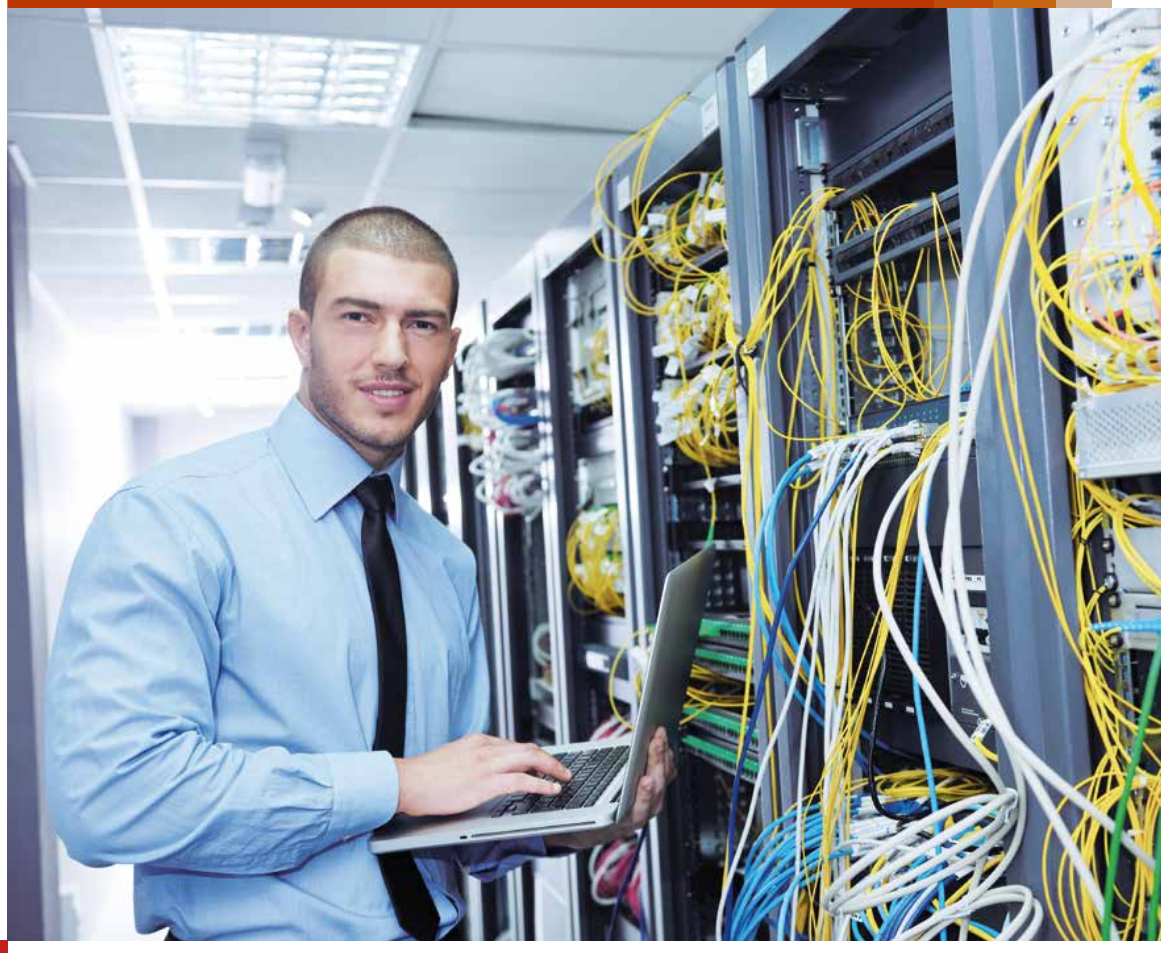
# *Wie steht es um die Informationssicherheit im deutschen Mittelstand?*

*Eine Erhebung zu aktuellen Trends und Herausforderungen in der Informationssicherheit in mittelständischen Unternehmen – mit Handlungsempfehlungen aus dem Hause PwC.*



pwc

# *Wie steht es um die Informationssicherheit im deutschen Mittelstand?*

*Eine Erhebung zu aktuellen Trends und Herausforderungen in der Informationssicherheit in mittelständischen Unternehmen – mit Handlungsempfehlungen aus dem Hause PwC.*

pwc

**Wie steht es um die Informationssicherheit im deutschen Mittelstand?**

Herausgegeben von der PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft (PwC)

Von Derk Fischer unter Mitwirkung von Dr. Johannes Barnickel, Philipp Engemann,
Prof. Dr. Peter Merz, Nial Moore, Katrin Otto, Aleksei Resetko

März 2014, 40 Seiten, 22 Abbildungen, Softcover



Die Inhalte dieser Publikation sind zur Information unserer Mandanten bestimmt. Sie entsprechen dem Kenntnisstand der Autoren zum Zeitpunkt der Veröffentlichung. Für die Lösung einschlägiger Probleme greifen Sie bitte auf die in der Publikation angegebenen Quellen zurück oder wenden sich an die genannten Ansprechpartner. Meinungsbeiträge geben die Auffassung der einzelnen Autoren wieder. In den Grafiken kann es zu Rundungsdifferenzen kommen.

# Inhaltsverzeichnis

Abbildungsverzeichnis ..... 6

A Executive Summary ..... 8

B Einleitung ..... 10

C Methodischer Aufbau ..... 11

D Stellenwert der Informationssicherheit ..... 12
1 Prozesse, formale Funktionen und Überwachung ..... 12
2 Informationssicherheitsprozesse im Unternehmen ..... 12
3 Richtlinien und Überwachung ..... 14
4 Formal definierte Mitarbeiterstellen für die Umsetzung von IT-Sicherheitsfunktionen ..... 16
5 Mitarbeitersensibilisierung ..... 18
6 Berücksichtigung im Budget ..... 19

E Trends und deren Auswirkungen auf die Informationssicherheit ..... 23

F Cyberattacken ..... 26
1 Auftreten von Attacken ..... 26
2 Reaktion auf PRISM und Tempora ..... 29

G Reaktion des Gesetzgebers ..... 32
1 Staatliche Motivation ..... 32
2 Internationale Initiativen ..... 32
3 Nationale Gesetze ..... 34

H Fazit und Ausblick ..... 36

Ihre Ansprechpartner ..... 37

# Abbildungsverzeichnis


Abb. 1 IT-Budget 2013 ..... 11

Abb. 2 Stellenwert von Standards für die Informationssicherheits-prozesse der Unternehmen ..... 13

Abb. 3 Sicherheitsrelevante Bereiche, für die Sicherheitsvorgaben definiert sind ..... 15

Abb. 4 Maßnahmen zur Überwachung der Einhaltung von Sicherheitsvorgaben ..... 16

Abb. 5 Formal beschriebene Rollen für die Umsetzung von Sicherheitsfunktionen in den Unternehmen ..... 16

Abb. 6 Stellen im Unternehmen, an die der CISO berichtet ..... 17

Abb. 7 Einschätzung des Sensibilisierungsgrads der Mitarbeiter für das Thema Informationssicherheit sowie Schulungsmaßnahmen im Unternehmen ..... 19

Abb. 8 Jährliches Budget für Informationssicherheit ..... 20

Abb. 9 Geschätzte Entwicklung der Ausgaben für Informationssicherheit 2014 ..... 21

Abb. 10 Gründe für Mehrausgaben für Informationssicherheit ..... 21

Abb. 11 Durchschnittliches IT-Security Budget international ..... 22

Abb. 12 IT-Themen, die in den kommenden fünf Jahren die größte Relevanz für die Informationssicherheit haben werden ..... 23

Abb. 13 Besonders risikoreiche Trends aus Sicht der Informationssicherheit ..... 24

Abb. 14 Risiko von Betrug und Missbrauch bei der Nutzung von Cloud Computing ..... 25

Abb. 15 Vorkommen von Cyberattacken ..... 27

Abb. 16 Ziele von Cyberattacken ..... 27

Abb. 17 Finanzieller Schaden durch Cyber-Attacken ..... 28

Abb. 18 Ergebnisse des Cybercrime Survey – Vorhandensein von Strategien gegen Insider Security Incidents in den Unternehmen .....29

Abb. 19 Einfluss von PRISM und Tempora auf die Sicherheitsstrategie .....30

Abb. 20 Mögliche Folgen von PRISM und Tempora für die Unternehmen.....30

Abb. 21 Wegen PRISM/Tempora zu überdenkende Bereiche .....31

Abb. 22 Bekanntheit des Meldegesetzes.....35

# A Executive Summary

Der deutsche Mittelstand war in der Berichterstattung zu Angriffen auf die IT überraschenderweise bislang selten Thema – trotz seiner großen Bedeutung für die deutsche Wirtschaft und seiner international bekannten und geschätzten Innovationsfähigkeit.

Im Auftrag von PwC wurden 405 Unternehmen aus Deutschland durch ein unabhängiges Marktforschungsinstitut zu aktuellen Fragen der Informationssicherheit hinsichtlich Strategie, Organisation und Umsetzung sowie zum Umgang mit den neuesten Entwicklungen in der Industrie- und Wirtschaftsspionage mittels standardisierten Fragebogen befragt.

Die Ergebnisse der Studie sind ernüchternd: Informationssicherheit ist zwar mittlerweile auch im Mittelstand als Thema angekommen, allerdings bestehen große Verbesserungspotenziale bei der Umsetzung angemessener Sicherheitsmaßnahmen.

Der Grund für die unzureichende Sicherheit liegt nicht selten in einer Fehleinschätzung seitens der Geschäftsführung hinsichtlich der Wichtigkeit des Themas. So hat die Aufdeckung der Spähprogramme PRISM und Tempora im Zuge des NSA-Skandals nur bei einem Drittel der befragten Unternehmen dazu geführt, dass die Angemessenheit der eigenen Sicherheitsstrategie zumindest einmal hinterfragt wird. Zudem verfügt ein Großteil der KMUs zwar über Vorgaben zur Informationssicherheit und damit über einen Governance-Rahmen, dieser folgt jedoch nur selten einem anerkannten Standard.

Informationssicherheit wird folglich mangels besseren Wissens im Eigenbau umgesetzt. Das mag für Maßnahmen wie Systemhärtung oder Einrichtung einer Firewall anhand frei verfügbarer Anleitungen noch ansatzweise funktionieren. Doch KMUs verfügen nur teilweise über eine angemessene Sicherheitsorganisation und sind daher nicht in der Lage, einen prozess- und risikoorientierten Ansatz zur Behandlung von Sicherheitsthemen zu verfolgen.

KMUs hinken in ihrem Schutz den Methoden und Möglichkeiten der Angreifer deutlich hinterher und tun sich mit der Anpassung an die neuen Herausforderungen schwer. Fast scheint es, als hätten sie sich entweder zum Aussitzen des momentanen Hypes oder aber zur Resignation entschlossen. Beide Reaktionen sind jedoch wenig erfolgversprechend, denn die Informationssicherheit hat für Unternehmen, unabhängig von ihrer Größe oder dem öffentlichem Interesse, längst die Nischenbedeutung einer technischen Funktion hinter sich gelassen. Will ein Unternehmen heute erfolgreich am Markt bestehen, muss es sich in einer zunehmend digitalisierten Welt behaupten.

Eine der wesentlichen Fragen neben der effizienten Neugestaltung geeigneter Geschäftsprozesse ist damit die Frage nach dem Vertrauen in die digitalisierten Prozesse: Wie und mit welchen Hilfsmitteln sollten Unternehmen in digitales Vertrauen investieren, um den Erwartungen der Geschäftspartner, Kunden und Mitarbeiter gerecht zu werden? Diese Frage stellt sich bereits beim Design der Prozesse, setzt sich bei der sicheren Umsetzung in Anwendungen und Systeme fort und erstreckt sich generell auf den nachhaltig sicheren und sich kontinuierlich an neue Situationen und Bedrohungslagen anpassenden Betrieb dieser Prozesse.

Hierauf sind Unternehmen allein auf Basis veralteter Richtlinien nicht angemessen vorbereitet und müssen umdenken, denn der Grundsatz „My home is my castle“ ist für eine Unternehmensarchitektur in einer digitalen Welt nicht mehr zeitgemäß. Vielmehr lautet der künftige (und teilweise auch schon aktuelle) Lösungsweg „Kollaboration“.

Um in diesem Umfeld mit angemessenem Sicherheitsniveau agieren und Unternehmenswerte wirkungsvoll schützen zu können, werden insbesondere KMUs nicht umhinkommen, im Bereich Informationssicherheit enger zusammenzuarbeiten. Der Austausch von Erfahrung und Lösungsansätzen wird künftig ein sehr wichtiger Erfolgsbaustein sein. Die derzeit von Einrichtungen wie dem BSI diskutierten Ideen rund um ein Meldegesetz für Sicherheitsvorfälle werden kurzfristig in ein Sharingprinzip für Sicherheitsfragen münden müssen, um insbesondere den KMUs im Wettlauf mit potenziellen Datendieben und Cyberkriminellen eine Chance einzuräumen. Leider verfügt der Mittelstand derzeit aber weder über die Voraussetzungen für mehr Transparenz noch über die technische Ausstattung, um hierzu einen angemessenen Beitrag zu leisten.

Dabei muss Informationssicherheit bei Weitem nicht so kostenintensiv sein, wie es auf den ersten Blick erscheint. Durch einen risikoorientierten Ansatz, der sich auf die wesentlichen Unternehmenswerte konzentriert, kann in puncto Schutzbedarf schon mit überschaubarem Aufwand viel erreicht werden. Allerdings macht dies nur dann Sinn, wenn diese Maßnahmen langfristig umgesetzt und weiterentwickelt werden und wenn die gemachten Erfahrungen, auch die negativen, in angemessener Form mit anderen geteilt werden.

# B Einleitung

***Chinesische Hacker greifen deutsche Industrieunternehmen an. Angreifer können die Steuerung von Autos übernehmen. Einzelhändler sperrt Internetseite nach massivem Angriff über das Internet. Behörden werden Opfer von Phishing. Zugangsdaten von 16 Millionen E-Mail-Konten wurden gehackt. 70 Millionen Nutzerdaten wurden bei einem Hersteller von Unterhaltungselektronik gestohlen.***

Es vergeht beinahe kein Tag, an dem nicht von Hackerangriffen, Datenlecks und Serverausfällen berichtet wird. Die Berichterstattung beschränkt sich dabei nicht mehr auf IT-Fachmagazine und Internetportale zum Thema IT-Sicherheit. Mit der Prominenz der Opfer solcher Angriffe auf die Daten, Netze und Computer steigt auch das öffentliche Interesse. Onlineshops von großen Einzelhändlern sind stundenlang offline, millionenfach werden Zugangsdaten von Onlinekonten und E-Mail-Konten gestohlen und Industrieanlagen werden durch Angriffe auf SCADA-Systeme (Supervisory Control and Data Acquisition – IT-Systeme zur Überwachung und Steuerung technischer Prozesse) lahmgelegt oder zerstört. Dies führt mittlerweile zu einem deutlich spürbaren Vertrauensverlust der Bevölkerung in digitale Medien, der auch die Unternehmen erfasst. Aufgrund der hohen Komplexität des Problems steht der Einzelne hilflos und resignierend davor – und das geht nicht nur dem „Normalverbraucher“ so, sondern auch einem Teil der verantwortlichen leitenden Mitglieder in den Führungsetagen deutscher Unternehmen.

Während der Fokus der öffentlichen Berichterstattung über das Versagen der Informationssicherheit vornehmlich auf den großen und bekannten Marken und Unternehmen liegt, konzentriert sich diese Studie auf eine Gruppe von Unternehmen, die trotz ihrer übergroßen Bedeutung für die deutsche Wirtschaft und ihrer international bekannten und geachteten Innovationsfähigkeit bisher in der Berichterstattung zu Angriffen auf die IT noch wenig in Erscheinung getreten ist. Ist der deutsche Mittelstand für Hacker und Computerviren kein lohnendes Ziel? Haben die IT-Abteilungen die mittelständischen Unternehmen schon so gut gegen Angreifer geschützt, dass es keinen Grund zur Sorge gibt? Oder werden gelungene Angriffe nur deshalb nicht öffentlich, weil sie von den Unternehmen entweder nicht erkannt werden oder bewusst geheim gehalten werden, um das Unternehmensimage nicht zu schädigen?

Die Befragung von IT-Experten mittelständischer Unternehmen und der Vergleich ihrer Antworten mit denen von Experten aus deutschen Großunternehmen erlaubt Einblicke in die Strategien der Mittelständler zur Abwehr von Cyberattacken und in ihre Überlegungen zu neuen Technologien und zeigt den Stellenwert, den sie der Informationssicherheit beimessen. Bei der Darstellung der Ergebnisse wurde insbesondere auch Wert darauf gelegt aufzuzeigen, wo mittelständische Unternehmen noch Nachholbedarf in Sachen Informationssicherheit haben und wo sie schon gut aufgestellt sind.

# C Methodischer Aufbau

Die PwC-Studie zum Thema „Informationssicherheit im Mittelstand“ beschreibt die Ergebnisse einer Befragung von 405 Unternehmen aus Deutschland. Durchgeführt wurde die Befragung von einem unabhängigen Marktforschungsinstitut im Auftrag von PwC. Die Befragung der 405 Unternehmen fand in Form von Computer Aided Telephone Interviews (CATI) auf Basis eines vollstrukturierten Fragebogens statt. Durchgeführt wurden die Interviews im Zeitraum vom 11. September bis zum 15. Oktober 2013.

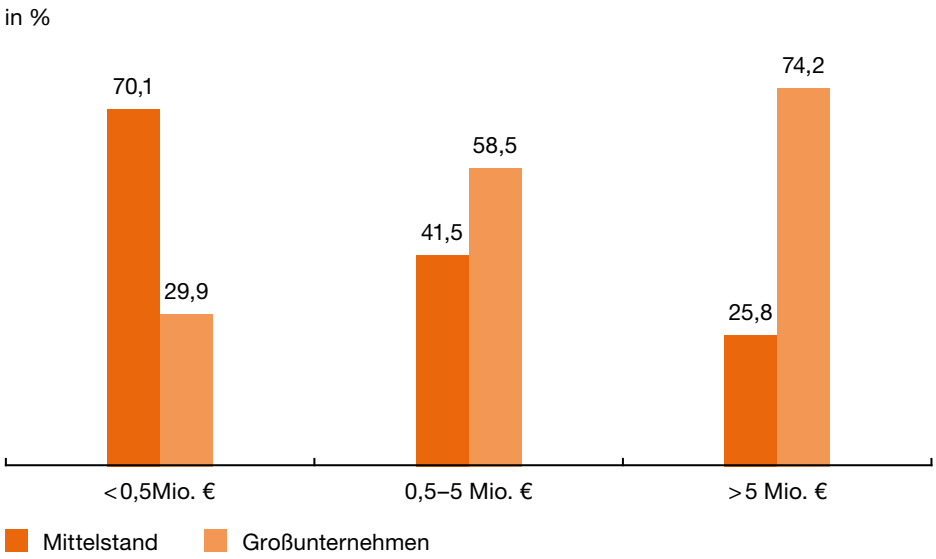
Um die besonderen Herausforderungen des Mittelstands im Vergleich zu denen von Großunternehmen und Konzernen zu beleuchten, wurden die befragten Unternehmen in zwei Klassen geteilt:

- Mittelstand: Unternehmen mit einer Mitarbeiterzahl von 200 bis 500 (202 Interviews)
- Großunternehmen: Unternehmen mit einer Mitarbeiterzahl von über 500 (203 Interviews)

Diese Kategorisierung wurde gewählt, um die Antworten auf die Unternehmensgröße beziehen und spezifische Tendenzen im Mittelstand im Vergleich zu denen in Großunternehmen herausstellen zu können und orientiert sich an der Grenze die das Institut für Mittelstandsforschung in Bonn definiert hat.

Auch hinsichtlich des Jahresnettoumsatzes wurden die befragten Unternehmen in Größenklassen eingeteilt: 46 % der Befragten erzielten im Vorjahr weniger als 250 Millionen Euro Nettoumsatz in Deutschland, 22 % erwirtschaften einen Nettojahresumsatz von über 250 Millionen Euro. Die übrigen Befragten sind Non-Profit-Organisationen aus Bund und Ländern, beispielsweise Bildungs- und Verwaltungsorganisationen. Der Fragebogen war auf Mitarbeiter der befragten Organisationen mit IT-Verantwortung ausgerichtet, sodass die IT-Leiter den größten Teil der befragten Personen stellten. Das zur Verfügung stehende IT-Budget der Unternehmen ist in Abbildung 1 dargestellt.

**Abb. 1 IT-Budget 2013**



# D Stellenwert der Informationssicherheit

## 1 Prozesse, formale Funktionen und Überwachung

Der deutsche Mittelstand mit seinen bundesweit rund 3,4 Millionen Unternehmen ist ein wesentlicher Bestandteil der deutschen Wirtschaft. Nicht zuletzt durch die Abbildung realer Unternehmensabläufe in der Unternehmens-IT sind moderne Informations- und Kommunikationstechnologien aus kleinen und mittleren Unternehmen (KMUs) nicht mehr wegzudenken. Für viele Unternehmen sind Informations- und Kommunikationstechnologien (IKTs) nicht einfach nur unterstützende Werkzeuge im Betriebsalltag, sondern fungieren als Treiber von Innovationen und bilden somit einen Grundstein für Wachstum und Entwicklung. Den vielen Vorteilen der IT stehen aber auch Gefahren und Risiken gegenüber. Daher ist ein sicherheitsbewusster Umgang mit Informationstechnologie notwendig. So müssen sich KMUs den Herausforderungen der IT-Sicherheit und damit verbundener Prozesse stellen, wie beispielsweise:

- der zunehmenden Zahl und Intensität von Angriffen auf die IT-Infrastruktur und elektronischen Daten,
- den neuen Trends und Technologien in der IT,
- dem Aufbau einer betrieblichen Sicherheitskultur,
- der Implementierung eines Informationssicherheitsmanagementsystems (ISMS)
- der kontinuierliche Aufrechterhaltung der IT-Sicherheit

Sind Unternehmen nicht in der Lage, ihre Daten und damit die Geschäftsprozesse adäquat abzusichern, laufen sie Gefahr, sowohl direkte finanzielle Schäden als auch Imageschäden zu erleiden.

## 2 Informationssicherheitsprozesse im Unternehmen

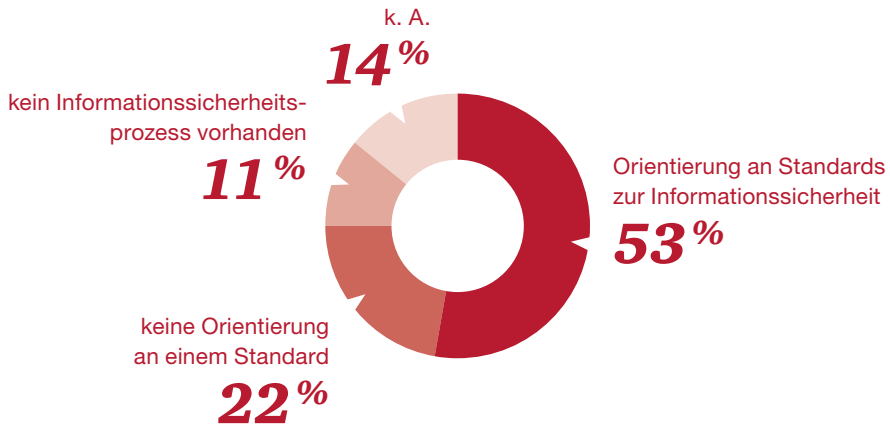
Um den heutigen Bedrohungen im Cyberspace gerecht zu werden, reichen die Sicherheitsstrategien von gestern nicht mehr aus. Vielmehr wird ein neues Modell des Umgangs mit Informationssicherheit benötigt, das auf dem Wissen um Gefährdungen, um Ziele und Motivationen potenzieller Angreifer und um die schützenswerten Unternehmenswerte basieren muss.

Um diesem Anspruch zu genügen, müssen Unternehmen zunächst ihre Unternehmenswerte identifizieren und klassifizieren sowie Prozesse und Maßnahmen zu deren Schutz priorisieren. Bei der Gestaltung der Sicherheitsorganisation und der Sicherheitsprozesse ist es sinnvoll, sich an bestehenden Standards der Informationssicherheit zu orientieren, um wichtige Informationen richtig zu schützen. Die Studie zur Informationssicherheit im Mittelstand ergab, dass 11 % der befragten mittelständischen und

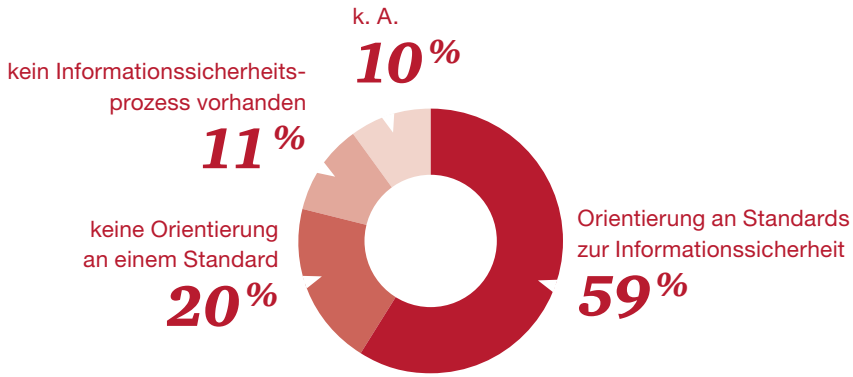
Großunternehmen keinen Informationssicherheitsprozess definiert und implementiert haben. Weitere 22 % der Mittelständler und 20 % der Großunternehmen orientieren sich derzeit bei der Ausarbeitung ihrer Prozesse nicht an einem Standard. Nimmt man diese Zahlen zusammen, wird deutlich, dass sich jedes dritte befragte Unternehmen nicht an gängige und bereits erfolgreich angewandte Standards wie ISO 27001 zur Gestaltung eines ISMS oder an die Vorgaben des Information Security Forums hält. Dies birgt die Gefahr, dass Maßnahmen zum Schutz der IT und der Daten des Unternehmens nicht ausreichend koordiniert und zu klein dimensioniert werden. Auch besteht das Risiko einer einseitigen Ausrichtung der Informationssicherheitsumgebung auf einzelne Bedrohungen wie beispielsweise Angriffe per Internet (Cyberattacken).

**Abb. 2 Stellenwert von Standards für die Informationssicherheitsprozesse der Unternehmen**

Orientierung der Informationssicherheitsprozesse an Standards im Mittelstand




Orientierung der Informationssicherheitsprozesse an Standards in Großunternehmen



Die Wesentlichen Treiber der Entscheidung zur Orientierung an Standards und Best Practices sind bei mittelständischen Unternehmen und Großunternehmen ähnlich gelagert. So sind regulatorische Anforderungen bei 55 % der Mittelständler der Grund für die Einführung eines ISMS (59 % bei Großunternehmen), gefolgt von Vorgaben des Vorstands mit 47 % (53 % bei Großunternehmen). An dritter Stelle steht die Möglichkeit, Informationssicherheit durch ein ISMS effektiv zu steuern (39 % für mittelständische Unternehmen bzw. 41 % bei Großunternehmen).

Unternehmen stehen in der Regel vor der Wahl, IT-Leistungen selbst zu erbringen oder von außen zu beziehen. Diese Frage nach dem Make-or-Buy stellt sich insbesondere bei IT-Sicherheitsdienstleistungen, da Unternehmen oft über kein oder nur eingeschränktes Know-how in diesem Bereich verfügen. Dies gilt gleichermaßen für mittelständische Unternehmen wie für Großunternehmen, deren Kernkompetenzen nicht im Bereich des IT-Managements liegen. Die Fremdvergabe von IT-Sicherheitsleistungen ist beispielsweise dann vorteilhaft, wenn beim Dienstleister Skalierungseffekte erzielt und Synergien gehoben werden, die sich auf Unternehmensseite nicht darstellen lassen. Die Qualität der Aufgabenerbringung ist bei erfahrenen IT-Sicherheitsdienstleistern meist dauerhaft gewährleistet, während sie beim Eigenbetrieb, gerade im Mittelstand, nicht in jedem Unternehmen ohne Weiteres sicherzustellen ist. Welche Leistungen in welchem Umfang von externen IT-Dienstleistern eingekauft werden, kann stark variieren. Wird ein Großteil der IT in Eigenleistung erbracht, kann es sinnvoll sein, Informationssicherheitsleistungen ebenfalls selbst zu erbringen.

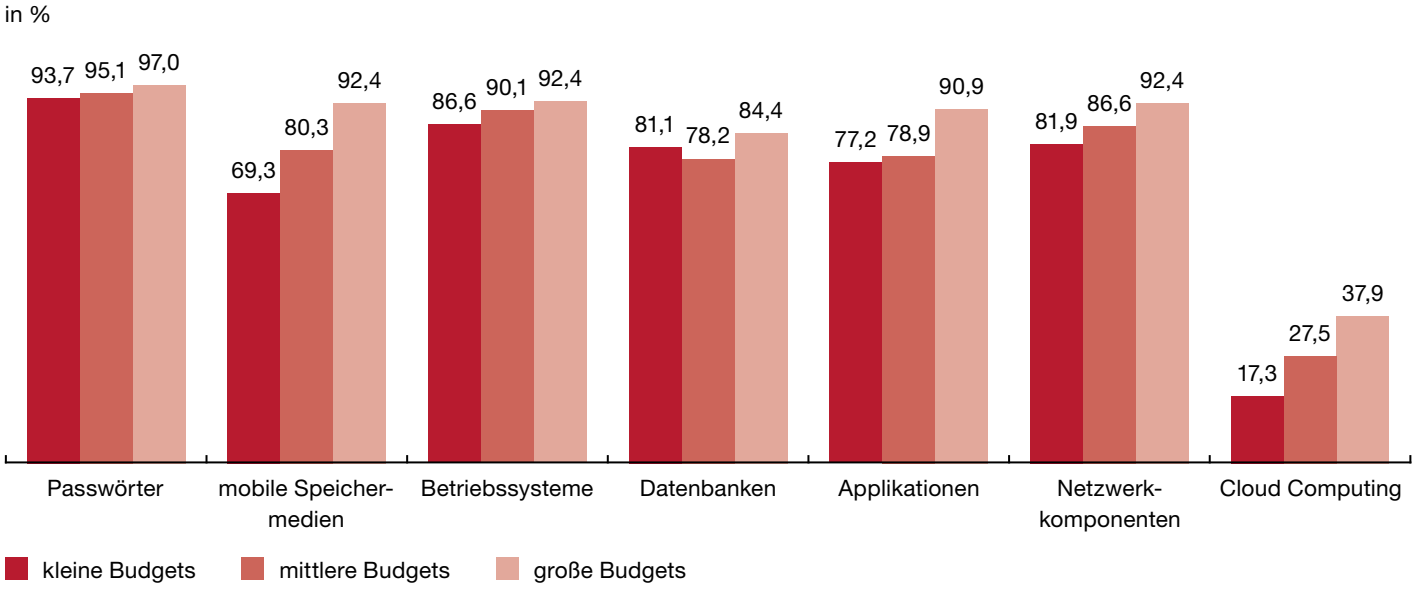
Eine weitere Möglichkeit besteht darin, bestimmte Aspekte des Sicherheitsmanagements von außen zu beziehen, beispielsweise die Überwachung der Unternehmensnetzwerke oder die Überprüfung des Informationssicherheitsprozesses beziehungsweise die Analyse des Sicherheitsniveaus durch Audits oder Penetrationstests. Allerdings verbleibt auch für den Fall einer Make-or-Buy-Entscheidung die Verantwortung für die Sicherheit der IT immer beim Unternehmen.

## 3 Richtlinien und Überwachung

Unabhängig davon, ob IT-(Sicherheits-)Leistungen vom Unternehmen selbst betrieben oder ausgelagert werden, ist es wichtig, dass das Unternehmen weiterhin die Steuerung der Informationssicherheit behält und diese auch überwacht. Eine effektive Steuerung ist nur mittels klar formulierter Richtlinien und Vorgaben für Informationssicherheit und Datenschutz möglich. Befragt nach den Bereichen, für welche die Unternehmen Sicherheitsvorgaben machen, zeigt sich, dass 95 % der Unternehmen Passwortvorgaben besitzen und 89 % Richtlinien zu den Betriebssystemen definiert haben. Am seltensten genannt wurden Sicherheitsvorgaben zu Cloud Computing (27 %). Insgesamt gibt es zwischen den mittelständischen Unternehmen und den Großunternehmen keinen wesentlichen Unterschied hinsichtlich der Zahl an definierten Richtlinien, was überrascht.

Wenn man die Zahl der Richtlinien in Abhängigkeit vom IT-Budget betrachtet, wird deutlich, dass sie von dessen Höhe abhängig ist:

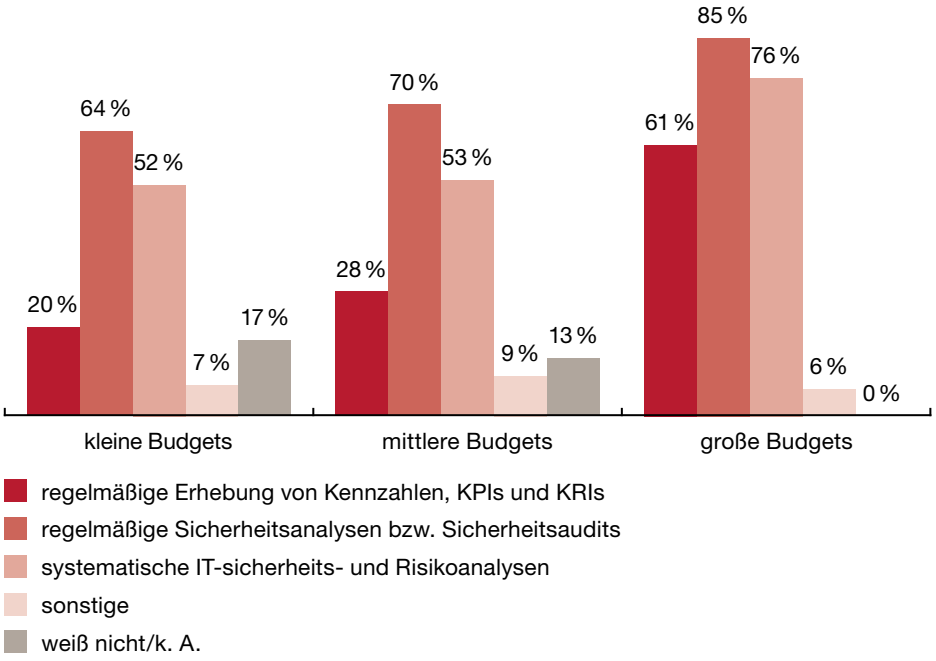
**Abb. 3 Sicherheitsrelevante Bereiche, für die Sicherheitsvorgaben definiert sind**




Insgesamt ist der Anteil der Unternehmen, die Vorgaben definiert haben, recht hoch – außer im Bereich Cloud Computing. Im Durchschnitt haben knapp 80 % der Unternehmen zu den übrigen Bereichen Vorgaben definiert, was zeigt, dass Informationssicherheit durchaus eine hohe Bedeutung beigemessen wird.

Das Definieren von Vorgaben zur Informationssicherheit ist aber nur der erste Schritt, denn zur effektiven Steuerung der Informationssicherheit muss das Unternehmen dafür sorgen, dass die Vorgaben auch durchgängig umgesetzt werden. Jedes zweite Unternehmen gab in der Befragung an, dass seine Sicherheitsrichtlinien nur teilweise umgesetzt sind. 33 % der Unternehmen gaben als Grund dafür an, dass der Prozess der Umsetzung der Richtlinien noch nicht abgeschlossen ist. 18 % nannten als Grund dafür die vorhandenen Altsysteme, bei denen die Umsetzung der Richtlinien technisch nicht möglich ist. Zur effektiven Steuerung der Informationssicherheit sind regelmäßige Erhebungen der Konfigurationen und Einstellungen notwendig. Nur wer die Einhaltung der Sicherheitsvorgaben an den Systemen überprüft, kann bei Bedarf steuernde Maßnahmen ergreifen, wie die Durchführung von Schulungen oder die Einführung einer Überwachung besonders wichtiger Einstellungen. Die Einhaltung von Sicherheitsvorgaben kann mit unterschiedlichen Maßnahmen überwacht werden. Die Zahlen zeigen, dass bei großen IT-Budgets (über 5 Mio. Euro) der Überwachungsprozess deutlich aufwendiger gestaltet wird: Wie aus Abbildung 4 ersichtlich ist, verwenden in der Gruppe der Unternehmen mit großen IT-Budgets über 60 % mindestens drei Überwachungstechniken, während von den Unternehmen mit kleinen IT-Budgets (unter 500.000 Euro) 17 % gar keine Überwachung vornehmen. Insbesondere im Mittelstand besteht somit weiterhin Nachbesserungsbedarf beim Einsatz von Werkzeugen zur Vorsorge vor und zur nachträglichen Analyse von Sicherheitsvorfällen, die anhand historischer und aktueller Analysedaten bei sicherheitsrelevanten Vorfällen bessere und schnellere Reaktionen ermöglichen.

**Abb. 4 Maßnahmen zur Überwachung der Einhaltung von Sicherheitsvorgaben**




Auch hinsichtlich des Einsatzes eines Computer-Emergency-Response-Teams (CERT) bestätigt sich dieser Trend: 76 % der Unternehmen mit kleinen IT-Budgets und 66 % der Unternehmen mit mittleren Budgets, aber nur 42 % der Unternehmen mit großen Budgets haben kein CERT etabliert, weder intern noch extern.

Somit lässt sich feststellen, dass die Bedeutung der Informationssicherheit zwar bekannt ist und entsprechende Vorgaben definiert wurden, der Grad der Umsetzung dieser Vorgaben und die Überprüfung ihrer Einhaltung jedoch insbesondere bei Unternehmen mit kleinen und mittleren IT-Budgets zu Wünschen übrig lassen.

## 4 Formal definierte Mitarbeiterstellen für die Umsetzung von IT-Sicherheitsfunktionen

Unsere Erfahrungen zeigen, dass der Stellenwert der Informationssicherheit in Unternehmen sich gut daran ablesen lässt, welche Sicherheitsfunktionen formal mit Stellenbeschreibungen in den Unternehmen verbunden sind. Die folgende Tabelle zeigt die Ergebnisse der Studie zu der Frage, ob bestimmte Rollen in Bezug auf die Informationssicherheit in den Unternehmen definiert sind.

**Abb. 5 Formal beschriebene Rollen für die Umsetzung von Sicherheitsfunktionen in den Unternehmen**

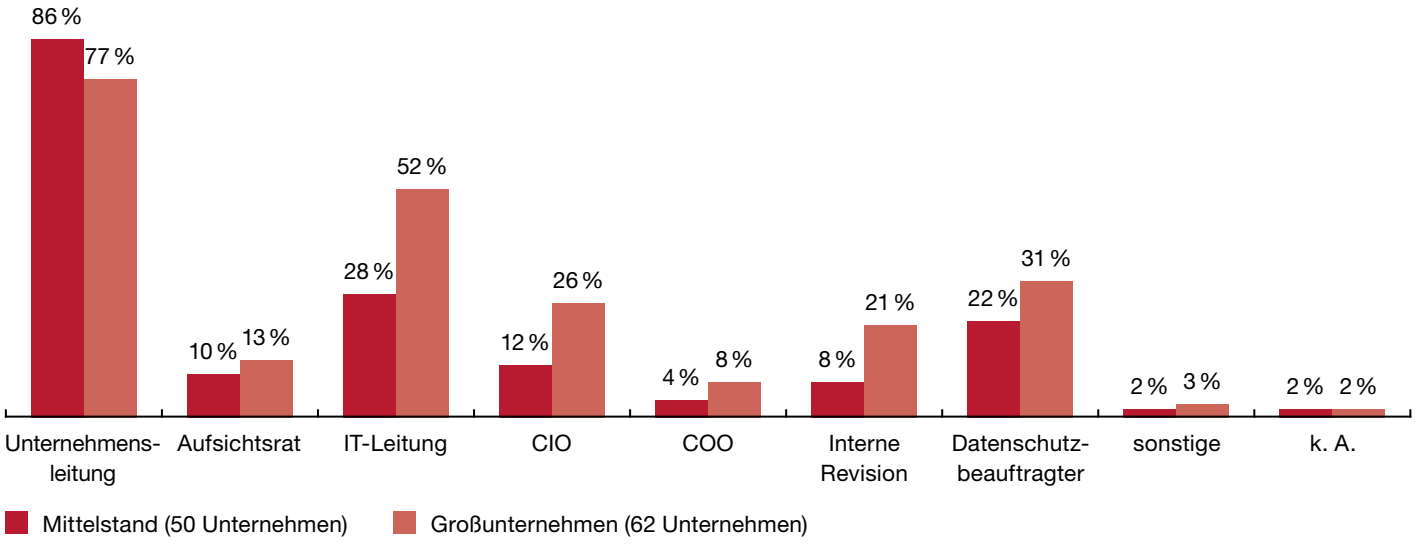
| Rolle | Umsatz < 250 Mio. | Umsatz > 250 Mio. |
|---|---|---|
| Sicherheitsadministrator | 57 % | 61 % |
| Netzwerkexperte | 54 % | 58 % |
| Sicherheitsauditor | 29 % | 48 % |
| Chief Information Security Officer (CISO) | 23 % | 48 % |
| Chief Security Officer (CSO) | 18 % | 40 % |
| k. A. | 22 % | 12 % |

Es wird deutlich, dass Rollen für den Betrieb der IT-Infrastruktur weit häufiger definiert sind als Rollen wie CISO, CSO und Sicherheitsauditor, welche die Informationssicherheit vor allem organisatorisch überwachen. Dies fällt besonders bei Unternehmen mit einem Umsatz unter 250 Millionen Euro im Jahr auf. Bemerkenswert ist auch, dass jedes fünfte Unternehmen keine Rollen für die Umsetzung der Informationssicherheit definiert.

Neben der reinen Definition einer Mitarbeiterstelle zur Informationssicherheit ist es natürlich auch entscheidend, wie deren Inhaber im Unternehmen und innerhalb der internen Berichtswege positioniert ist. Wenn es im Unternehmen einen CISO gibt, berichtet dieser häufig direkt an den Vorstand beziehungsweise die Geschäftsführung (Mittelstand: 86 %, Großunternehmen: 77 %). Seltener berichten der IT-Leiter und der Datenschutzbeauftragte direkt der Geschäftsführung. Zu berücksichtigen ist dabei, dass in mittelständischen Unternehmen aufgrund der flacheren Hierarchien meist ausschließlich an die Leitungsebene und seltener an andere Stellen berichtet wird.

**Abb. 6 Stellen im Unternehmen, an die der CISO berichtet**

Mehrfachnennungen waren möglich




Die Ergebnisse der Studie zeigen, dass das Thema Informationssicherheit längst nicht bei allen Unternehmen den Stellenwert einnimmt, den es haben sollte. Dies betrifft sowohl die Wahrnehmung der Unternehmensleitung als auch die Besetzung der Stelle des CISO bzw. CSO. Diese Stellen sind unabdingbar zur Implementierung eines effektiven ISMS. Auch die Tatsache, dass 19 % der vorhandenen CISOs nicht direkt an die Unternehmensleitung berichten, zeigt, dass Informationssicherheit in diesen Unternehmen noch nicht den notwendigen Stellenwert hat. Denn erst wenn die Unternehmensinformationen als schützenswertes Gut angesehen werden, wird auch die Informationssicherheit als Aufgabe der Unternehmensleitung bzw. des Vorstands wahrgenommen und nicht mehr als Aufgabe der IT. Diese Änderung der Wahrnehmung ist eine wesentliche Voraussetzung für die Gestaltung eines effektiven ISMS.

Aber auch wenn das Unternehmen die Wichtigkeit der Informationssicherheit erkannt hat, bedeutet dies nicht zwingend, dass eine Umsetzung auch möglich ist. Ein Grund hierfür sind fehlende Fachkräfte. Das effektive Management der Informationssicherheit in Unternehmen ist eine komplexe Aufgabe, der nur IT-Spezialisten mit der entsprechenden Qualifikation gerecht werden können. Hier hat es der Mittelstand schwer, geeignete Fachkräfte zu finden. Insgesamt fehlen laut dem Branchenverband der deutschen Informations- und Kommunikationsbranche (BITKOM) in Deutschland 39.000 IT-Experten, davon 16.000 in der ITK-Branche selbst und 23.000 in Unternehmen anderer Branchen. Mittelständische Unternehmen sind besonders stark betroffen. So entfallen rund 80 % der offenen IT-Stellen in der ITK-Branche auf den Mittelstand.

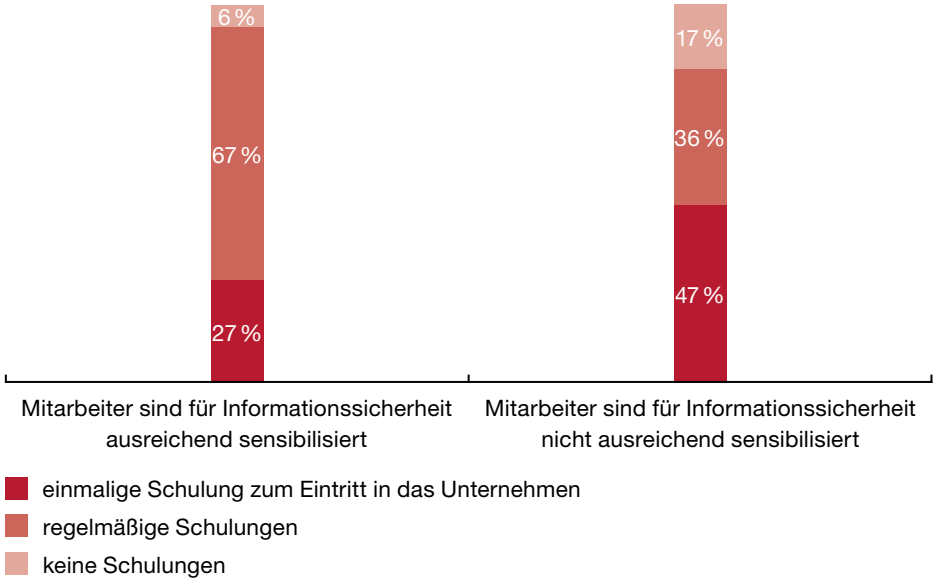
## 5 Mitarbeitersensibilisierung

Richtlinien zur Informationssicherheit und zum Schutz der IT-Systeme und Daten funktionieren nur, wenn sich die Mitarbeiter darüber bewusst sind, warum diese eingesetzt werden und welche Risiken damit vermindert werden sollen. Dieses Bewusstsein (Awareness) für die Bedeutung von Informationssicherheit muss bei den Mitarbeitern geweckt werden. Dies erfolgt häufig durch unternehmensinterne Informationskampagnen, bei denen die Mitarbeiter beispielsweise durch Plakataktionen und Flyer zu den wichtigsten Themen sensibilisiert werden sollen.

Gerade bei komplexeren Sachverhalten im Bereich der Informationssicherheit sind Schulungen ein effektiver Weg, um die Mitarbeiter des Unternehmens auf die Risiken im Umgang mit der IT und den Daten des Unternehmens aufmerksam zu machen. Allerdings wird dieser Weg immer noch von zu vielen Unternehmen nicht oder zu selten genutzt. 11 % der befragten Unternehmen schulen die Mitarbeiter gar nicht zum Thema Informationssicherheit. Weitere 37 % halten eine einmalige Schulung beim Eintritt des Mitarbeiters in das Unternehmen für ausreichend. Hier gibt es keine großen Unterschiede zwischen Mittelstand und Großunternehmen. Gerade vor dem Hintergrund sich ständig ändernder Anforderungen an die Informationssicherheit im Unternehmen ist die kleine Zahl von Unternehmen mit regelmäßigen IT-Schulungen ein klarer Hinweis darauf, dass technische und organisatorische Schutzmaßnahmen zwar implementiert werden, die Mitarbeiter und deren IT-Awareness aber nur eine untergeordnete Rolle spielen.

Die Befragung zeigt auch, dass von den Unternehmen, die ihre Mitarbeiter für ausreichend sensibilisiert für Informationssicherheit halten, 6 % gar keine Schulungen zu diesem Thema durchführen und sich 27 % auf eine einmalige Schulung beim Unternehmenseintritt eines Mitarbeiters beschränken. Auch Unternehmen, die realisiert haben, dass ihre Mitarbeiter nicht ausreichend mit den Anforderungen der Informationssicherheit vertraut sind, beschränken sich zu 47 % auf einmalige Schulungen. 17 % von ihnen führen sogar keinerlei Schulungen zur Informationssicherheit durch und vergeben somit die Möglichkeit, ihre Mitarbeiter ausreichend zu sensibilisieren. Mögliche Gründe hierfür sind zu kleine Budgets oder das Fehlen von Know-how zum Thema Informations- und Datensicherheit.

**Abb. 7 Einschätzung des Sensibilisierungsgrads der Mitarbeiter für das Thema Informationssicherheit sowie Schulungsmaßnahmen im Unternehmen**




Die Inhalte der Schulungen lassen erkennen, dass sich viele Unternehmen auf die altbekannten IT-Sicherheitsrisiken konzentrieren und neue Gefahren erst nach und nach in den Fokus nehmen. So stehen Schulungen zur Passwortsicherheit und zum Datenschutz bei den Unternehmen am höchsten im Kurs (92 % der schulenden Unternehmen), gefolgt von Schulungen zur Vorgehensweise bei konkretem Verdacht auf eine Gefährdung der Informationssicherheit (70 %) und schließlich Schulungen zum Phishing und Social Engineering (40 %).

## 6 Berücksichtigung im Budget

Auch die Ausgaben und das zur Verfügung stehende Budget für die IT im Unternehmen und speziell für die Informationssicherheit wirken sich direkt auf den Umfang der Sicherheitsmaßnahmen und -prozesse aus und zeigen den Stellenwert, den die Unternehmensleitung der Informationssicherheit beimisst.

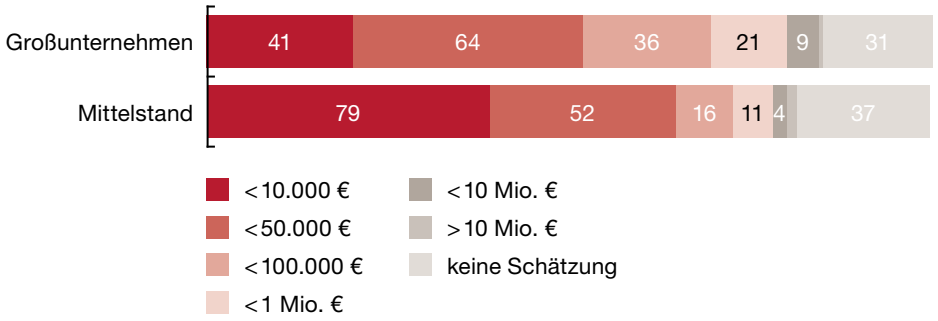
Von den 405 von PwC befragten Unternehmen haben 127 ein IT-Budget von unter 500.000 Euro, bei 142 liegt das Budget zwischen 500.000 Euro und 5 Millionen Euro und 66 Unternehmen haben ein IT-Budget von über 5 Millionen Euro.

Die Gruppe mit den größten Budgets schneidet in vielen abgefragten Bereichen der Informationssicherheit erwartungsgemäß am besten ab. 61 % von ihnen schulen ihre Mitarbeiter regelmäßig zu Informationssicherheit. Damit liegen sie deutlich vor den Unternehmen mit mittleren Budgets (51 %) und kleinen Budgets (43 %). Auch bei der Umsetzung von Sicherheitsmaßnahmen liegen die Unternehmen mit den größeren IT-Budgets vorn. 52 % von ihnen haben ihre geplanten IT-Sicherheitsmaßnahmen durchgehend umgesetzt. Von den Unternehmen mit mittleren Budgets sind es 40 % und von denen mit kleinen Budgets 43 %.

Unsere Studie zeigt einen klaren Zusammenhang zwischen den verfügbaren IT-Budgets und dem Umfang und der Qualität der IT-Sicherheitsmaßnahmen der Unternehmen. Bisher investieren gerade mittelständische Unternehmen noch wenig fokussiert in den Bereich Informationssicherheit.

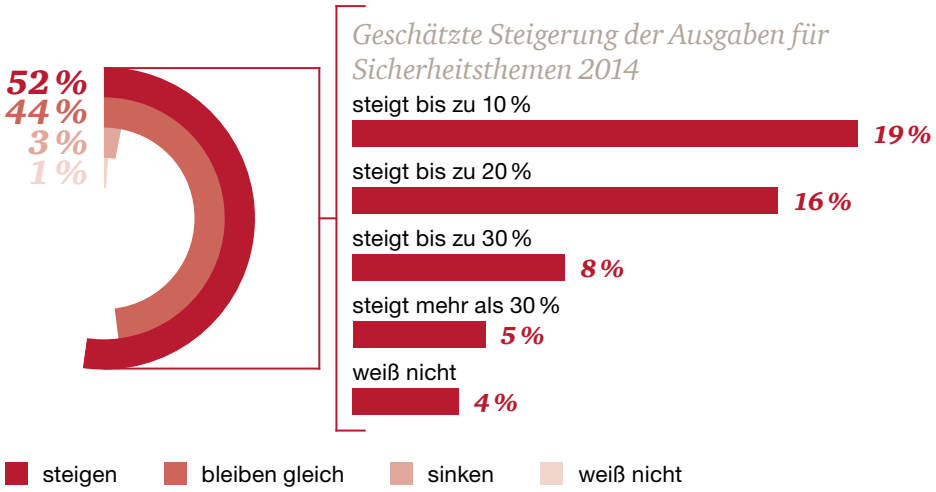
85 % der befragten Unternehmen gaben an, ein Budget von weniger als 100.000 Euro für Maßnahmen im Bereich der Informationssicherheit zur Verfügung zu haben. Vergleicht man den Mittelstand mit der Gruppe der Großunternehmen, so ergibt sich, dass nur etwa 21 % der mittelständischen Unternehmen 50.000 Euro oder mehr pro Jahr für die IT-Sicherheit aufbringen, während 39 % der Großunternehmen 50.000 Euro oder mehr aufwenden. Das Budget für Informationssicherheit verhält sich dabei proportional zum gesamten IT-Budget.

**Abb. 8 Jährliches Budget für Informationssicherheit**



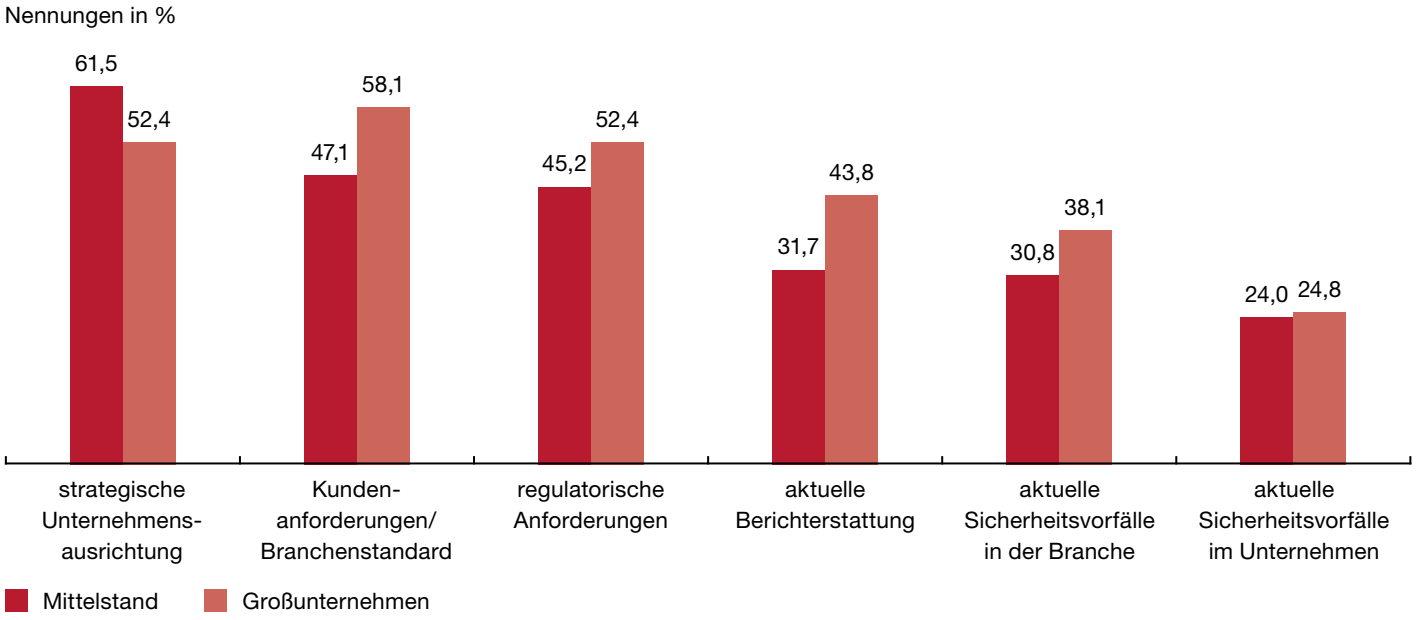

Auf die Frage, wie sich die Ausgaben für Informationssicherheit im Vergleich zu 2013 entwickeln werden, gaben 52 % der Befragten an, dass sie einen Anstieg erwarten. Nur 1 % ging davon aus, dass die Ausgaben eher sinken werden. Hinsichtlich der erwarteten Höhe der Steigerung der Ausgaben für Informationssicherheit gegenüber 2013 zeigt sich, dass der Mittelstand von stärker steigenden Kosten ausgeht. Zwar erwarten sowohl 36 % des Mittelstandes als auch 36 % der Großunternehmen Mehrausgaben von bis zu 10 %. Mit größeren Mehrausgaben rechnen aber vor allem die mittelständischen Unternehmen. 13 % von ihnen erwarten eine Steigerung um bis zu 30 %, bei den Großunternehmen sind es nur 6 %. Mit Ausgabensteigerungen über 30 % rechnet jedes dritte mittelständische Unternehmen, aber nur 13 % der Großunternehmen tun das. Hieraus lässt sich ableiten, dass aktuell besonders die mittelständischen Unternehmen erkennen, dass die Informationssicherheit zunehmend an Bedeutung gewinnt und dass sie andererseits einen großen Nachholbedarf haben, der Investitionen mit entsprechenden Kosten erforderlich macht.

**Abb. 9 Geschätzte Entwicklung der Ausgaben für Informationssicherheit 2014**




Die Gründe für die Mehrausgaben für Informationssicherheit werden von Mittelstand und Großunternehmen tendenziell ähnlich gewichtet, wie die folgende Abbildung zeigt.

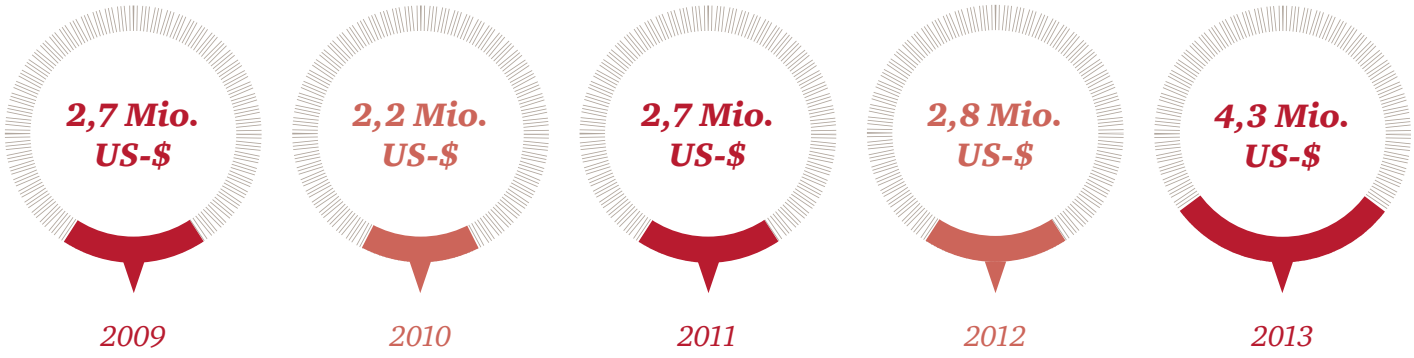
**Abb. 10 Gründe für Mehrausgaben für Informationssicherheit**



Es wird deutlich, dass externe Faktoren, wie beispielsweise Branchen- oder Kundenanforderungen, sowie übergreifende interne Anforderungen, wie die strategische Ausrichtung, weit häufiger als Gründe für steigende Mehrausgaben gesehen werden als tatsächliche IT-Sicherheitsvorfälle. In Verbindung mit einem anderen Ergebnis dieser Studie (siehe Abb. 4), dass nämlich nur 60 % der Unternehmen mit großen IT-Budgets – und weniger als 30 % der Unternehmen mit mittleren und kleinen IT-Budgets – regelmäßig Sicherheitskennzahlen erheben und auswerten, ergeben sich allerdings Zweifel, ob die Unternehmen die eigenen IT-Sicherheitsvorfälle überhaupt zuverlässig erkennen können und ob diese demnach in ihre Investitionsentscheidungen einfließen.

Der Trend, mehr Budget für IT Sicherheit bereitzustellen, wird nicht nur in den auf deutsche Unternehmen bezogenen Ergebnissen dieser Studie, sondern auch im *Global State of Information Security Survey* auf internationaler Ebene deutlich. Die Abbildung 11 stellt die Entwicklung des durchschnittlichen Informationssicherheitsbudgets von Großunternehmen seit 2009 dar. Aus der Abbildung geht hervor, dass 2013 eine signifikante Steigerung des Budgets (51 %) gegenüber 2012 zu verzeichnen gewesen ist. Auch wenn im deutschen Mittelstand ein ähnlicher Trend festgestellt werden kann, bleibt die durchschnittlich erwartete Steigerung der Budgets im deutschen Mittelstand (ca. 10 %) deutlich hinter den weltweiten Entwicklungen des letzten Jahres zurück. Der Vergleich verdeutlicht die Zwickmühle, in der sich viele mittelständischen Unternehmen befinden: Einerseits steigt die Bedeutung der Informationssicherheit und die Unternehmen müssen in die Informationssicherheit investieren. Auf der anderen Seite lassen die straffen Budgets ähnlich hohe Investitionen wie im internationalen Vergleich nicht zu.

**Abb. 11 Internationale Entwicklung der durchschnittlichen IT-Sicherheitsbudgets**




Quelle: PwC US (Hg.), Defending yesterday – Key findings from The Global State of Information Security® Survey 2014, S. 14.

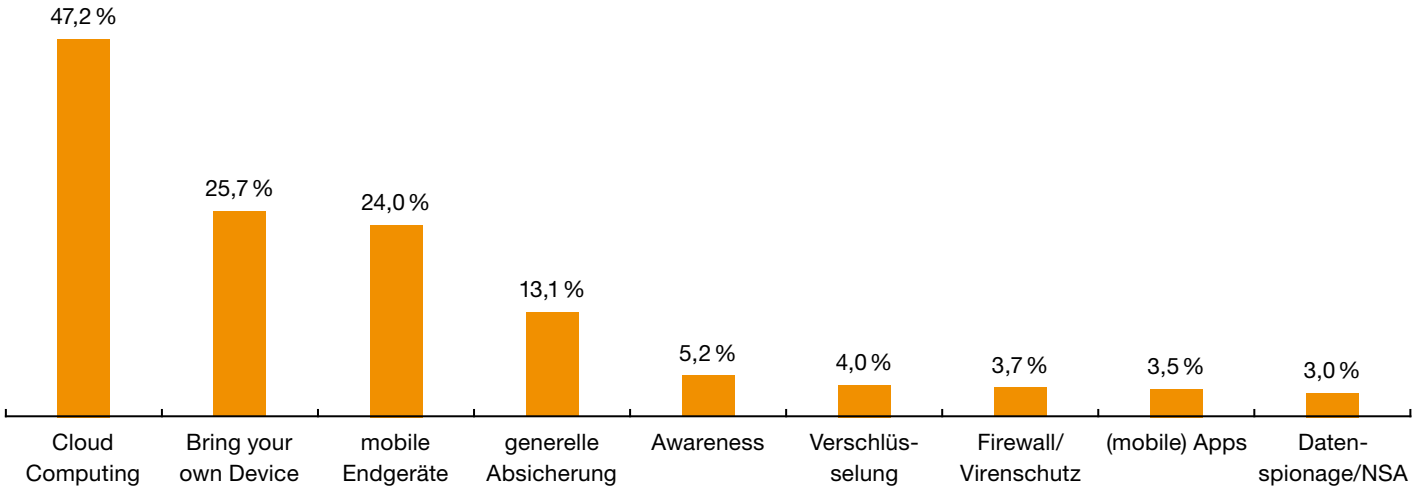
# E Trends und deren Auswirkungen auf die Informationssicherheit

Derzeit stehen die Unternehmen im Bereich IT-Sicherheit vor einer Vielzahl neuer Herausforderungen. Neue Technologien verändern die IT-Nutzungskultur sehr stark. Cloud Computing und Smartphones sind die Megatrends der 2010er-Jahre und haben sich mittlerweile so stark am Endanwendermarkt durchgesetzt, dass selbst Unternehmen, für die IT nicht Kern des Geschäftsmodells ist, sich damit auseinandersetzen müssen. Auch die zunehmende Digitalisierung, beispielsweise in den Bereichen Zahlungsmethoden, Banking und Marketing bringt neben einer Vielzahl von Möglichkeiten auch Herausforderungen für den Schutz der IT-Systeme und der Daten im Unternehmen mit sich.

Auf die Frage nach den IT-Themen, die in den kommenden fünf Jahren die größte Relevanz für die Informationssicherheit gewinnen werden, wählten die Unternehmen am häufigsten die Antwortmöglichkeiten Cloud Computing (47 %), Bring your own Device (26 %) und mobile Endgeräte (24 %). Diese Techniken werden mittlerweile wie selbstverständlich von Kunden und auch von Mitarbeitern genutzt, können allerdings die IT-Sicherheit im Unternehmen stark gefährden. Die Relevanz klassischer IT-Sicherheitsthemen wird im Vergleich dazu als deutlich geringer eingeschätzt, beispielsweise wurde das Thema Awareness nur von 5 % der Befragten genannt und nur 4 % nannten das Thema Firewall/Virenschutz. Diese Themen sind mittlerweile bekannt und werden aus Sicht der Unternehmen ausreichend beherrscht. Vor dem Hintergrund, dass, wie oben beschrieben, 17 % der befragten Unternehmen ihre Mitarbeiter gar nicht und 37 % sie nur beim Eintritt in das Unternehmen einmalig zum Thema Informationssicherheit schulen, verdeutlicht die Einschätzung, dass die Unternehmen die Bedeutung einer angemessenen und kontinuierlichen Sensibilisierung der eigene Mitarbeiter weiterhin unterschätzen. Dies ist umso bedauerlicher, da diese häufig auch automatisiert umsetzbare Maßnahme einen hohen Wirkungsgrad erreicht, aber im Vergleich zu einigen technischen Lösungen mit weit moderaterem Aufwand realisiert werden könnte.

**Abb. 12 IT-Themen, die in den kommenden fünf Jahren die größte Relevanz für die Informationssicherheit haben werden**

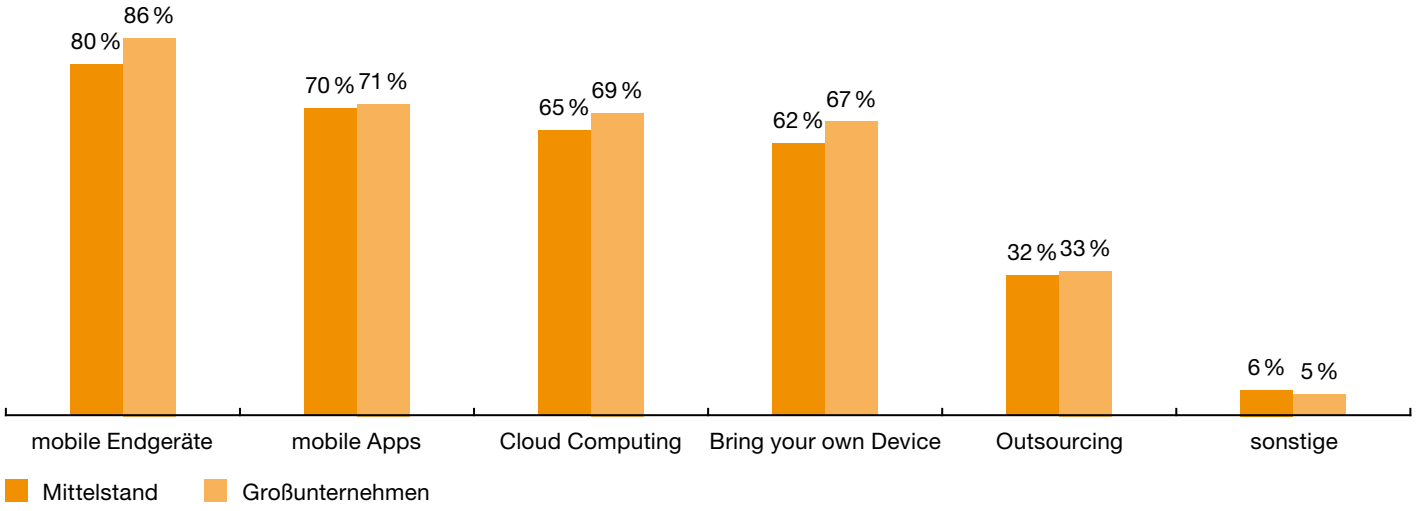
Mehrfachnennungen waren möglich



Neben der Frage nach der zukünftigen Relevanz der Themen wurde auch untersucht, welche Bereiche die größten Sicherheitsrisiken mit sich bringen. Hier zeigt sich bei Mittelständlern und Großunternehmen ein ähnliches Bild. Am risikoreichsten schätzen die Unternehmen demnach mobile Endgeräte wie Smartphones oder Tablets ein (Mittelstand 80 %, Großunternehmen 86 %). Danach folgen mobile Apps, Cloud Computing und Bring-your-own-Device-Ansätze. Mit deutlichem Abstand nannten Mittelstand und Großunternehmen das Outsourcing (32 %). Ein möglicher Grund hierfür ist, dass viele Unternehmen schon Erfahrung mit der Auslagerung bestimmter Unternehmensbereiche und den damit zusammenhängenden Risiken für die Informationssicherheit haben.

**Abb. 13 Besonders risikoreiche Trends aus Sicht der Informationssicherheit**

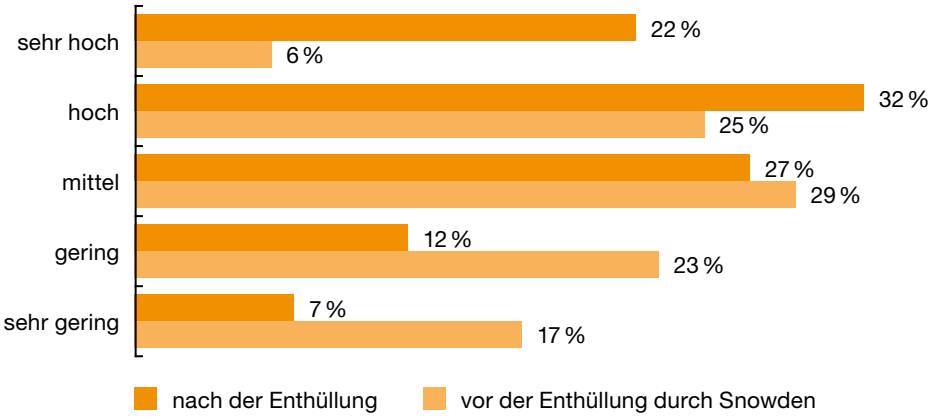
Welche Trends sind vor dem Hintergrund der Informationssicherheit besonders risikoreich?
Mehrfachnennung waren möglich




Auch hier lohnt sich ein Blick auf die Zusammenhänge zwischen dem wahrgenommenen Risiko, das mit den Trends verbunden ist, und dessen Wiederspiegelung in den Strategien und Maßnahmen der Unternehmen. So haben lediglich 28 % derjenigen, die Cloud Computing im Unternehmen als Risiko betrachten, dieses Thema auch in ihre Sicherheitsvorgaben aufgenommen.

Die von PwC publizierte Studie *Wirtschaftskriminalität und Unternehmenskultur* geht genauer auf das wahrgenommene Risiko bei der Nutzung von Cloud-Dienstleistungen ein und verknüpft die Ergebnisse mit den kürzlich erfolgten Veröffentlichungen zur NSA-Spähaffäre. Anhand der nachfolgenden Abbildung 14 wird deutlich, wie stark sich die Wahrnehmung der Sicherheit von Cloud Computing in den befragten Unternehmen geändert hat. Während vor den Veröffentlichungen zur Spähaffäre noch 6 % meinten, mit Cloud Computing sei ein sehr hohes Betrugs- und Missbrauchsrisiko verbunden, stieg diese Zahl nach den Enthüllungen auf 22 %.

**Abb. 14 Risiko von Betrug und Missbrauch bei der Nutzung von Cloud Computing[1]**




[1] in Anlehnung an PwC, Wirtschaftskriminalität und Unternehmenskultur 2013, S. 19.

Die Einstellung deutscher Unternehmen zu den Risiken aktueller Trends in der IT beeinflusst auch die Nutzung dieser neuen Technologien. So gaben 77 % der Befragten an, dass Sicherheitsrisiken dazu führen, dass neue Technologien deutlich verzögert eingeführt werden. Hierbei gibt es keinen Unterschied zwischen dem Mittelstand und Großunternehmen.

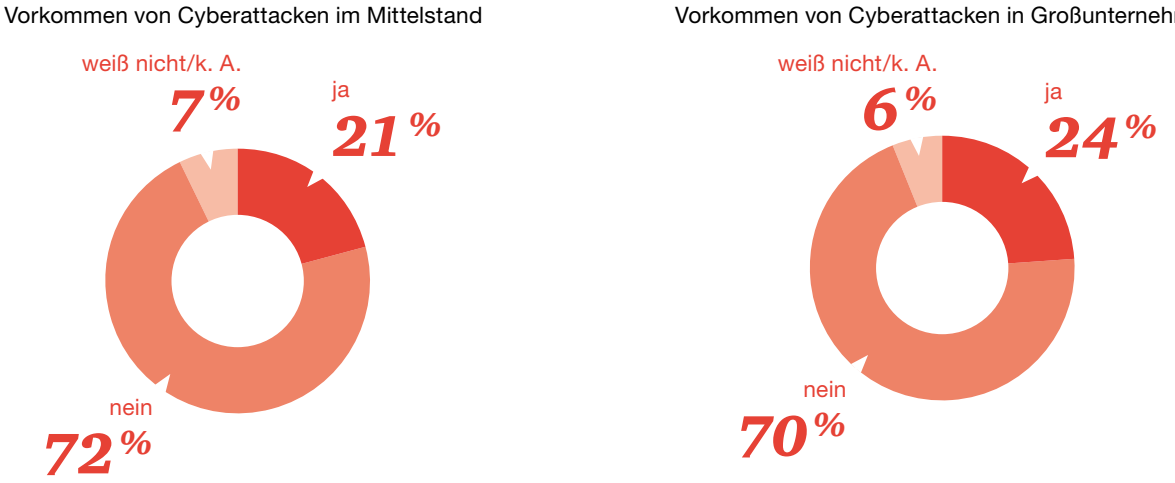
# F Cyberattacken

## 1 Auftreten von Attacken

Das Internet stellt heute für die meisten Unternehmen im Rahmen ihrer Geschäftstätigkeit die zentrale Kommunikationsader dar, um sich innerhalb des Unternehmens selbst, mit Kunden und mit Zulieferern abzustimmen. Das Portfolio reicht dabei von der einfachen Präsentation des Unternehmens auf einer Internetseite über Onlineshop-Lösungen bis hin zur automatischen Abwicklung von Bestellungen beim Zulieferer. Die Internetnutzung schafft allerdings auch neue Angriffspunkte für Kriminelle. Die Zahl von Hackerangriffen, Viren und Phishing-Versuchen steigt ständig. Gelungene Angriffe auf die Unternehmens-IT treffen immer prominentere Opfer. Die Folge sind nicht nur direkte, finanzielle Schäden, sondern auch Imageschäden, vor allem dann, wenn dabei personenbezogene oder geheime Daten gestohlen oder veröffentlicht werden.

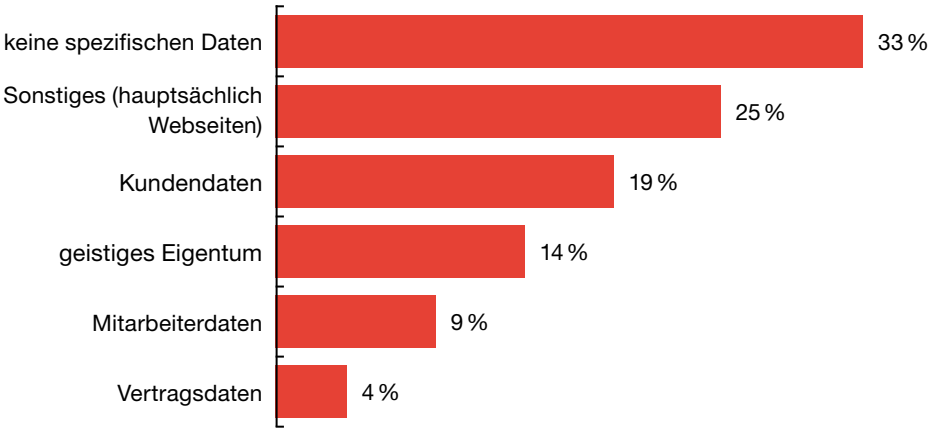
Inwieweit Cyberattacken auch mittelständische Unternehmen betreffen, wurde im Rahmen der Studie mithilfe mehrerer Fragen untersucht. Annähernd 16 % der Unternehmen mit einem Umsatz unter 250 Millionen Euro gaben an, schon einmal Opfer eines solchen Angriffes gewesen zu sein. Bei den Unternehmen mit einem Umsatz über 250 Millionen Euro waren es sogar 33 %. Dieser höhere Wert ist vor dem Hintergrund, dass Unternehmen mit einem höheren Umsatz ein potenziell lohnenswerteres Ziel darstellen und somit das Interesse von Angreifern an ihnen größer ist, plausibel. Die Zahlen verdeutlichen darüber hinaus, dass Mittelständler ähnlich im Fokus von Angriffen stehen wie Großunternehmen. So waren von den befragten mittelständischen Unternehmen insgesamt 21 % bereits Opfer einer Cyberattacke; bei den Großunternehmen waren es 24 %.

**Abb. 15 Vorkommen von Cyberattacken**



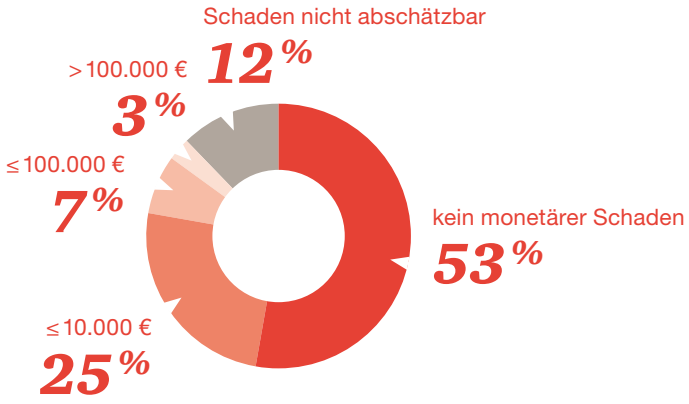

Bei der Frage, ob sie Ziel von Cyberangriffen geworden sind, wählten die Befragten am häufigsten die Antworten „keine spezifischen Daten“ und „Sonstiges“. Eine mögliche Begründung hierfür ist, dass im Nachhinein oft nur schwer nachvollziehbar ist, welche Daten Ziel des Angriffs waren. Diese Antworten weisen aber auch darauf hin, dass die Nachbereitung sowohl von erfolgreichen als auch von erfolglosen Angriffen auf die Unternehmens-IT noch nicht in jedem Unternehmen zu den Standardabläufen in der Informationssicherheit gehört. Dies scheint vor allem auf den Mittelstand zuzutreffen, was daraus abzulesen ist, dass sich die Antworten auf Fragen nach den konkret betroffenen Datentypen sehr von denen der Großunternehmen unterscheiden. So gaben 14 % der Großunternehmen an, dass Mitarbeiterdaten Ziel der Angriffe waren, im Mittelstand antworteten so nur 2 %. Auf Kundendaten hatten es die Angreifer bei 22 % der angegriffenen Groß-unternehmen abgesehen, bei mittelständischen Unternehmen waren es nur 14 %.

**Abb. 16 Häufigsten Ziele von Cyberattacken**



Der Schaden durch einen Cyberangriff wird von den Unternehmen unterschiedlich eingeschätzt wie die Abbildung 17 zeigt. Die Hälfte der Befragten glaubt demnach, dass durch die Angriffe kein monetärer Schaden entstanden ist. Doch sind bei solchen Angriffen Imageverluste gegenüber Kunden und Geschäftspartnern zu befürchten, die man nicht leicht quantifizieren kann. 35 % der mittelständischen Unternehmen, die schon einmal Opfer einer Cyberattacke geworden sind, gaben die Höhe des Schadens durch diese Attacke mit bis zu 100.000 Euro an. Ein Mittelständler gab an, mit einem Gesamtschaden von über einer Million Euro konfrontiert worden zu seien, der durch Informationssicherheitsvorfälle verursacht worden ist.

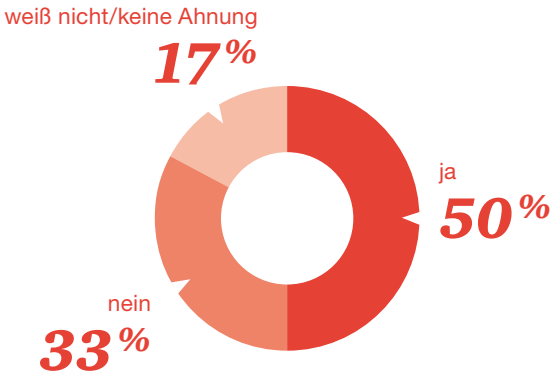
**Abb. 17 Finanzieller Schaden durch Cyberattacken**



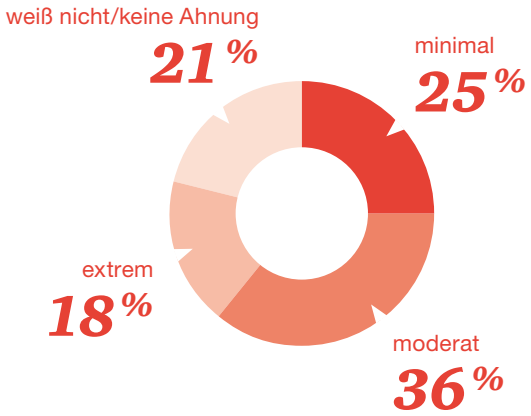

Ein ähnliches Bild wie bei den Angriffen von außen auf die Unternehmens-IT zeigt sich bei Gefahren innerhalb des Unternehmens. Zahlreiche Unternehmen haben bisher keine oder nur ineffektive Strategien, um auf Insider-Gefahren zu reagieren. Dies hat auch die von PwC im Frühjahr 2013 in den USA durchgeführte Studie *2013 US State of Cybercrime Survey* bestätigt, deren Ergebnisse in Abbildung 18 gezeigt werden.

**Abb. 18 Ergebnisse des Cybercrime Survey – Vorhandensein von Strategien gegen Insider Security Incidents in den Unternehmen**

Hat Ihr Unternehmen eine Strategie, um auf Insider Security Incidents zu reagieren ?




Wie effektiv ist Ihr Unternehmen bei der Erfassung und dem Umgang mit internen Sicherheitsverstößen sowie beim Ableiten von Gegenmaßnahmen?



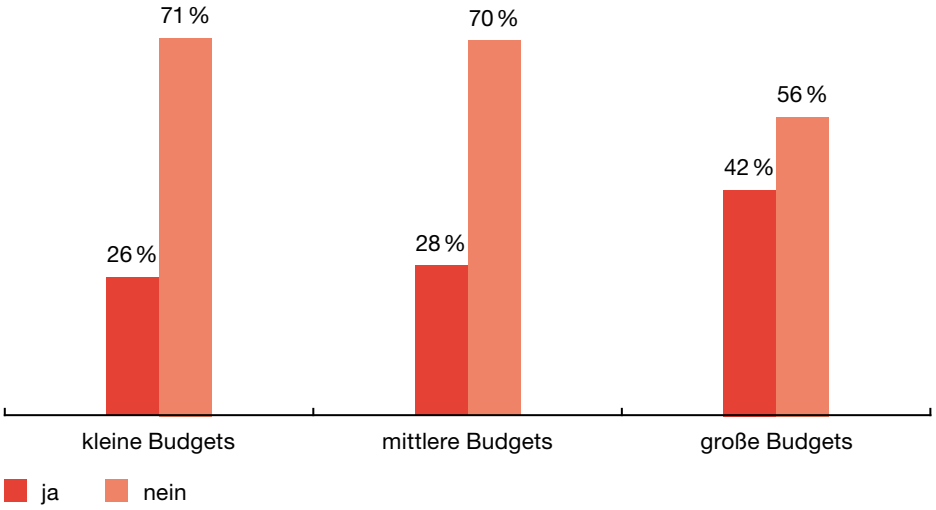

Quelle: PwC USA (Hg.), „http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/us-state-of-cybercrime.pdf“ 2013 US State of Cybercrime Survey, S. 11.

## 2 Reaktion auf PRISM und Tempora

Im Jahr 2013 wurde durch Enthüllungen des ehemaligen Geheimdienstmitarbeiters Edward Snowden bekannt, dass die amerikanischen und britischen Nachrichtendienste NSA und GCHQ im Rahmen der Programme PRISM und Tempora global Verbindungsdaten anlassunabhängig auf Vorrat speichern. Hiervon sind sowohl Metadaten als auch Verbindungsinhalte betroffen. Die Daten werden mittels geheimer Gerichtsbeschlüsse bei Providern erhoben oder an zentralen Punkten des Netzwerks, wie beispielsweise Überseekabeln, abgezapft.

Wie die Befragung zur Informationssicherheit im Mittelstand ergab, fühlen sich viele deutsche Unternehmen gerade aufgrund dieser Vorkommnisse verunsichert. So gaben 28 % der mittelständischen Unternehmen und 32 % der Großunternehmen an, dass die bekannt gewordenen Datensammlungen einen Einfluss auf ihre zukünftige Sicherheitsstrategie haben werden. Die Antworten zeigen, dass vor allem Unternehmen mit hohem IT-Budget (über 5 Mio. Euro) ihre Strategie ändern wollen, während 71 % der Unternehmen mit einem IT-Budget von unter 500.000 Euro dafür keine Veranlassung sehen. Ein Grund für ihre Untätigkeit könnte aber auch darin liegen, dass sich eine Veränderung der Sicherheitsstrategie auf viele Bereiche der IT-Infrastruktur auswirkt und entsprechend teuer ist.

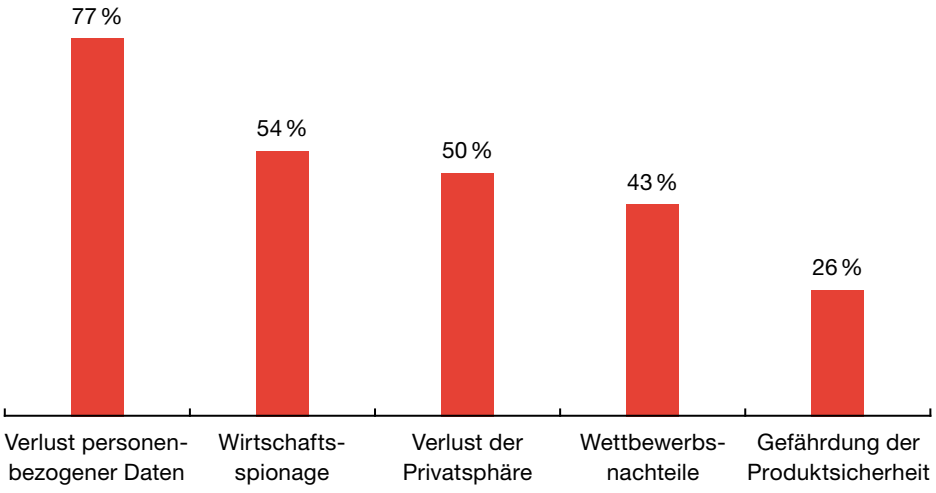
**Abb. 19 Einfluss von PRISM und Tempora auf die Sicherheitsstrategie**




29 % der befragten Unternehmen gehen davon aus, dass sie selbst Opfer von PRISM oder Tempora geworden sind. Als mögliche Folgen nannten sie am häufigsten den Verlust personenbezogener Daten (77 %), gefolgt von Wirtschaftsspionage (54 %) und einen Verlust der Privatsphäre (50 %). Auch hier weichen die Ergebnisse von mittelständischen Unternehmen und Großunternehmen nur leicht voneinander ab. Ein mit 43 % großer Teil der Unternehmen befürchtet auch Wettbewerbsnachteile, da zum Befragungszeitpunkt schon die Möglichkeit im Raum stand, dass geheimdienstliche Abhörmaßnahmen auch der Wirtschaftsspionage dienen. Mittlerweile wird offen kommuniziert, dass die Abhörmaßnahmen auch zur Wirtschaftsspionage genutzt werden, sodass die Bedeutung der Informationssicherheit in den Unternehmen weiter zugenommen haben dürfte.

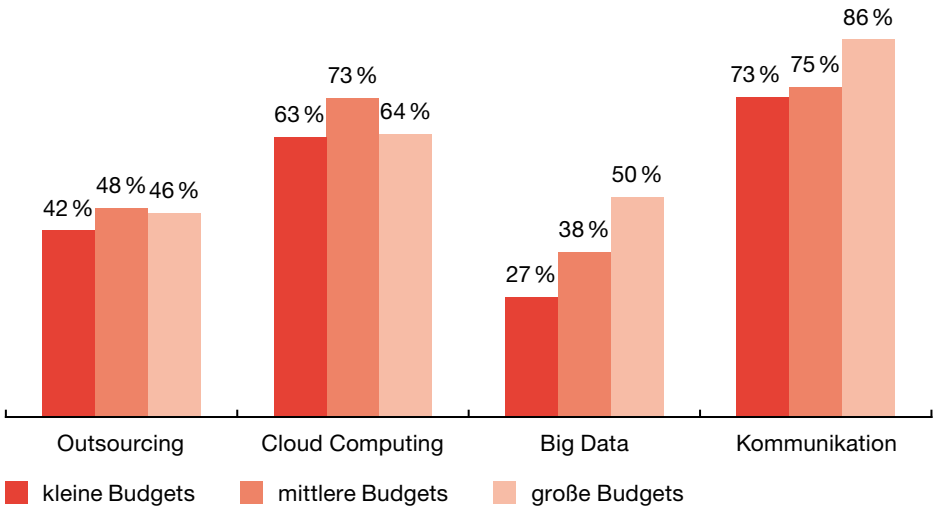
**Abb. 20 Häufigkeiten der Nennung von möglichen Folgen von PRISM und Tempora für die Unternehmen**

Mehrfachnennung waren möglich



Infolge der neuen Erkenntnisse aus den bekannt gewordenen Spähaktionen werden viele Konzepte der betroffenen Unternehmen neu überdacht und angepasst. Großer Bedarf dafür wird vor allem in den Bereichen Technologien der Kommunikation mit Partnern und Kunden (74 %), Cloud Computing (63 %) und Outsourcing (43 %) gesehen. Diese Zahlen zeigen den großen Einfluss der Abhörprogramme auf die deutschen Unternehmen, da mit Cloud Computing und Outsourcing gleich zwei wesentliche Themen sehr häufig genannt wurden.

**Abb. 21 Bereiche, die aufgrund der PRISM und Tempora Enthüllungen zukünftig überdacht werden**




Im Rückblick auf ihre Einschätzung vor dem Bekanntwerden der Spähprogramme geben 77 % der befragten Unternehmen an, dass sie ihre IT-Risikobewertung nach wie vor als angemessen einschätzen und damit der Meinung sind, die Abhörmaßnahmen in ihrer IT-Risikobewertung bereits angemessen zu berücksichtigen. Diese Zahl scheint allerdings zu hoch zu sein, vor allem vor dem Hintergrund, dass, wie in Abbildung 21 dargestellt, viele Unternehmen noch Bedarf an der Überarbeitung verschiedener grundlegender Bereiche wie Kommunikation, Cloud Computing oder Outsourcing haben, die durchaus wesentlichen Einfluss auf die zugrunde liegende IT-Infrastruktur haben. So planen 27 % der Befragten, zukünftig Maßnahmen zum Schutz vor verdeckten behördlichen Datenzugriffen zu ergreifen, wobei nur 32 % der Meinung sind, dass es möglich ist, sich überhaupt ausreichend dagegen zu schützen. Hier sind die mittelständischen Unternehmen mit 37 % etwas optimistischer.

Auf die Frage, welches die schwerwiegendere Bedrohung der Informationssicherheit sei, antworteten nur 5 % der Befragten mit „Abhörprogramme aus dem angelsächsischen Raum“. Bedrohlicher eingeschätzt wurden Cyberattacken aus Asien (17 %) und aus Osteuropa (8 %). Mehr als zwei Drittel der Befragten schätzen das Risiko, von amerikanischen oder westeuropäischen Geheimdiensten abgehört zu werden, genauso hoch ein wie das Risiko von Cyberattacken aus Asien und Osteuropa.

# G Reaktion des Gesetzgebers

## 1 Staatliche Motivation

Die Regierungen haben erkannt, dass IT-Sicherheit auf nationaler wie internationaler Ebene zur zentralen Herausforderung für Staat, Wirtschaft und Gesellschaft geworden ist. Angriffe auf IKT-Infrastrukturen haben in den letzten Jahren zugenommen und weisen gleichzeitig eine größere Komplexität und Professionalität auf. Kriminelle, terroristische und nachrichtendienstliche Akteure missbrauchen die Offenheit des Internets und machen vor Landesgrenzen nicht halt. Auch wichtige industrielle Infrastrukturbereiche sind zunehmend gefährdet.

Aus diesen Gründen hat das Bundesministerium des Innern eine Cyber-Sicherheitsstrategie für Deutschland entwickelt. Zu den Zielen dieser Strategie zählt der Schutz kritischer Infrastrukturen in den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur. Ferner ist mit der Cyber-Sicherheitsstrategie beabsichtigt, die Sicherheit der IT-Systeme der Bürgerinnen und Bürger sowie der kleinen und mittelständischen Unternehmen zu erhöhen. So hat das Bundesministerium für Wirtschaft und Technologie unter Beteiligung der Wirtschaft eine Taskforce „IT-Sicherheit in der Wirtschaft“ eingerichtet. Weiterhin sollen die IT-Sicherheit in der öffentlichen Verwaltung gestärkt, ein nationales Cyber-Abwehrzentrum und ein nationaler Cyber-Sicherheitsrat eingerichtet und die Zusammenarbeit auf internationaler Ebene verstärkt werden.

Ein wesentlicher Baustein der Cyber-Sicherheitsstrategie ist das geplante *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*, welches das Ziel verfolgt, die IT-Sicherheit bei Betreibern kritischer Infrastrukturen durch die Zusammenarbeit von Staat und Betreibern zu verbessern und sicherzustellen, dass sie ein Mindestniveau erreicht.

## 2 Internationale Initiativen

Informationssicherheit ist natürlich nicht nur ein Thema für deutsche Unternehmen, sondern steht global im Fokus des Interesses. Nach und nach sind internationale Initiativen und Institute entstanden, welche die Unternehmen beim Schutz ihrer Informationen unterstützen. Die wohl bekannteste Zusammenfassung von Standards rund um das Thema IT- und Informationssicherheit ist die ISO-27000-Familie, allen voran die Norm ISO 27001. Diese beschreibt die Anforderungen an die Organisation der Sicherheit einer IT-Infrastruktur. Ziel ist die Erstellung eines dokumentierten ISMS, aus dem alle für die Sicherheit der Informationssysteme relevanten Informationen ersichtlich sind. Unternehmen können sich von ausgewählten Auditoren nach ISO/IEC 27001 zertifizieren lassen. Zertifizierungen nach weiteren Modulen der ISO-27000-Familie sind im Einzelfall möglich; diese Erweiterungen bieten detailliertere Informationen und Rahmenwerke zum Thema der IT-Sicherheit.

Die Umsetzung der Anforderungen der ISO 27001 gewährleistet ein standardisiertes Vorgehens zu Definition, Umsetzung und Kontrolle der Schutzmaßnahmen für die IT-Infrastruktur. Der Status „ISO/IEC-27001-zertifiziert“ kann gegenüber Kunden als Gütesiegel für diese Umsetzungsbemühungen kommuniziert werden. Die Zertifikate müssen regelmäßig erneuert werden, um den Status zu erhalten. ISO/IEC 27001 geht auch auf neue Herausforderungen ein. Die letzte Anpassung erfolgte 2013.

Neben internationalen Standards gibt es auch Initiativen und Organisationen, die ihre Aktivitäten auf bestimmte geografische Gebiete beschränken. So gibt es Programme wie European Programme for Critical Infrastructure Protection (EPCIP) und Organisationen wie European Network and Information Security Agency (ENISA), die in erster Linie auf die Sicherheit in der Informationstechnik in Europa abzielen.

Das EPCIP definiert Strategien zum Schutz von kritischen Infrastrukturen gegen terroristische Angriffe. Unter kritischen Infrastrukturen werden jene verstanden, deren Ausfall oder Zerstörung nationale oder internationale Schäden verursachen kann, zum Beispiel ein Atomkraftwerk. Die Ergebnisse des Programmes sind im Dokument EU COM (2006) 786 zusammengefasst.

ENISA ist zuständig für die Netz- und Informationssicherheit in der Europäischen Union. Sie unterstützt die Europäische Kommission und die Mitgliedsstaaten bei Sicherheitsfragen zur IT mit dem Ziel, die Zusammenarbeit der Akteure zu verbessern. ENISA berücksichtigt in ihren Empfehlungen aktuelle Risikoanalysen. Neben Empfehlungen zum Schutz von kritischen Infrastrukturen und zu Cloud-Diensten werden auch praktische Empfehlungen für den Einsatz aktueller kryptographischer Verfahren gegeben.

In den USA übernimmt die Rolle des Standardsetzers, unter anderem im Bereich Informationstechnologie, das National Institute of Standards and Technology (NIST). NIST-Richtlinien im Bereich Informationstechnologie werden häufig international anerkannt. Das NIST stellt Standards, Metriken und Tests zum Messen und Validieren von Informationssystemen und Informationsservices bereit. Außerdem ist das NIST für die Auswahl und Verbreitung sicherer Verschlüsselungsverfahren in der IT zuständig. In 2013 gerieten vom NIST standardisierte Verschlüsselungsverfahren allerdings in den Verdacht, Schwachstellen zu besitzen, die von Geheimdiensten systematisch ausgenutzt werden können.

Neben den geografisch orientierten Organisationen gibt es eine Vielzahl von Initiativen für spezielle Technologien und Trends in der Informationstechnik. Als ein Beispiel soll hier die Cloud Security Alliance (CSA) genannt werden, die Best Practices zur Erreichung von Sicherheitszielen im Bereich Cloud Computing fördert. Dazu unterstützet die CSA beispielsweise das NIST und die Europäische Kommission bei der Definition von Sicherheitsrichtlinien im Cloud-Bereich. Außerdem bietet sie Schulungen und Zertifizierungen im Bereich Cloud Computing an, bei denen auch allgemeine Informationen zur IT-Sicherheit vermittelt werden.

## 3 Nationale Gesetze

Neben den internationalen Programmen und Organisationen haben viele Länder ihre eigenen Behörden, Vereine und Gesetze zum Thema Informationssicherheit. Die erste Adresse zur Informationssicherheit in Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik. Die 1991 gegründete Behörde bildet den Sammelpunkt für die meisten Initiativen zur Informationssicherheit in Deutschland. Das BSI informiert Bürger und Unternehmen über sämtliche Themen zur IT-Sicherheit, unter anderem auch über Cybersicherheit und Sicherheit bei neuen Technologien wie Cloud Computing. Eines der größten Produkte des BSI ist der IT-Grundschutzkatalog, eine Sammlung von Richtlinien, welche sich an der ISO 27001 orientiert und diese um praktische Umsetzungsmaßnahmen erweitert. Ein solches Rahmenwerk zur Informationssicherheit ist international bisher einzigartig.

Auch das Bundesministerium für Wirtschaft und Energie (BMWi) befasst sich mit dem Thema Informationssicherheit und Schutz vor Cyberattacken. So wurde 2011 die Taskforce „IT-Sicherheit in der Wirtschaft“ ins Leben gerufen, um KMUs bei der Erhöhung ihres IT-Sicherheitsniveaus zu unterstützen. Hierfür hat die Taskforce konkrete Informationen und Services zusammengetragen, bei denen es sich meist um Angebote, Veranstaltungen und Veröffentlichungen von Initiativen und Verbänden handelt. Unter bestimmten Umständen übernimmt die Taskforce bzw. das BMWi auch die gezielte Förderung von gemeinnützigen IT-Sicherheitsprojekten. Darüber hinaus stellt die Taskforce auf ihrer Website selbst Informationen und Tipps zur Verbesserung der IT-Sicherheit bereit. Dazu zählen unter anderem Poster zur Sensibilisierung der Mitarbeiter für den sicheren Umgang mit der IT und mit elektronischen Daten, die kostenlose Überprüfung der Website eines KMU auf Schadprogramme sowie Hilfestellung bei der Beseitigung etwa vorhandener Malware.

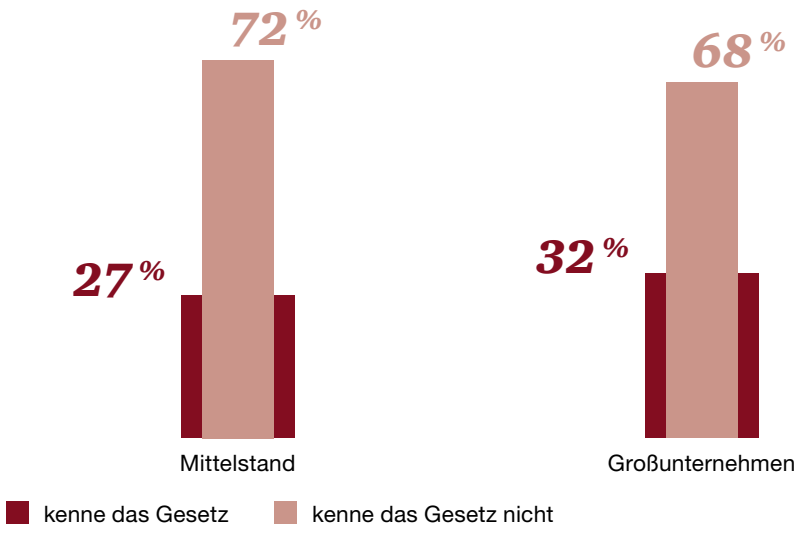
Neben diesen beiden Organisationen gibt es eine Vielzahl weiterer Initiativen und Vereine. Beispielhaft seien hier das nationale Cyber-Abwehrzentrum (NCAZ) und der Bundesverband IT-Sicherheit e. V. genannt. Das NCAZ ist eine Vereinigung mehrerer Kernbehörden (BSI, Bundesamt für Verfassungsschutz, BBK, BND, Bundespolizei, Bundeswehr, Zollkriminalamt) mit der Aufgabe, eine behördenübergreifende Koordination von Schutz- und Abwehrmaßnahmen gegen IT-Sicherheitsvorfälle zu etablieren.

Von Programmen und Aktivitäten des NCAZ ist allerdings wenig zu hören, was sich nicht zuletzt auf das begrenzte Personal von nur 10 Bediensteten zurückführen lässt. Der Bundesverband IT-Sicherheit ist ein Zusammenschluss von privaten Unternehmen und öffentlichen Institutionen (BKA, BSI) mit dem Ziel, die Vertrauenswürdigkeit der Informations- und Kommunikationstechnik zu fördern.

Bestimmte Bereiche der Informationssicherheit sind auch im deutschen Rechtssystem verankert, wie beispielsweise im Telemediengesetz oder den *Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen* (GDPdU). Außerdem liegt derzeit ein Entwurf für das *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme* (BSI-Gesetz oder auch Meldegesetz) vor. Es zielt auf die Etablierung von Mindeststandards in der IT-Sicherheit kritischer Infrastrukturen. Kritische Infrastrukturen sind solche, die direkt mit dem Gemeinwohl zusammenhängen. Betreiber solcher Strukturen sind demnach verpflichtet, schwerwiegende IT-Sicherheitsvorfälle an das BSI zu melden.

Sie sind dazu verpflichtet, anerkannte Sicherheitsstandards zu etablieren und diese alle zwei Jahre durch Audits zertifizieren zu lassen. Davon sind auch Telekommunikationsanbieter betroffen – sie werden stärker als bisher dazu verpflichtet, die Kommunikationsstruktur zu schützen sowie die Verfügbarkeit, Integrität und Authentizität datenverarbeitender Systeme zu sichern. Bekannt gewordene Sicherheitsvorfälle sollen sie dem BSI melden. Außerdem sollen sie Bürgern beim Schutz ihrer Systeme helfen, indem sie die Anwender über aufgetretene und bekannt gewordene Sicherheitsvorfälle informieren und entsprechende Präventivmaßnahmen ermöglichen.

**Abb. 22 Bekanntheit des Meldegesetzes**




Viele Führungskräfte scheuen sich allerdings davor, Sicherheitsinformationen mit anderen zu teilen und zu veröffentlichen. 70 % der im Rahmen der Studie zur Informationssicherheit im Mittelstand befragten Personen gaben an, den Gesetzesentwurf nicht zu kennen. Unter den mittelständischen Unternehmen lag diese Quote sogar bei 72 %. Auf die Frage, ob sie den Anforderungen zur Meldung von Cyberattacken derzeit nachkommen könnten, gaben 32 % der Vertreter von Großunternehmen an, dass dies nicht der Fall sei, 55 % fühlten sich dazu in der Lage. Noch bedenklicher scheint die Lage im Mittelstand, dessen Vertreter zu 36 % angaben, dass sie einer solchen Meldepflicht derzeit nicht nachkommen könnten. Befragt nach ihrer Meinung zu dem Gesetzesentwurf äußerten 29 % der Unternehmensvertreter die Meinung, dass ein solches Gesetz keinen echten Mehrwert bringen und nur zur weiteren Bürokratisierung führen würde.

Bei dieser Vielzahl von Programmen, Organisationen, Richtlinien und Gesetzen ist es gerade für Mittelständler nicht leicht, den Überblick zu bewahren und die für sie wichtigen Maßnahmen und Best Practices zur Informationssicherheit zu identifizieren. Dies wird dadurch verstärkt, dass die Initiativen teilweise in unterschiedliche Richtungen gehen und keine Abstimmung stattfindet. Daher ist es umso wichtiger, dass sich die Unternehmen nicht blind auf Rahmenwerke und Richtlinien verlassen, sondern ein für ihr Unternehmen angemessenes Informationssicherheitsmanagement etablieren.

# H Fazit und Ausblick

Ziel dieser Studie war es, den Stand der Informationssicherheit in mittelständischen Unternehmen abzufragen und auszuwerten. Bei der Befragung hat sich herausgestellt, dass für einen Großteil dieser Unternehmen die Sicherheit ihrer IT und der elektronischen Daten durchaus von Bedeutung ist. Allerdings scheint die Umsetzung von Schutzstrategien und -maßnahmen eher unstrukturiert abzulaufen. Dies ist darauf zurückzuführen, dass die IT bei vielen Unternehmen eine Unterstützungsfunktion hat.

Aus den Antworten wird ersichtlich, dass viele der befragten Mittelständler mit selbstgestrickten Sicherheitsprozessen arbeiten und sich nur selten an gängigen Standards und Best Practices wie dem IT-Grundschutz des BSI orientieren. Während die meisten zwar Richtlinien für die Passwortsicherheit oder die Anwendungssysteme haben, schulen nur wenige ihre Mitarbeiter regelmäßig zu Themen der Informationssicherheit. Fast jedes fünfte der befragten mittelständischen Unternehmen führt keinerlei Schulungen durch. Weiterhin zeigt die Studie, dass formal definierte Mitarbeiterstellen für die Gewährleistung der Informationssicherheit, allen voran der CISO, bei Mittelständlern – anders als bei Großunternehmen – oft nicht vorhanden sind. Dies birgt die Gefahr, dass die Sicherheit von IT-Systemen als nachrangig betrachtet wird und sich niemand dafür verantwortlich fühlt. All diese Faktoren geben Hinweise auf den Stellenwert der Informationssicherheit im Unternehmen

Die Angriffe auf die Unternehmens-IT, von denen man in der Presse liest, sind längst im Mittelstand angekommen. So berichtet jedes fünfte Unternehmen, dass es schon einmal Opfer von Cyberangriffen geworden ist. Hinzu kommt erfahrungsgemäß noch eine Anzahl von Angriffen, die aufgrund unzureichender Monitoring-Verfahren bisher nicht entdeckt wurden. Diese Angriffe scheinen sich aber nicht, wie bei den Großunternehmen, auf Kunden- oder Mitarbeiterdaten zu konzentrieren. Vielmehr ist das Ziel von Cyberattacken gegen Mittelständler häufig der Diebstahl von Know-how. Gerade weil in Deutschland viele mittelständische Unternehmen Marktführer in ihrer Branche oder ihrem Marktsegment sind und die Innovationsfähigkeit der Unternehmen bekannt ist, sollte diesen sehr daran gelegen sein, ihr Wissen zu schützen. Staat und Gesetzgeber können dabei mit Initiativen zur Informationssicherheit helfen, allerdings muss der Wille zum aktiven Schutz der IT-Infrastruktur und der Daten im Unternehmen selbst vorhanden sein. Hier ist Umdenken auf Unternehmensebene erforderlich: Der schnelle und transparente Austausch über aktuelle neue Gefährdungen, gegebenenfalls von einer unternehmensneutralen Instanz organisiert, wird eine Schlüsselaufgabe der nächsten Jahre im Kampf gegen Cybercrime und Cyberterrorismus sein müssen, um die Reaktionsgeschwindigkeiten in den Unternehmen signifikant zu verbessern: Auch hier wird der Gedanke des Teilens von Erfahrungen und Wissen schnell Einzug halten müssen, am besten systemübergreifend.

Die Angriffe auf die IT-Infrastruktur und die elektronischen Daten von Unternehmen werden in Zukunft, verstärkt durch neue Trends und Technologien, weiter zunehmen. Den mittelständischen Unternehmen ist daher zu empfehlen, sich der Bedeutung von Informationssicherheit bewusst zu sein und diese weiterhin im Fokus zu behalten.

# Ihre Ansprechpartner

***Derk Fischer***
Tel.: +49 211 981-2192
derk.fischer@de.pwc.com

***Joachim Mohs***
Tel.: +49 40 6378-1838
joachim.mohs@de.pwc.com

***Rene Sieben***
Tel.: +49 211 981-2064
rene.sieben@de.pwc.com

***Aleksei Resetko***
Tel.: +49 69 9585-5059
aleksei.resetko@de.pwc.com

***Über PwC***

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expertennetzwerks in 157 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC. 9.300 engagierte Menschen an 28 Standorten. 1,55 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.