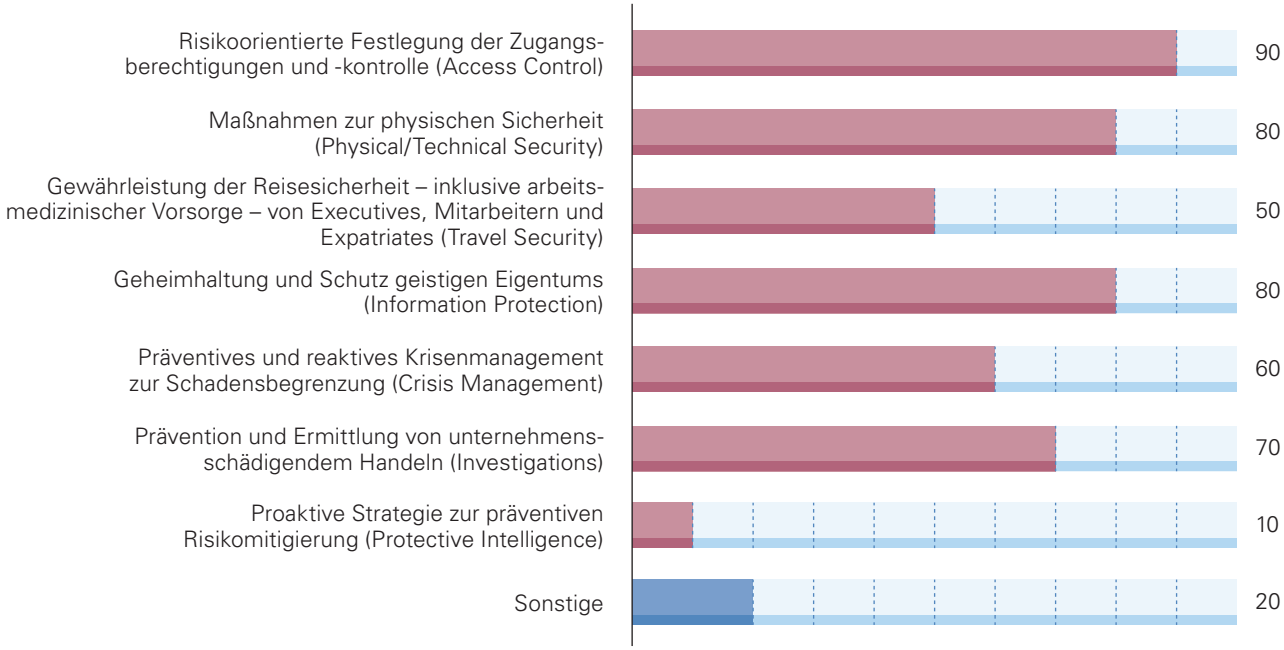
IDW PS 980

„Ein […] Programm setzt sich aus den Grundsätzen und Maßnahmen zusammen, die auf die Begrenzung der […] Risiken und damit auf ein regelkonformes Verhalten abzielen. […]

Die Maßnahmen des […] Programms zielen auf die Verhinderung von Regelverstößen ab (Prävention); dies umfasst auch das rechtzeitige Erkennen von Risiken für […] Verstöße […] und die Reaktionen auf die erkannten Risiken. (Tz. A17)“

Abb. 4 Hauptaugenmerk der Befragten liegt auf Access Control – proaktive Strategien verfolgen die wenigsten

„Welche der folgenden Schwerpunkte sind Bestandteil Ihres Security-Programms?“

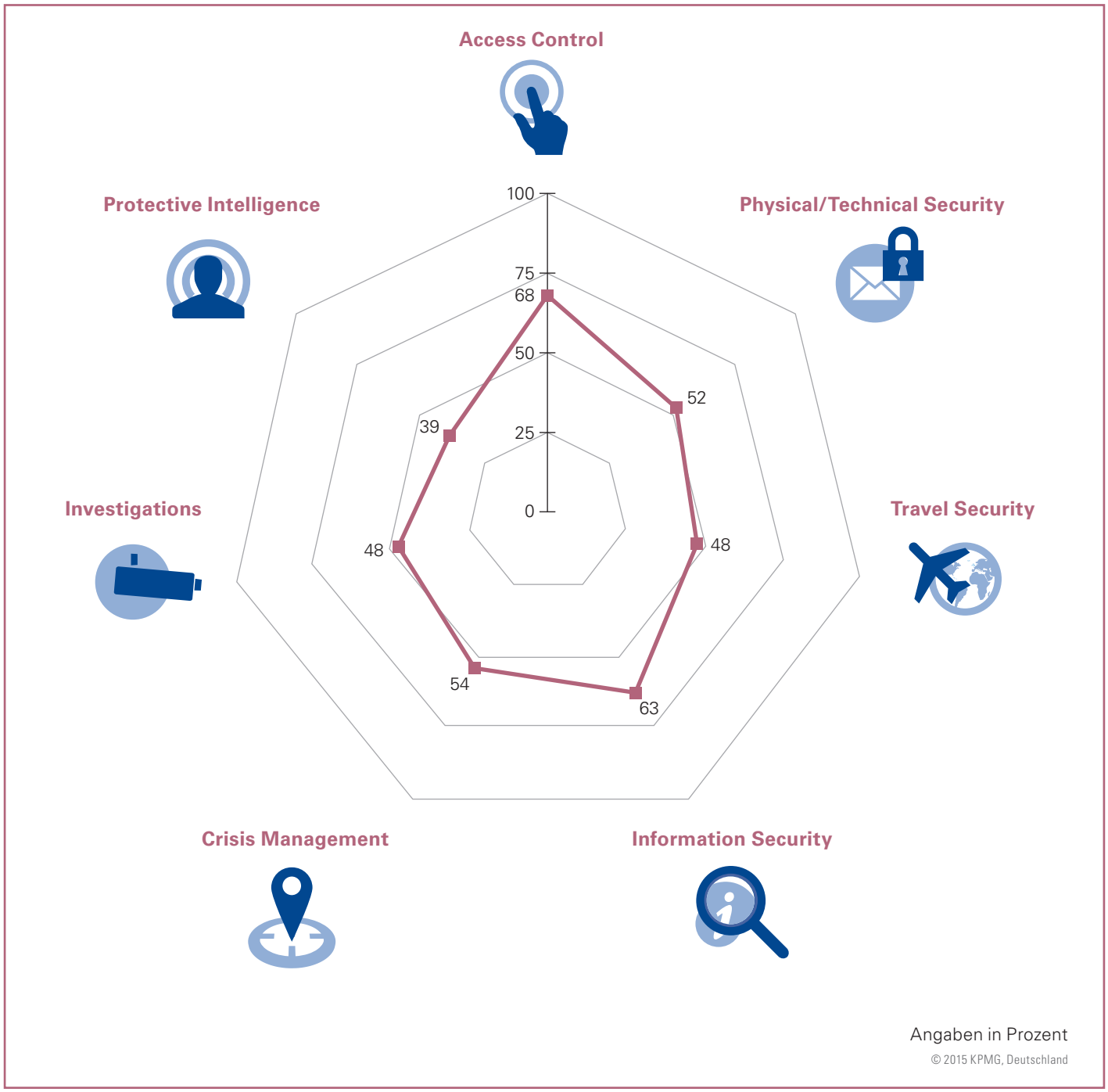


Mehrfachnennungen möglich, Angaben in Prozent

© 2015 KPMG, Deutschland

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.

Abb. 5 Ausgestaltungsgrad der einzelnen Elemente des Security-Programms als Indexwert (0 bis 100 Prozent) bei den befragten Unternehmen



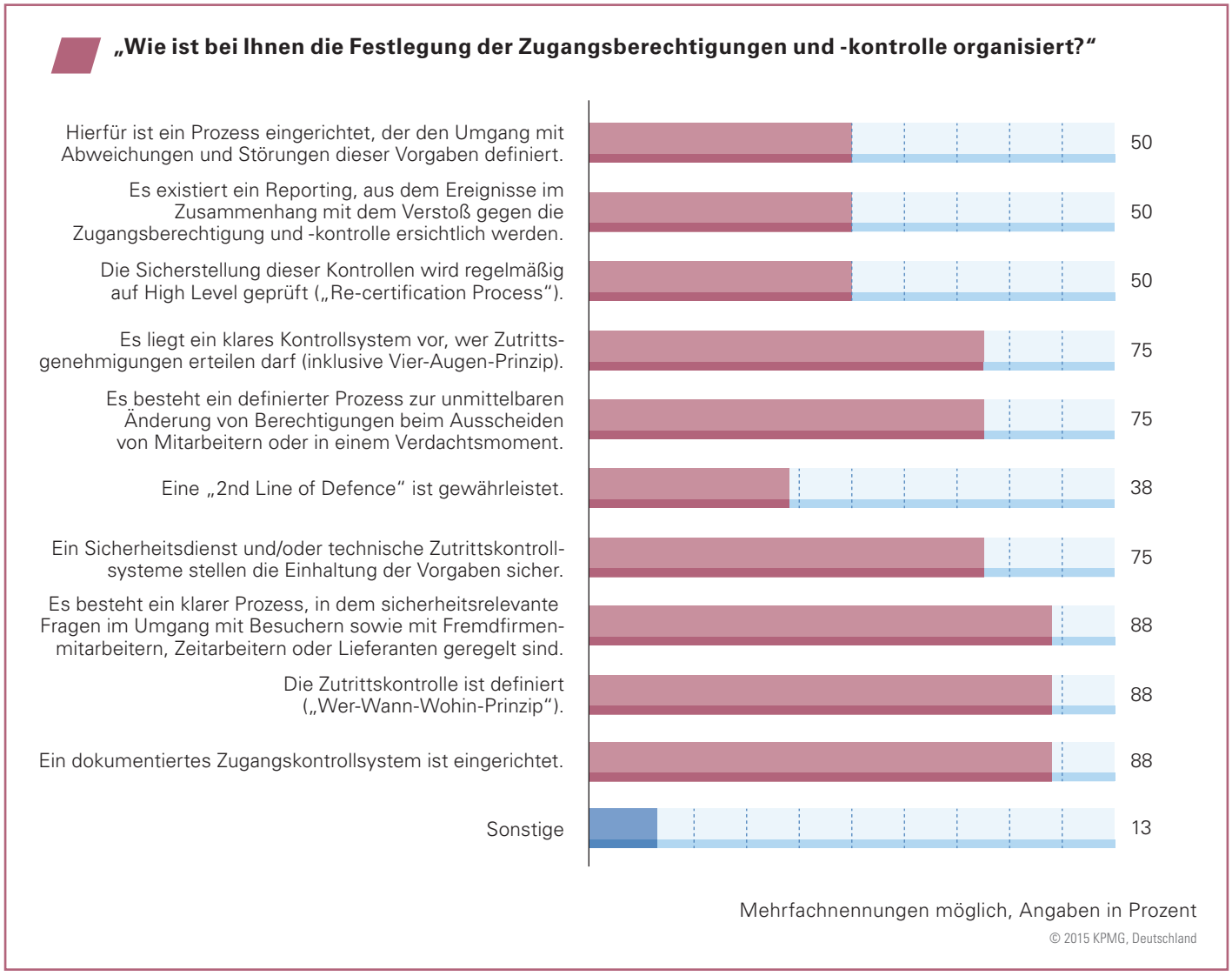
© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

3.5.2 Access Control

Welch hohe Bedeutung die Befragten dem Bereich Access Control beimessen, spiegelt sich auch in der detaillierten Festlegung der Prozesse und Regelungen wider: Bei den meisten Unternehmen existiert ein klar definiertes Zugangskontrollsystem. Auch die Zutrittskontrolle ist bei 88 Prozent der Befragten nach dem „Wer-Wann-Wohin-Prinzip" genau definiert. Ein ebenso hoher Anteil der Unternehmen verfügt über eine festgelegte Verfahrensweise, mittels derer sicherheitsrelevante Fragen im Umgang mit Besuchern sowie mit Fremdfirmenmitarbeitern, Zeitarbeitern oder Lieferanten detailliert geregelt sind.

Hinsichtlich der Einhaltung der Vorgaben setzen zwei Drittel der Unternehmen auf Sicherheitsdienste und/oder technische Zutrittskontrollsysteme.

Abb. 6 Mehrheit der Unternehmen verfügt über klar definierte Kontrollsysteme und nutzt technische Zutrittskontrollsysteme oder Sicherheitsdienste



© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

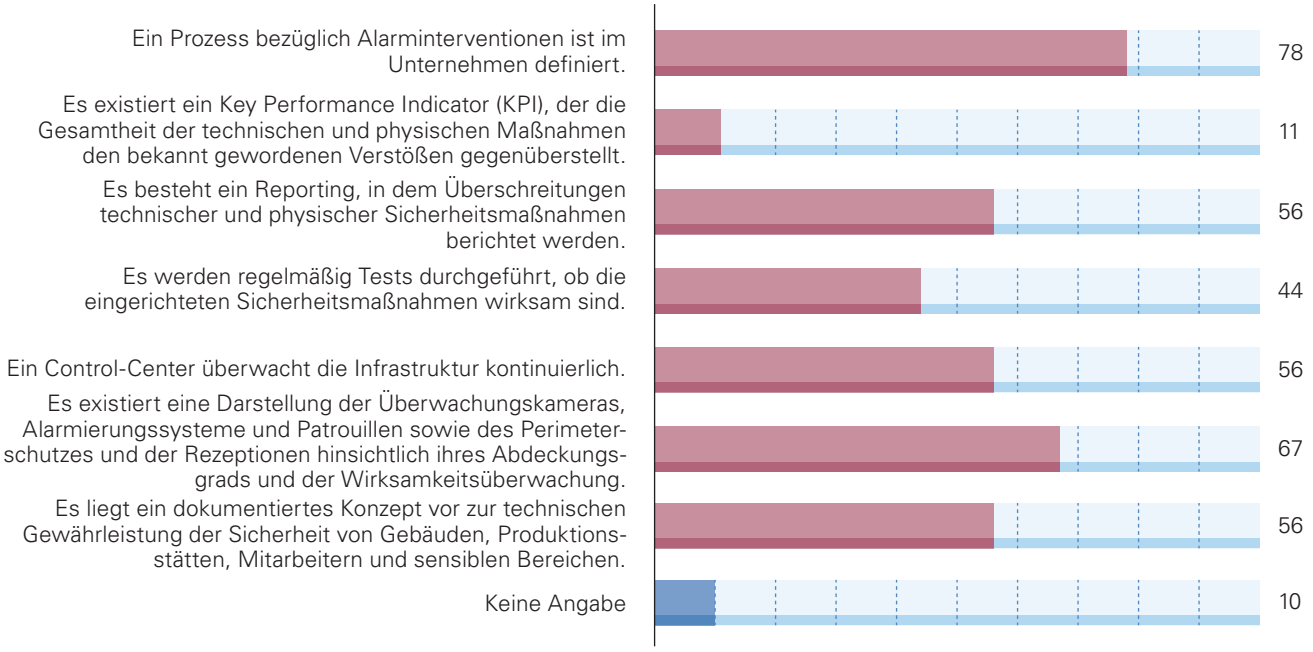
3.5.3 Physical/Technical Security

Physischer und technischer Sicherheit messen die meisten Unternehmen große Bedeutung bei. So haben beispielsweise 78 Prozent der Befragten einen Prozess implementiert, der Alarminterventionen definiert. Bei zwei Dritteln (67 Prozent) existiert eine Darstellung der Überwachungskameras, Alarmierungssysteme und Patrouillen sowie des Perimeterschutzes und der Rezeptionen hinsichtlich ihres Abdeckungsgrads und der Wirksamkeitsüberwachung.

Über ein dokumentiertes Konzept zur technischen Gewährleistung der Sicherheit von Gebäuden, Produktionsstätten, Mitarbeitern und sensiblen Bereichen verfügen 56 Prozent. Lediglich bei 11 Prozent der Befragten existiert ein Key Performance Indicator (KPI), der die Gesamtheit der technischen und physischen Maßnahmen den bekannt gewordenen Verstößen gegenüberstellt.

Abb. 7 Mehrheit der Befragten verfügt über einen definierten Prozess der Alarminterventionen

„Wie garantieren Sie die physische Sicherheit der Mitarbeiter in Ihrem Unternehmen?“



Mehrfachnennungen möglich, Angaben in Prozent

© 2015 KPMG, Deutschland

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.

3.5.4 Travel Security

„Wie gewährleisten Sie die Reisesicherheit von Executives, Mitarbeitern und Expatriates?“

Der überwiegende Teil der befragten Unternehmen (80 Prozent) verfügt über eine Reiserichtlinie, in der sämtliche Regelungen zur Buchung und Durchführung von Dienstreisen festgelegt sind. Sie ist für alle Reisenden verpflichtend.

Bei 63 Prozent dieser Unternehmen umfasst die Reiserichtlinie alle Mitarbeiter der Gruppe.

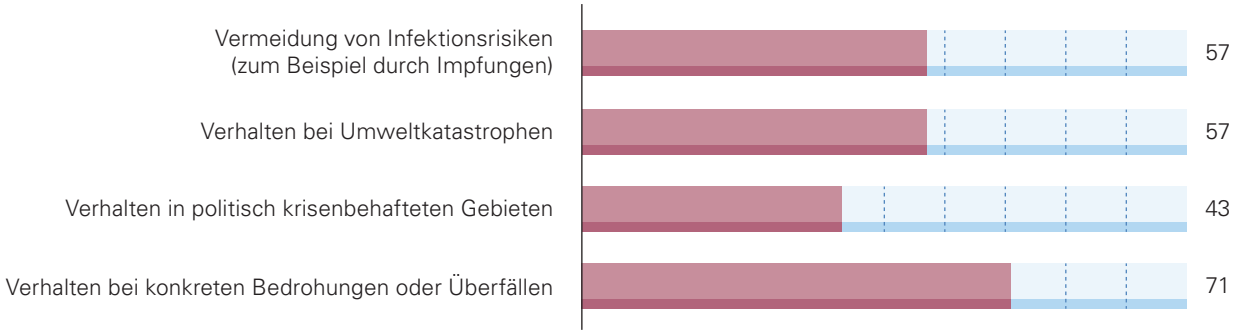
Dabei ist bei einigen Unternehmen, je nach Risikoeinstufung des Reiselands, eine zusätzliche Genehmigung nötig, um die Reise vorzunehmen.

50 Prozent der Unternehmen haben einen Prozess implementiert, der misst, wie viele Reisende, für die die Sicherheitsprozesse relevant sind, tatsächlich erfasst und entsprechend durch die Sicherheitsmaßnahmen geschützt werden.

Mehr als ein Drittel der Unternehmen (38 Prozent) geben an, bei Abweichungen von den definierten Vorgaben sowie bei Störungen mit entsprechenden, genau definierten Sicherheitsmaßnahmen zu reagieren.

Abb. 8 Mehrheit der Unternehmen sieht für Mitarbeiter auf Dienstreisen größtes Gefährdungspotenzial in Überfällen und Bedrohungen

„Auf welche Risiken im Zusammenhang mit Dienstreisen bereiten Sie Ihre Mitarbeiter vor?“



Mehrfachnennungen möglich, Angaben in Prozent

© 2015 KPMG, Deutschland

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.

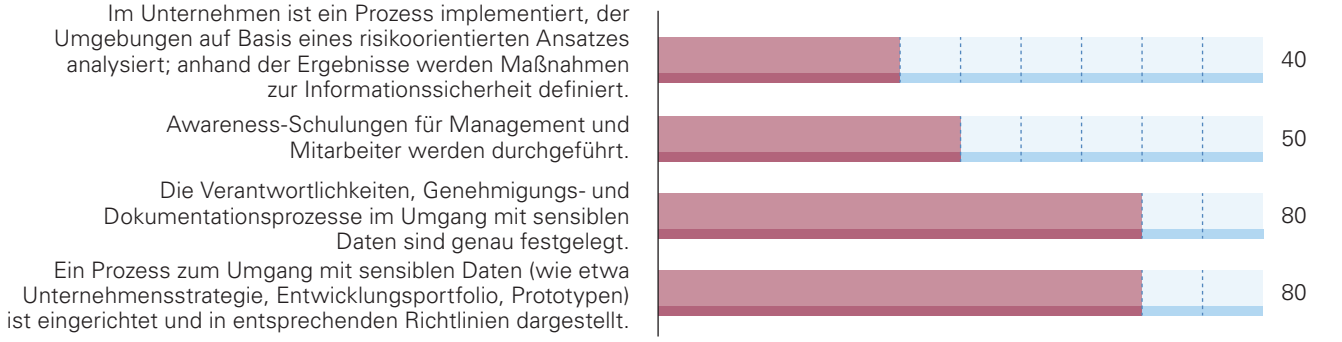
3.5.5 Information Security

Zum Schutz des geistigen Eigentums setzen die befragten Unternehmen verschiedene Programmelemente ein. Bei mehr als zwei Dritteln (80 Prozent) wurden die Verantwortlichkeiten, Genehmigungs- und Dokumentationsprozesse im Umgang mit sensiblen Daten definiert.

Bei ebenfalls 80 Prozent der Befragten wurde ein Prozess zum Umgang mit sensiblen Daten (etwa Unternehmensstrategie, Entwicklungsportfolio oder Prototypen) definiert; er ist in entsprechenden Richtlinien dargestellt.

Abb. 9 Mehrheit der Unternehmen misst Information Security hohe Bedeutung bei und definiert Prozesse zum Schutz sensibler Daten

„Welche der folgenden Programmelemente zum Schutz geistigen Eigentums sind bei Ihnen im Einsatz?“



Mehrfachnennungen möglich, Angaben in Prozent

© 2015 KPMG, Deutschland

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.

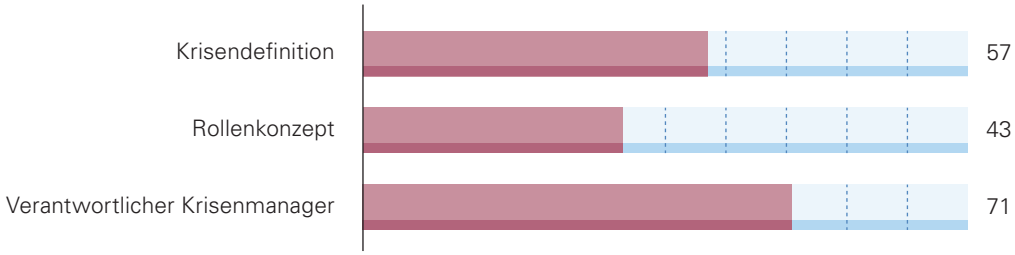
3.5.6 Crisis Management

70 Prozent der Unternehmen verfügen über einen Krisenmanagementprozess.

- Ein Drittel der Befragten führt regelmäßig Krisenstabtrainings durch.
- Circa die Hälfte der Unternehmen
  - definieren und kommunizieren Triggering Events/Points.
  - haben einen Prozess zur kontinuierlichen Weiterentwicklung des Krisenmanagements hinsichtlich etwaiger Szenarien implementiert.
  - haben einen „After Action Report" eingerichtet, der die Lessons Learned einer überstandenen Krise analysiert und Maßnahmen ableitet.

Abb. 10 Für etwa zwei Drittel der Befragten ist Schadensbegrenzung im Fall einer Krise Aufgabe des verantwortlichen Krisenmanagers

„Welche der folgenden Programmelemente werden im Rahmen des Krisenmanagements zur Schadensbegrenzung genutzt?"



Mehrfachnennungen möglich, Angaben in Prozent

© 2015 KPMG, Deutschland

Abb. 11 Im Fokus der Befragten stehen vor allem IT-Risiken und physische Gefahren – Travel Security eher nachrangiges Thema

„Für welche Szenarien bestehen in Ihrem Unternehmen Krisenmanagementpläne?"

© 2015 KPMG, Deutschland

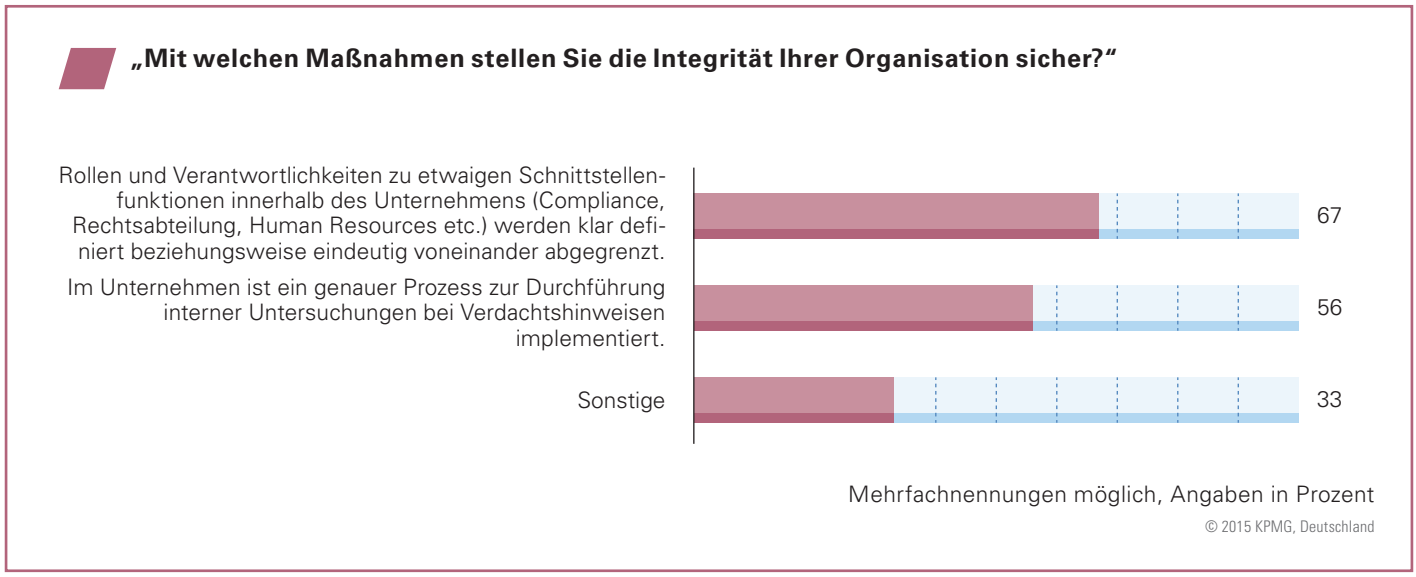
© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

3.5.7 Investigations

Zur Sicherstellung der Integrität ihres Unternehmens setzen die Befragten verschiedenste Maßnahmen ein. Bei mehr als der Hälfte (67 Prozent) werden die Rollen und Verantwortlichkeiten zu etwaigen Schnittstellenfunktionen innerhalb des Unternehmens (Compliance, Rechtsabteilung, HR etc.) klar voneinander abgegrenzt und genau definiert.

Etwa ein Drittel der Befragten setzt zur Sicherstellung der Integrität unter anderem auf die Zusammenarbeit mit Behörden oder führt Internal Audits durch.

Abb. 12 Mehrheit der Unternehmen setzt zur Sicherstellung der Integrität überwiegend auf klare Zuordnung der Verantwortlichkeiten und Rollen



© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.

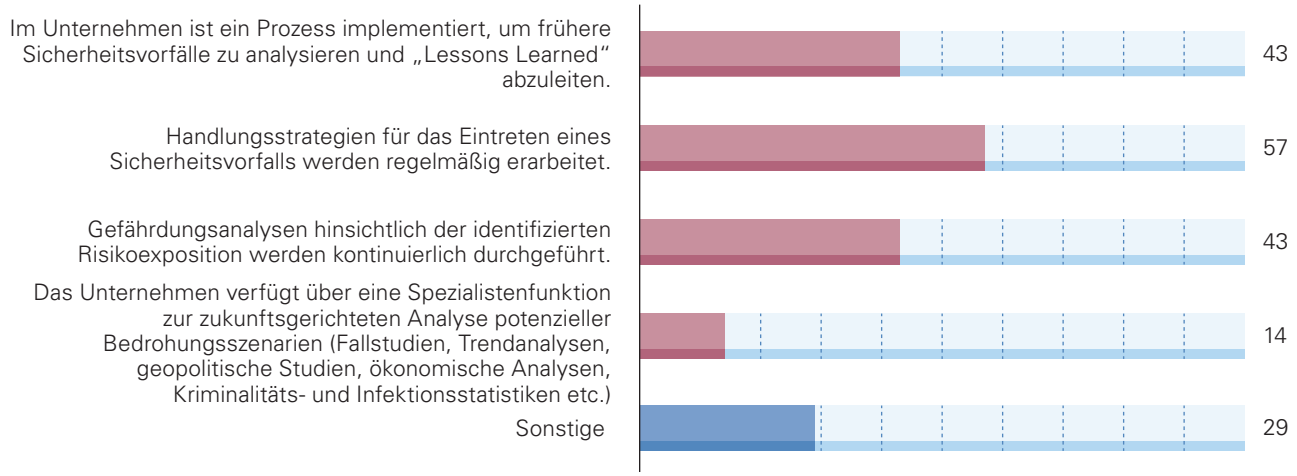
3.5.8 Protective Intelligence

Im Fokus der Protective Intelligence steht insbesondere die Frage, wer über Aktualisierungen in der Risikoexposition informiert werden muss – und in welcher Form.

Um adäquat reagieren zu können und gegebenenfalls erforderliche Maßnahmen rechtzeitig ergreifen zu können, sollten sämtliche Unternehmensbereiche in Kenntnis gesetzt werden. Dies gilt zum einen für die Geschäftsführung, den Leiter des Krisenstabs, den Leiter der Arbeitssicherheit und den Leiter des Bereichs Umweltschutz. Zum anderen müssen auch die Rechtsabteilung, das Risikomanagement, die Kommunikationsabteilung und der Sicherheitsdienst über Veränderungen hinsichtlich der Unternehmensrisiken stets auf dem Laufenden sein.

Abb. 13 Mehrheit der Befragten erarbeitet Handlungsstrategien zur Anwendung bei Ereigniseintritt

„Inwieweit verfügen Sie über ein System zur frühzeitigen Identifizierung von neuartigen Risiken beziehungsweise veränderten Risikoszenarien?“



Mehrfachnennungen möglich, Angaben in Prozent

© 2015 KPMG, Deutschland

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.

3.6 Unsere Empfehlungen

Sicherheitsmanagement sollte sich nicht auf eine Momentaufnahme beschränken. Im Fokus einer effektiven Governance steht vielmehr die Verfolgung nachhaltiger Maßnahmen zur kontinuierlichen Verbesserung des Sicherheitsmanagementsystems.

Dies bietet Ihnen unter anderem folgende Vorteile:

- Schaffung und Weiterentwicklung eines Unternehmensumfelds, in dem höchste Sicherheitsstandards umgesetzt wurden – damit Sie sich auf Ihre geschäftlichen Ziele fokussieren können
- Sicherstellung der Einhaltung gesetzlicher Anforderungen, interner Richtlinien und Standards
- Dokumentierter Nachweis der erbrachten Sorgfalts- und Überwachungspflichten
- Vermeiden eines Informationsverlusts firmeneigenen Wissens
- Erarbeitung eines Konzepts, das nach Eintritt eines Krisenszenarios die Rückkehr zum wirtschaftlichen Normalbetrieb steuert und die Kommunikation mit externen Ansprechpartnern festlegt
- Vorhandensein von definierten Prozessen, Kontrollmechanismen und Überwachungsfunktionen
- Sicherstellung eines fundierten, geplanten Umgangs mit Abweichungen und Störungen der Regelprozesse
- Maßnahmen zum Schutz vor unkontrollierten Risiken wie Vermögensschädigung, Reputationsschäden oder Verlust geistigen Eigentums
- Erstellung eines umfassenden Sicherheitskonzepts, in dem Ihre Sicherheitsrisiken zusammengefasst dargestellt und im Hinblick auf Good Practices bewertet werden sowie bestehender Handlungsbedarf aufgezeigt wird
- Entwicklung eines Präventivkonzepts, in dem die bestehenden Sicherheitsrisiken adressiert und mitigiert werden

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

Ihre Frage

Wie kann ein Unternehmen wesentlichen Sicherheitsrisiken wirkungsvoll vorbeugen?

Unsere Antwort

- Anhand einer Bestandsanalyse (Quick Scan) unterstützen unsere Fachleute Sie dabei, rechtliche und prozessuale Fallstricke zu ermitteln; zudem geben sie Handlungsempfehlungen zum Vermeiden der aufgezeigten Sicherheitsrisiken.
- Im Fokus steht dabei stets die Sicherstellung der Einhaltung gesetzlicher Anforderungen sowie der spezifischen internen Richtlinien und Standards des Unternehmens.
- Auf Wunsch erstellen unsere Experten für Sie ein umfassendes Sicherheitskonzept, in dem sämtliche diesbezüglichen Risiken abgebildet und im Hinblick auf Good Practices bewertet werden. Darüber hinaus zeigen wir potenziellen Handlungsbedarf auf.

Ihre Frage

Wie sollte ein wirksames Security Management-System ausgestaltet sein?

Unsere Antwort

Auf Basis langjähriger Erfahrung unterstützen unsere Sicherheitsspezialisten Sie bei folgenden Herausforderungen:

- Konzeption der Sicherheitsstrategie unter Berücksichtigung Ihrer spezifischen Unternehmensziele und der gegebenen Rahmenbedingungen
- Entwicklung eines Präventivkonzepts, in dem die bestehenden Sicherheitsrisiken adressiert und mitigiert werden
- Erarbeitung eines globalen Sicherheitskonzepts, in dem die Rollen und Verantwortlichkeiten festgelegt, die Risiken identifiziert und bewertet sowie geeignete Maßnahmen und Kontrollen definiert werden
- Identifizierung von möglichem Optimierungsbedarf bezüglich der Ausgestaltung der einzelnen Bestandteile sowie der übergreifenden Elemente des Security Management-Systems

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

Ihre Frage

Wie kann Governance-Anforderungen effektiv begegnet werden?

Unsere Antwort

Gerne stehen wir Ihnen bei der Einrichtung eines angemessenen Steuerungs- und Regelungssystems der Aufbau- und Ablauforganisation zur Seite – mit dem Ziel der Risikomitigierung sicherheitsrelevanter Themen.

Darüber hinaus empfiehlt sich die Definition der Prozess- und Risikoverantwortlichen im Unternehmen sowie die Festlegung sowohl prozessintegrierter als auch prozessunabhängiger Kontrollmaßnahmen.

Ihre Frage

Was ist im Hinblick auf Qualitätssicherung zu beachten?

Unsere Antwort

Auf Wunsch unterstützen unsere Fachleute Sie bei der Prüfung ausgewählter Sicherheitsprozesse und führen ein Benchmarking bestehender Sicherheitsmaßnahmen durch.

Des Weiteren überprüfen wir für Sie unternehmensweit die Umsetzung wesentlicher Sicherheitsvorgaben – auch in dezentralen Standorten sowie gegebenenfalls bei ausländischen Tochtergesellschaften.

Zudem bescheinigen wir für Sie die Konzeption, Implementierung und Wirksamkeit Ihrer Sicherheitsmaßnahmen oder ausgewählter Prozesse und Kontrollen.

Unsere Leistungen zielen auf die Schaffung und Weiterentwicklung eines Unternehmensumfelds ab, in dem höchste Sicherheitsstandards umgesetzt werden – zur Fokussierung auf die geschäftlichen Chancen.

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Jens C. Laue
Partner
Head of Governance & Assurance Services
T +49 211 475-7901
jlaue@kpmg.com

Dr. Antonia Steßl
Manager
Governance & Assurance Services
T +49 89 9282-4276
astessl@kpmg.com

www.kpmg.de/assurance

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Printed in Germany. Der Name KPMG, das Logo und „cutting through complexity" sind eingetragene Markenzeichen von KPMG International.