Deloitte.

Cyber-Security Report 2017 – Teil 2:

Cyber-Risiken in Unternehmen

Vorwort 05

Executive Summary 06

1. Gefährdung von Unternehmen 08

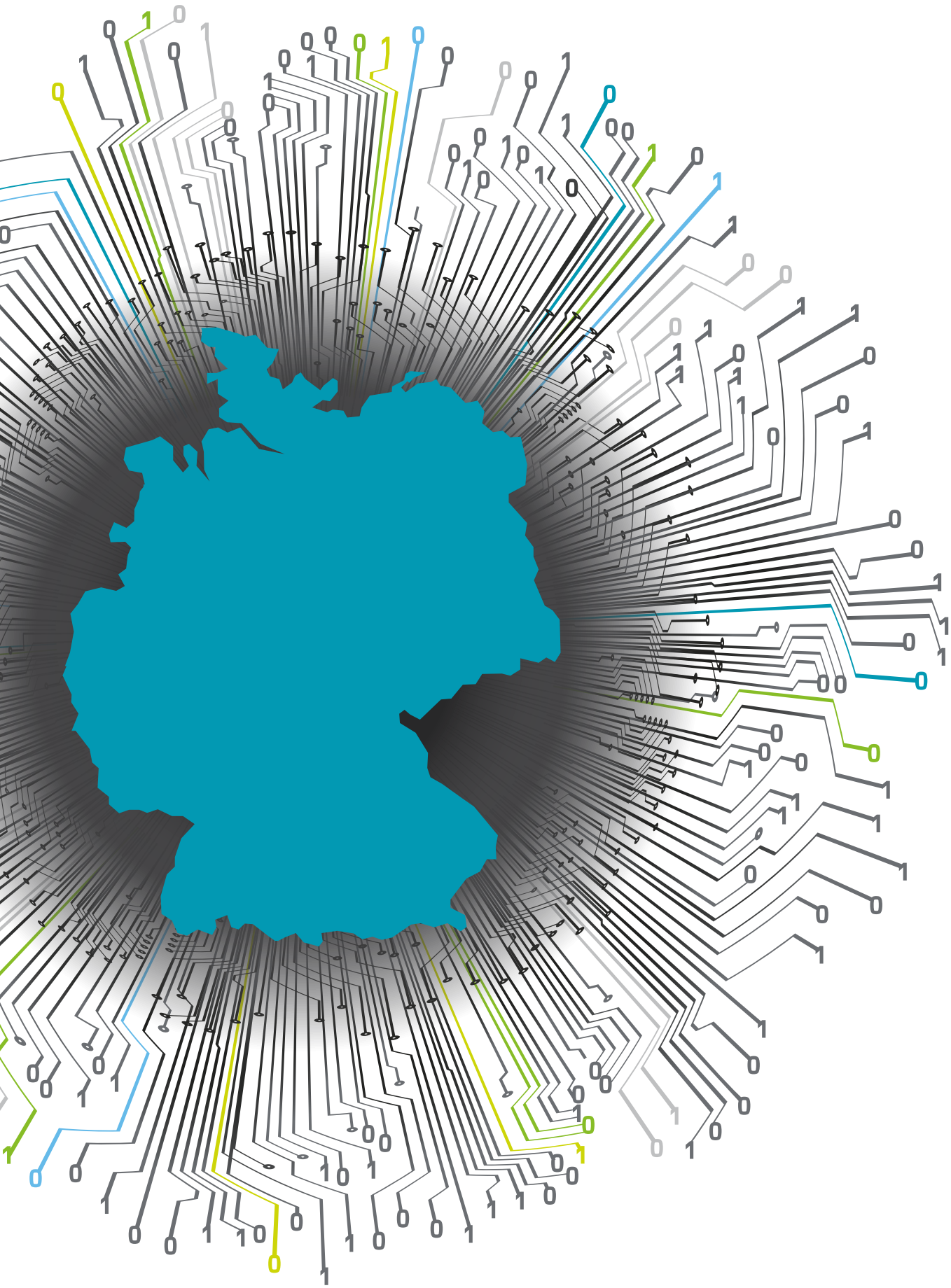
2. Auswirkungen auf Unternehmen 10

3. Risikofaktoren für Unternehmen 14

4. Vorbereitung und Abwehr 18

5. Verantwortung und Kompetenz im Unternehmen 24

6. Handlungsempfehlungen 30



Vorwort

Digitalisierung in der Wirtschaft, der öffentlichen Verwaltung und allen Bereichen des gesellschaftlichen Lebens ist der Schlüssel für ein zukunftsfähiges Deutschland. Nur so erzielen wir die erforderlichen Produktivitätsgewinne und behaupten als gesamte Volkswirtschaft unseren Platz in einer globalisierten Welt. Die Gestaltung dieses Wandels ist Aufgabe von Politik und Wirtschaft gemeinsam und erfordert eine neue Art der Zusammenarbeit und Kooperation zwischen diesen Bereichen.

Die Digitalisierung betrifft nicht nur große und global agierende Unternehmen oder einzelne Branchen, sondern die gesamte Wirtschaft: den Handwerker wie das Internet-Start-up, den Einzelhändler wie das Finanzunternehmen, das Krankenhaus ebenso wie den Energieversorger, das Verkehrsunternehmen wie den Fahrzeughersteller. Für alle ändern sich die Form der Einbindung in Lieferketten, der angebotene Service, die Art und Weise der Produktion, das Produkt selbst, Distribution und Logistik sowie die Abwicklung von Finanztransaktionen und Zahlungsströmen. Einfach jeder Bereich des unternehmerischen Handelns wird von digitalen Veränderungen berührt, wenn nicht sogar revolutioniert.

Grundlage ist die Vernetzung der IT-Systeme im Unternehmen z.B. in der Produktion und ihrer Steuerung, in den Unternehmenssteuerungs- und -überwachungssystemen, in der Office-IT und zu Softwarekomponenten der Produkte. Die Konvergenz dieser Systeme in den Organisationen steigt und ihre Vernetzung zu Bereichen außerhalb des Unternehmens nimmt zu. Damit steigen aber auch externe Bedrohung und Gefährdung – die Anforderungen an die erforderlichen IT- und Cyber-Security-Maßnahmen werden umfassender und komplexer.

Die Umsetzung von Maßnahmen, die diesen erhöhten Anforderungen an die Security gerecht werden, wird zum kritischen Erfolgsfaktor der Digitalisierung. Aufgrund der Vernetzung macht eine wirksame Security-Strategie nicht an der Unternehmensgrenze halt – sie erfordert vielmehr intensive Kooperationen zwischen Unternehmen untereinander und mit staatlichen Stellen auf der Basis eines wirksamen und verlässlichen Regulierungsrahmens.

Durch unsere Cyber-Security-Projekte unterstützen wir Unternehmen bei der erfolgreichen Umsetzung ihrer Digitalisierungsstrategie. Wir bringen unsere Erfahrungen in die Zusammenarbeit mit staatlichen Stellen ein, um die Schaffung der erforderlichen Rahmenbedingungen zu unterstützen.

Gemeinsam mit dem Institut für Demoskopie Allensbach hat Deloitte in diesem Jahr eine insgesamt zum siebten Mal erscheinende repräsentative Trendstudie durchgeführt, um den Stand der Cyber-Security in Deutschland zu erheben. Es wurden 403 Führungskräfte aus großen und mittleren Unternehmen sowie 103 Abgeordnete aus Länderparlamenten, Deutschem Bundestag und Europaparlament zwischen dem 9. Juni und dem 12. Juli 2017 befragt. Die Befragten sind keine IT-Experten aus Unternehmen und keine Fachpolitiker für diese Thematik. Die Ergebnisse zeigen somit die Wahrnehmung auf Ebene von Entscheidern, deren Tagesgeschäft nicht allein auf diese Thematik fokussiert ist.

Wie in den Vorjahren bildet die Einschätzung der Bedrohung durch Cyber- und IT-Risiken und der daraus folgenden Gefahren für Unternehmen den Schwerpunkte der Studie. Unternehmen geben Auskunft über die Zahl der erfolgten Angriffe und die Art der daraus resultierenden Schäden sowie über die von ihnen ergriffenen Maßnahmen.

Wir haben die Kernaspekte der Studie in diesem Jahr um wesentliche Punkte der aktuellen Situation in den Unternehmen und wichtige Fragestellungen aus der gesellschaftlichen und politischen Debatte ergänzt.

Teil 1 der Studie befasst sich daher mit der institutionellen Verantwortung staatlicher Stellen und der Frage, wie die Verantwortungsbereiche von Staat, Wirtschaft und Gesellschaft für Cyber-Security ineinandergreifen. Weiterhin haben wir dort hinterfragt, inwieweit „Fake News“ als Gefahr für die Manipulation von Meinungen gesehen werden.

Der hier vorliegende Teil 2 zeigt die Sicht der befragten Entscheider aus Wirtschaft und Politik auf die Situation in den Unternehmen. Hierbei haben wir einen Schwerpunkt auf die Verantwortung und Mitwirkung von Führungsgremien in der Cyber-Sicherheit in Unternehmen gesetzt.

Executive Summary

Die Ergebnisse der Befragung führen zu folgenden Kernaussagen:

Die Gefährdung der Unternehmen steigt ungebremst rasant an
Der dramatische Anstieg der Informationssicherheitsvorfälle als solches ist nicht unerwartet, jedoch ist die Breite der Auswirkungen und deren Wahrnehmung in Unternehmen ein neuer Trend. Fast die Hälfte der Unternehmen wird wöchentlich attackiert, davon die überwiegende Anzahl sogar täglich. Die Zahl der erkannten Cyber-Vorfälle steigt mit der Unternehmensgröße. Führungskräfte schätzen, dass eine beachtliche Dunkelziffer an Angriffen sogar unerkannt bleibt, und dies besonders in kleinen Unternehmen.

Die Schadenspotenziale sind vielfältig
Die Liste möglicher Auswirkungen von Cyber-Angriffen ist umfangreich. Sie reicht vom Produktionsausfall über Know-how-Verlust und Imageschaden bis hin zu persönlichen Konsequenzen für Führungskräfte. Fast die Hälfte der befragten Führungskräfte stuft das Risiko, durch einen Cyber-Angriff gravierend geschädigt zu werden, als eher groß bis sehr groß ein, 10 Prozent sehen sogar ein sehr großes Risiko für gravierende Schäden. Die Einschätzungen der Führungskräfte zeigen auch, dass die Wahrnehmung des Schadensrisikos mit der eigenen Unternehmensgröße steigt.

Risikofaktor Mensch
Der Zugriff auf Unternehmensdaten aus allen Ecken der Welt stellt Unternehmen vor große Herausforderungen, wenn Unternehmensgrenzen verschwinden und das virtuelle Büro in den Zug, ins Flugzeug, ins Internet-Cafe oder gar an den Strand verlegt wird. Dass Mitarbeiter – unwissentlich, versehentlich oder vorsätzlich – leichtfertig mit Daten oder Sicherheitsstandards umgehen und verhaltensbedingt Schaden anrichten, ist für Führungskräfte mit Abstand am häufigsten eine große Gefahrenquelle.

Unsicherheiten im Umgang mit den Risiken
Die Mehrheit der Führungskräfte aus mittleren und großen Unternehmen räumt ein, dass man im eigenen Unternehmen nicht genau wisse, welche Arten von Angriffen es aktuell in der eigenen Branche gibt und worauf man sein Unternehmen einstellen muss. Bemerkenswerterweise bestehen solche Unsicherheiten auch bei Führungskräften, deren Unternehmen täglich IT-Angriffen ausgesetzt sind. In dem Zusammenhang ist auch hervorzuheben, dass gesetzliche oder regulatorische Anforderungen der Mehrheit der Führungskräfte nicht bekannt sind.

Security als Chefsache?
Das Thema Cyber-Security scheint auf der Agenda der Geschäftsleitungsebene angekommen zu sein. In drei Viertel der Unternehmen beschäftigen sich Vorstand beziehungsweise Geschäftsführung intensiv oder sogar sehr intensiv mit Cyber-Security. Im Umkehrschluss bedeutet das allerdings, dass sich in jedem vierten Unternehmen die Unternehmensführung weniger intensiv bis gar nicht damit auseinandersetzt. Zudem steht bei einem Drittel der Vorstände beziehungsweise Geschäftsführer Cyber-Security lediglich anlassbezogen oder gar nicht auf der Tagesordnung. Nur eine Minderheit sieht in ihren Unternehmen ausreichend Fachkompetenz im Bereich Cyber-Security auf Geschäftsleitungsebene, um sich damit überhaupt eingehend zu beschäftigen. In Organisationen, die über einen Aufsichtsrat verfügen, befasst sich dieser nur in 50 Prozent der Fälle mit dem Thema.

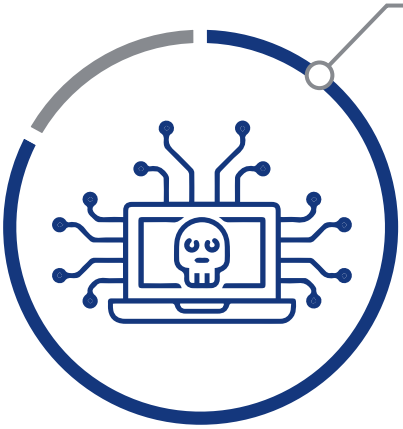
1. Gefährdung von Unternehmen

Cyber-Angriffe sind allgegenwärtig und gehören mittlerweile zum Unternehmensalltag. Dieser Trend ist deutlich erkennbar, auch wenn keine allgemein gültige Definition besteht, ab wann ein Vorfall als „Angriff" zu werten ist. So berichten fast 50 Prozent der Befragten von wöchentlichen Angriffen. Die Zahl der erkannten Angriffe steigt mit der Unternehmensgröße deutlich an. 83 Prozent der Unternehmen mit mehr als 1.000 Mitarbeitern werden nach Aussage der Befragten mehrmals monatlich attackiert – die Hälfte davon täglich.

Abb. 1 – Deutsche Unternehmen sind häufig Ziel von IT-Angriffen

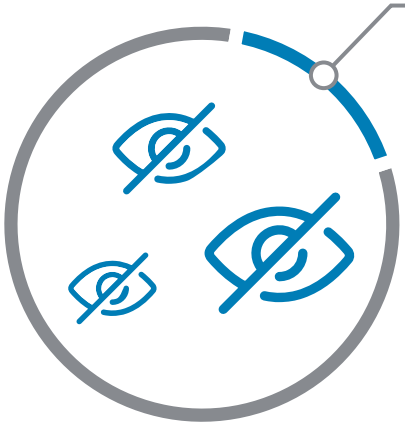
83%

der Unternehmen mit mehr als 1.000 Mitarbeitern registrieren mehrmals im Monat Angriffe auf die IT – die Hälfte davon nahezu täglich.



27%

der Unternehmen glauben, dass Cyber-Angriffe häufig unbemerkt bleiben.



+88%
in fünf Jahren

Die Anzahl der täglichen bis wöchentlichen Angriffe hat sich in den letzten fünf Jahren fast verdoppelt.

Eine hohe Dunkelziffer wird von Führungskräften in Rechnung gestellt.

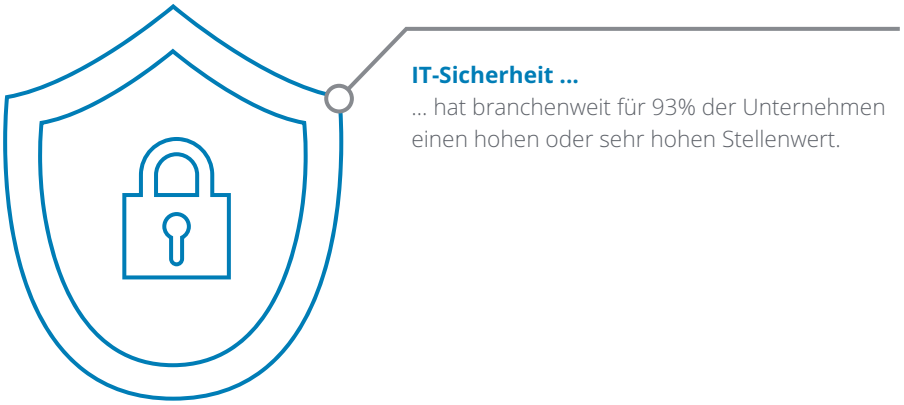
Betrachtet man diese Einschätzung im Mehrjahresvergleich, wird die drastische Zunahme der Gefährdung deutlich. Seit 2013 hat sich demnach die Anzahl der täglichen bis wöchentlichen Angriffe fast verdoppelt.

Hinzu kommt eine beträchtliche Dunkelziffer. Rund jede vierte Führungskraft geht davon aus, dass Cyber-Angriffe auf das eigene Unternehmen unbemerkt bleiben.

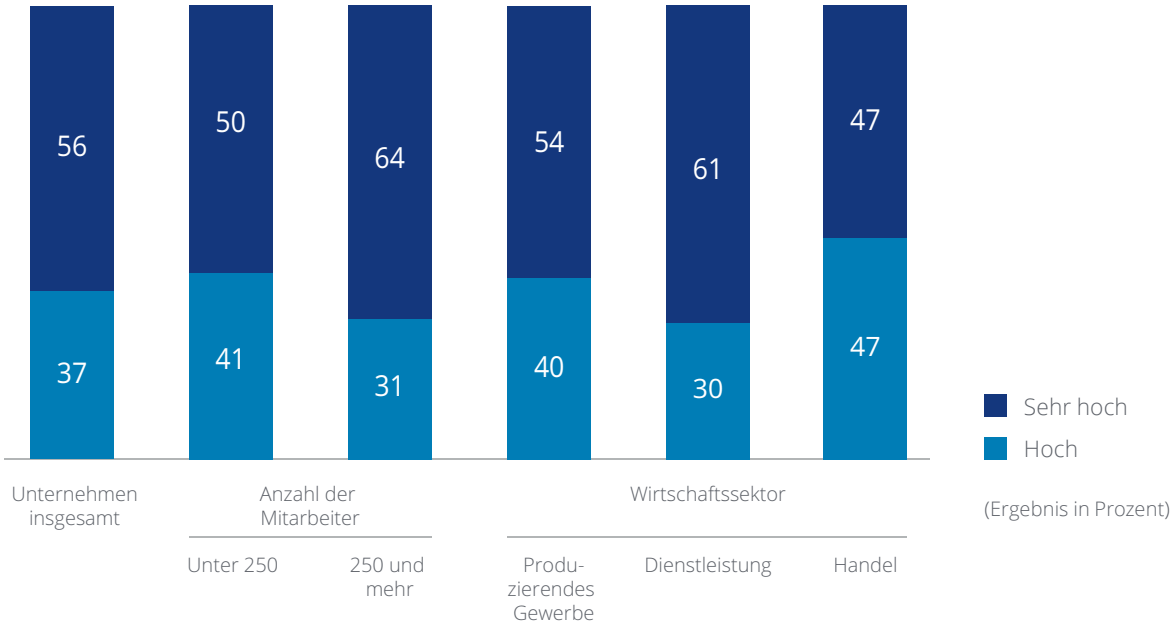
Dies schätzen insbesondere kleinere Unternehmen so ein, in denen üblicherweise die personellen Ressourcen und ergriffenen Maßnahmen auf dem Gebiet der Informationssicherheit hinter Großunternehmen zurückbleiben.

Die Gefährdung wird in den Unternehmensführungen erkannt und demzufolge dem Thema Informationssicherheit auch ein hoher bis sehr hoher Stellenwert beigemessen.

Abb. 2 – Hoher Stellenwert der Informationssicherheit in deutschen Unternehmen



IT-Sicherheit ...
... hat branchenweit für 93% der Unternehmen einen hohen oder sehr hohen Stellenwert.



2. Auswirkungen auf Unternehmen

Stillstand, Produktionsausfall, Wettbewerbsnachteile, finanzielle Verluste, physische Schäden, Wiederherstellungsaufwand, rechtliche Sanktionen, Reputationsverlust und persönliche Konsequenzen für Führungskräfte und Mitarbeiter – die Liste möglicher Auswirkungen von Cyber-Angriffen auf Unternehmen ist umfangreich. Die direkten Kosten dieser Attacken können im Einzelfall womöglich quantifiziert werden. Die langfristigen Auswirkungen auf die Reputation und die Marke eines Unternehmens jedoch sind schwer zu schätzen. Insbesondere der Verlust von Kundendaten kann zum Vertrauensverlust führen, der sich direkt auf den Umsatz auswirkt.

Die Schäden von Cyber-Angriffen sind nur zum Teil direkt quantifizierbar; daneben treten Reputations- und Imageschäden und entgangene Chancen. Ein durchschnittlicher wirtschaftlicher Schaden durch einen Angriff wird auf ca. 700.000 € geschätzt.[1] Der deutschen Wirtschaft entstehen dadurch jährlich Schäden in schwindelerregender Höhe. Schätzungen gehen von bis zu rund 51 Mrd. € jährlich aus.[2]

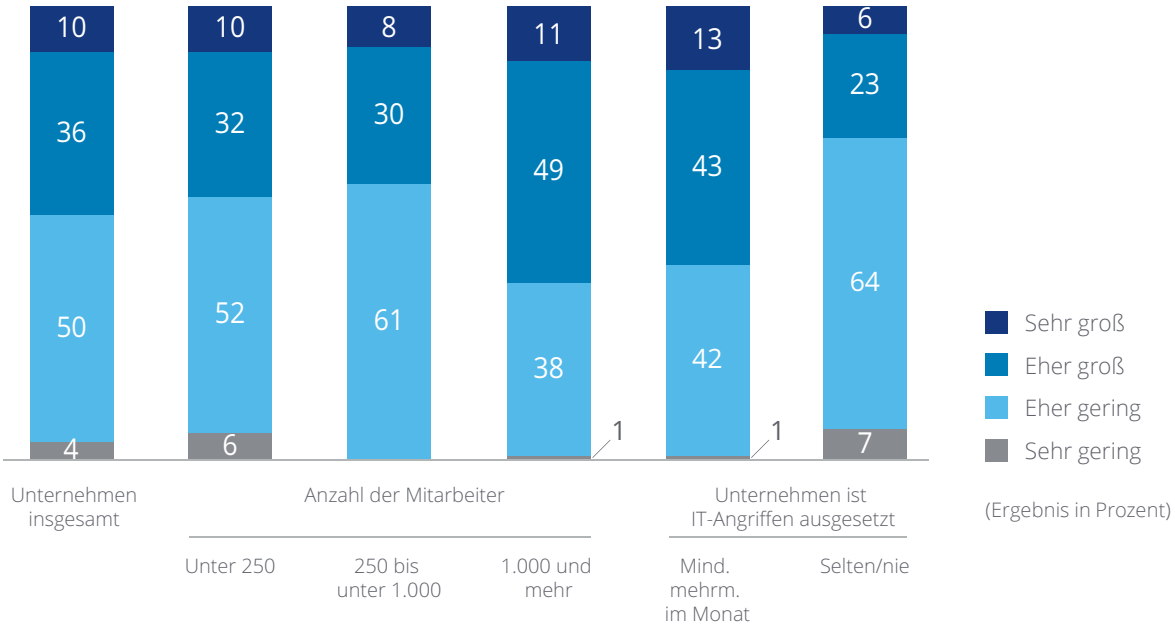
46 Prozent der befragten Wirtschaftsführer stufen das Risiko, dass ihr Unternehmen durch einen Cyber-Angriff gravierend geschädigt wird, als eher groß bis sehr groß ein. Darunter sehen 10 Prozent ein sehr großes Risiko für gravierende Schäden. Während Führungskräfte aus großen Unternehmen mit 1.000 und mehr Mitarbeitern hierbei überdurchschnittlich häufig große Risiken sehen, glaubt die Mehrheit der Studienteilnehmer aus Unternehmen mit unter 1.000 Mitarbeitern eher an ein geringes Schadenspotenzial.

Die Einschätzungen der Führungskräfte zeigen, dass die Wahrnehmung des Schadensrisikos mit der eigenen Unternehmensgröße korreliert. Sehr deutlich lässt sich auch ein Zusammenhang zwischen den Einschätzungen der Führungskräfte und der Häufigkeit der erfassten Cyber-Attacken feststellen. Von den Unternehmen, die mindestens mehrmals im Monat angegriffen werden, stufen mehr als die Hälfte der Führungskräfte das Schadensrisiko als eher groß bis sehr groß ein. Bei selten bis nie betroffenen Unternehmen gehen nur 29 Prozent der Befragten von einem eher großen bis sehr großen Schadensrisiko aus.

[1] Vgl. Buhleier, Wirnsperger, Brocard (2017): Cyber Security und der Aufsichtsrat, Herausforderungen und Aufgaben, BOARD 2/2017, S. 170..
[2] Bitkom e.V. (2017): http://www.bitkom.org, abgerufen am 04.12.2017.

Abb. 3 – Geteilte Meinung bei der Einschätzung des Schadensrisikos durch Hacker-Angriffe

Schadensrisiko
Nicht einmal die Hälfte der Unternehmen stuft das Risiko einer gravierenden Schädigung durch einen Hacker-Angriff als (eher) groß ein.

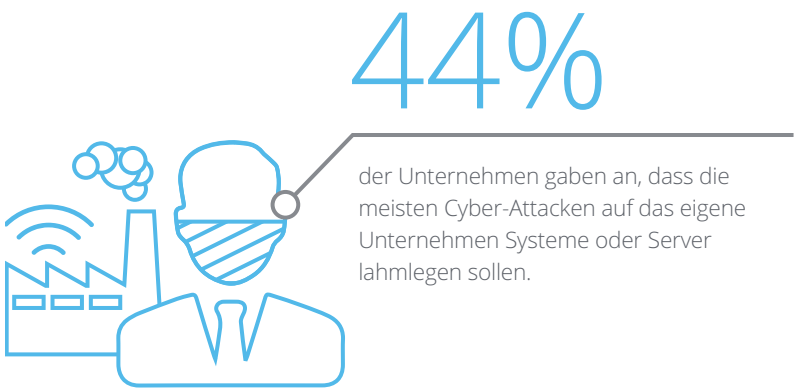


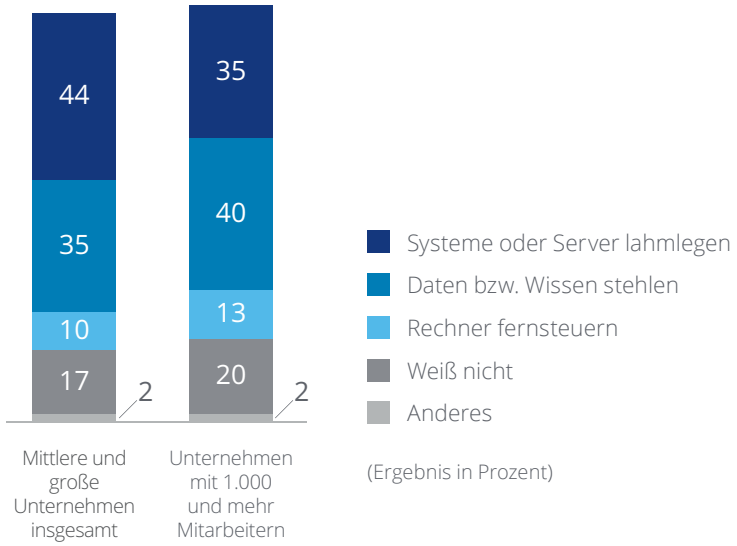
Auf 100 fehlende Prozent: Unentschieden, keine Angabe.

Führungskräfte aus angegriffenen mittleren und großen Unternehmen haben den Eindruck, dass Cyber-Angriffe am ehesten auf ihre Systeme sowie Server zielen, 44 Prozent vermuten destruktive Absichten der Angreifer. Dagegen berichten mit 40 Prozent Studienteilnehmer großer Unternehmen mit 1.000 und mehr Mitarbeitern mit 40 Prozent am häufigsten von Versuchen, Daten oder Wissen zu stehlen.

Dramatisch ist, dass knapp ein Fünftel der Befragten nicht weiß, worauf es die meisten Angreifer abgesehen haben, mit denen ihr Unternehmen konfrontiert ist. Somit besteht bei Führungskräften eine beachtliche Ungewissheit, ob Systeme und Server lahmgelegt oder Daten und Wissen gestohlen werden sollen.

Abb. 4 – Führungskräfte sehen bei Cyber-Attacken am häufigsten destruktive Ziele





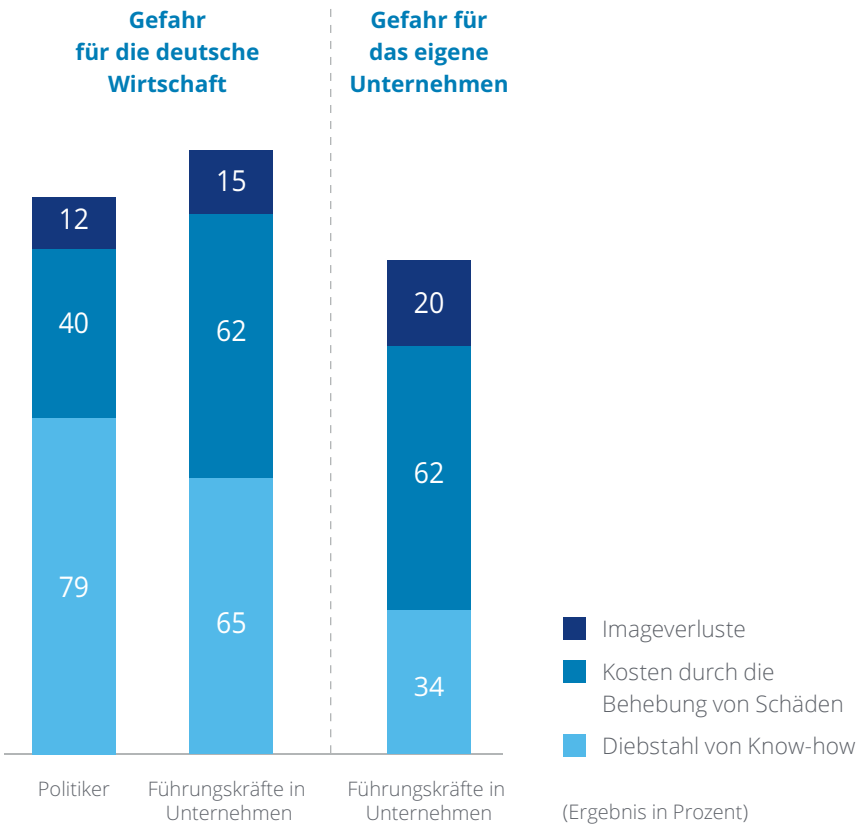
Aufgrund von Mehrfachnennungen ist die Summe anteiliger Antworten größer als 100 Prozent.

Bei der Einschätzung der Schadenspotenziale durch Cyber-Angriffe für die deutsche Wirtschaft insgesamt wird von Politikern und Wirtschaftsführern eher der Diebstahl von Know-how als größte Gefahr gesehen, wobei Politiker darin in noch höherem Anteil eine wesentliche Gefahr für die deutsche Wirtschaft sehen. Die für die Unternehmen entstehenden Kosten durch Ausfälle und Schäden haben sie dagegen deutlich weniger vor Augen.

Als größte Gefahr von Cyber-Angriffen für das eigene Unternehmen benennen Wirtschaftsführer zu rund zwei Dritteln und damit mit Abstand am häufigsten die Kosten, die durch den Ausfall der Infrastruktur oder die Behebung von Schäden entstehen. Der Diebstahl von Unternehmenswissen wird von einem Drittel und der Imageverlust durch einen bekannt gewordenen Cyber-Angriff von einem Fünftel als größte Cyber-Gefahr sehen.

Abb. 5 – Schadenspotenziale durch Cyber-Angriffe

Gespaltenes Meinungsbild
Bei der Einschätzung der Schadenspotenziale von Cyber-Angriffen gehen die Meinungen der Politiker und die Wahrnehmungen in den Unternehmen auseinander.



Aufgrund von Mehrfachnennungen ist die Summe anteiliger Antworten größer als 100 Prozent.

„Deutsche Unternehmen sind aufgrund ihres Know-hows beliebte Angriffsziele. Angreifer streben nach Informationen über Produkte und Geschäftsprozesse, um aus erbeuteten Daten Profit zu schlagen. Ein angemessen hohes Niveau an Cyber-Security ist der Schlüssel zur erfolgreichen Verteidigung. Schließlich geht es hier um die ‚digitalen Kronjuwelen' der Unternehmen."

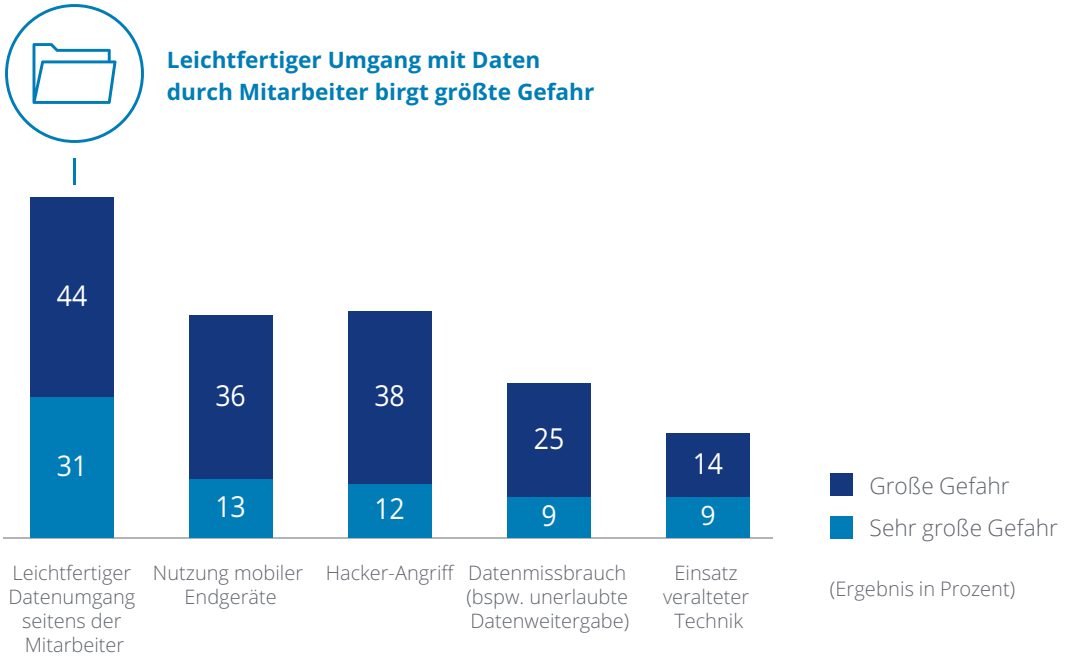
Peter J. Wirnsperger, Cyber Risk Leader

3. Risikofaktoren für Unternehmen

Die Chancen durch die Digitalisierung in Unternehmen sind enorm. Die Risiken sind es allerdings auch und müssen deshalb berechenbar und beherrschbar bleiben.

Vorschriften, Prozesse und Technologien leisten einen wichtigen Beitrag zum IT-Risikomanagement des Unternehmens. Doch ein noch so gutes Risikomanagement versagt, wenn Mitarbeiter – unwissentlich, versehentlich oder vorsätzlich – falsch entscheiden, unsauber arbeiten und verhaltensbedingt Schaden anrichten. Der Risikofaktor Mensch kann auch allein aus Neugier oder Gutgläubigkeit zur Schwachstelle des Unternehmens werden.
Im Vergleich verschiedener Risiken im Bereich Cyber-Sicherheit im eigenen Unternehmen sehen Führungskräfte den leichtfertigen Umgang mit Daten und Sicherheitsstandards durch Mitarbeiter mit Abstand am häufigsten als Gefahrenquelle. Drei Viertel der Führungskräfte sehen darin eine große, sogar sehr große Gefahr. Im Vergleich zum Vorjahr stieg die Anzahl der Führungskräfte von 20 auf 31 Prozent, die im leichtfertigen Umgang mit Daten seitens der Mitarbeiter eine sehr große Gefahr für die Informationssicherheit des eigenen Unternehmens sehen.

Abb. 6 – IT-Sicherheitslecks
Die größte Gefahr für IT-Sicherheit im Unternehmen geht von leichtfertigem Umgang mit Daten seitens der Mitarbeiter aus.

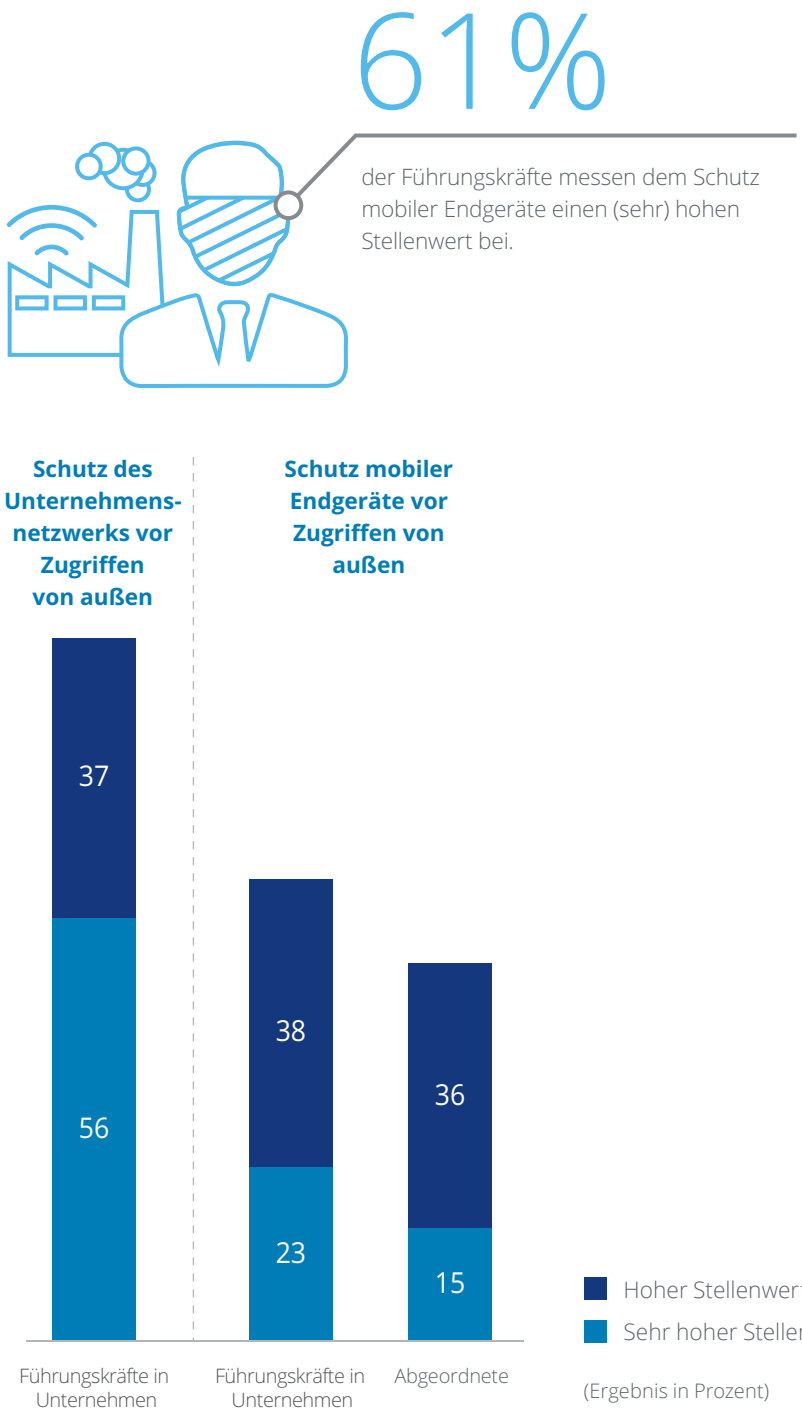


„Technische Maßnahmen alleine reichen nicht aus, um Unternehmen vor Cyber-Bedrohungen zu schützen. Vorschriften und Verhaltensrichtlinien müssen nicht nur erlassen, sondern gelebt werden. Dazu gehört zum einen die Umsetzung in den Prozessen, zum Beispiel in Form von Berechtigungen, Funktionstrennungen und Kontrollen. Zum anderen aber auch eine gelebte Risikokultur in der Zusammenarbeit im Unternehmen und ein angemessenes Risikobewusstsein jedes einzelnen Mitarbeiters.“

Katrin Rohmann, Public Sector Leader

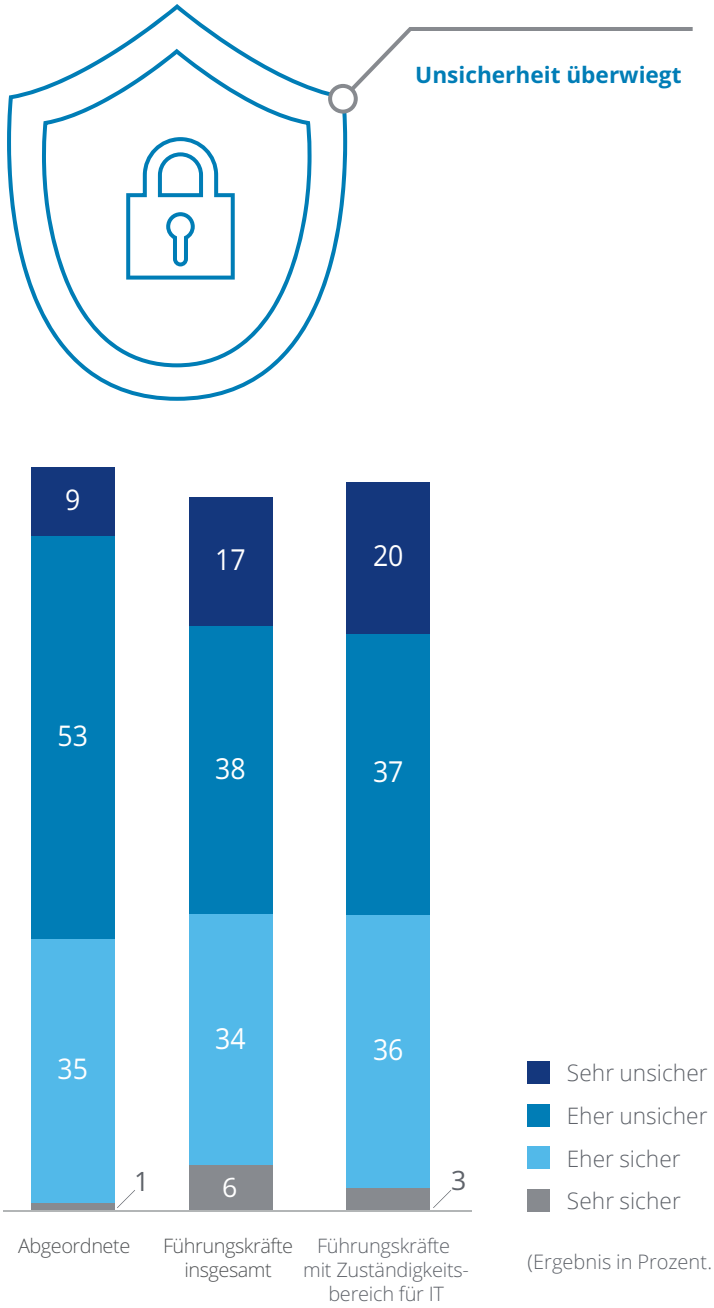
Weitere (sehr) große Gefahren sehen Führungskräfte bei der Nutzung mobiler Endgeräte. Zwar berichtet auch hier eine Mehrheit der Befragten von einem hohen oder sehr hohen Stellenwert des Schutzes mobiler Endgeräte im eigenen Unternehmen. Verglichen mit dem Stellenwert der Informationssicherheit in Unternehmen insgesamt wird diesem Feld aber deutlich weniger Beachtung geschenkt und im Vergleich zum Vorjahr ist der Stellenwert des Schutzes mobiler Endgeräte signifikant zurückgegangen.

Abb. 7 – Bedeutung des Schutzes mobiler Endgeräte

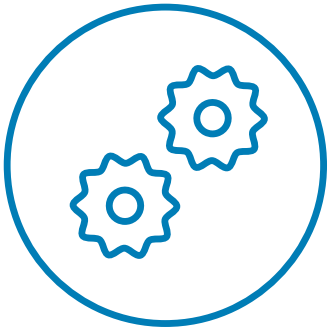


Cloud-Computing – die Bereitstellung von IT-Infrastruktur wie zum Beispiel Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung über das Internet – wird weiter als überwiegend unsicher bewertet. 55 Prozent der Führungskräfte schätzen es als (sehr) unsicher und 40 Prozent als (sehr) sicher ein, wobei das Vertrauen in den letzten Jahren zugenommen hat. Führungskräfte in Unternehmen, die Cloud-Computing nutzen, nutzen vor allem externe Cloud-Dienste für geschäftliche Zwecke. Aber auch Führungskräfte, die die Sicherheit dieser technischen Dienstleistung skeptisch sehen, nutzen sie mit insgesamt 28 Prozent zu einem nicht unerheblichen Teil.

Abb. 8 – Verbreitet Zweifel an der Sicherheit von Cloud-Computing



(Ergebnis in Prozent. Auf 100 fehlende Prozent: Keine Angabe oder es kommt darauf an.)



4. Vorbereitung und Abwehr

Cyber-Angriffe sind eine Realität, der sich Unternehmen im täglichen Umgang stellen müssen. Es geht nicht darum ob, sondern wann ein Unternehmen angegriffen wird. Deshalb müssen sich Führungskräfte fragen, was die „digitalen Kronjuwelen" ihres Unternehmens sind. Anders ausgedrückt: welche Daten, Geschäftsprozesse und IT-Infrastrukturen für ihr Unternehmen kritisch oder für den Betriebsablauf unerlässlich sind. Eine strukturierte Aufstellung „der Kronjuwelen" kann Unternehmen unterstützen, die individuelle Informationssicherheitsstrategie zu erstellen, die Priorisierungen vorzunehmen und geeignete Schutzmaßnahmen umzusetzen.

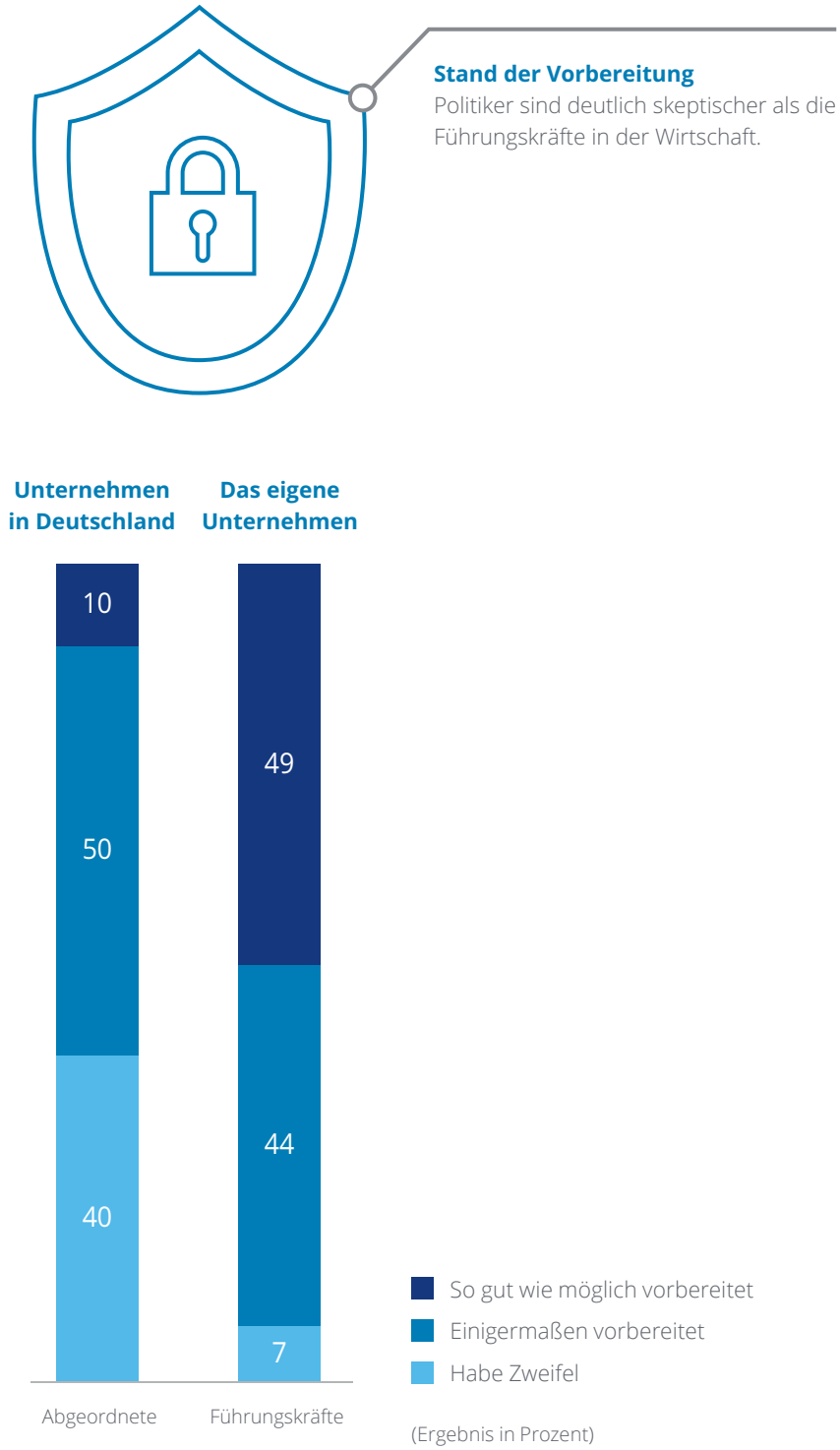
Politiker haben nur zu 10 Prozent den Eindruck, dass Unternehmen in Deutschland im Bezug auf Cyber-Angriffe bestmöglich gerüstet wären. 40 Prozent haben daran ausdrücklich Zweifel und genau die Hälfte der befragten Politiker hat den Eindruck, dass die Unternehmen hierzulande nur einigermaßen vorbereitet sind.

Zu diesem Thema befragt, schätzen die teilnehmenden Führungskräfte den Stand der Vorbereitung für ihre Organisation deutlich positiver ein: Die Hälfte von ihnen sieht ihr Unternehmen gegenüber möglichen Gefahren für die Informationssicherheit so gut wie möglich vorbereitet. Im Umkehrschluss zweifelt demnach die andere Hälfte an ihren Maßnahmen oder befürchtet, dass sie nur einigermaßen vorbereitet ist.

Diese Einschätzung macht das Erfordernis der Einführung prophylaktischer. Informationssicherheitsmaßnahmen nur zu deutlich. Dazu zählen technische und nicht-technische Schritte.

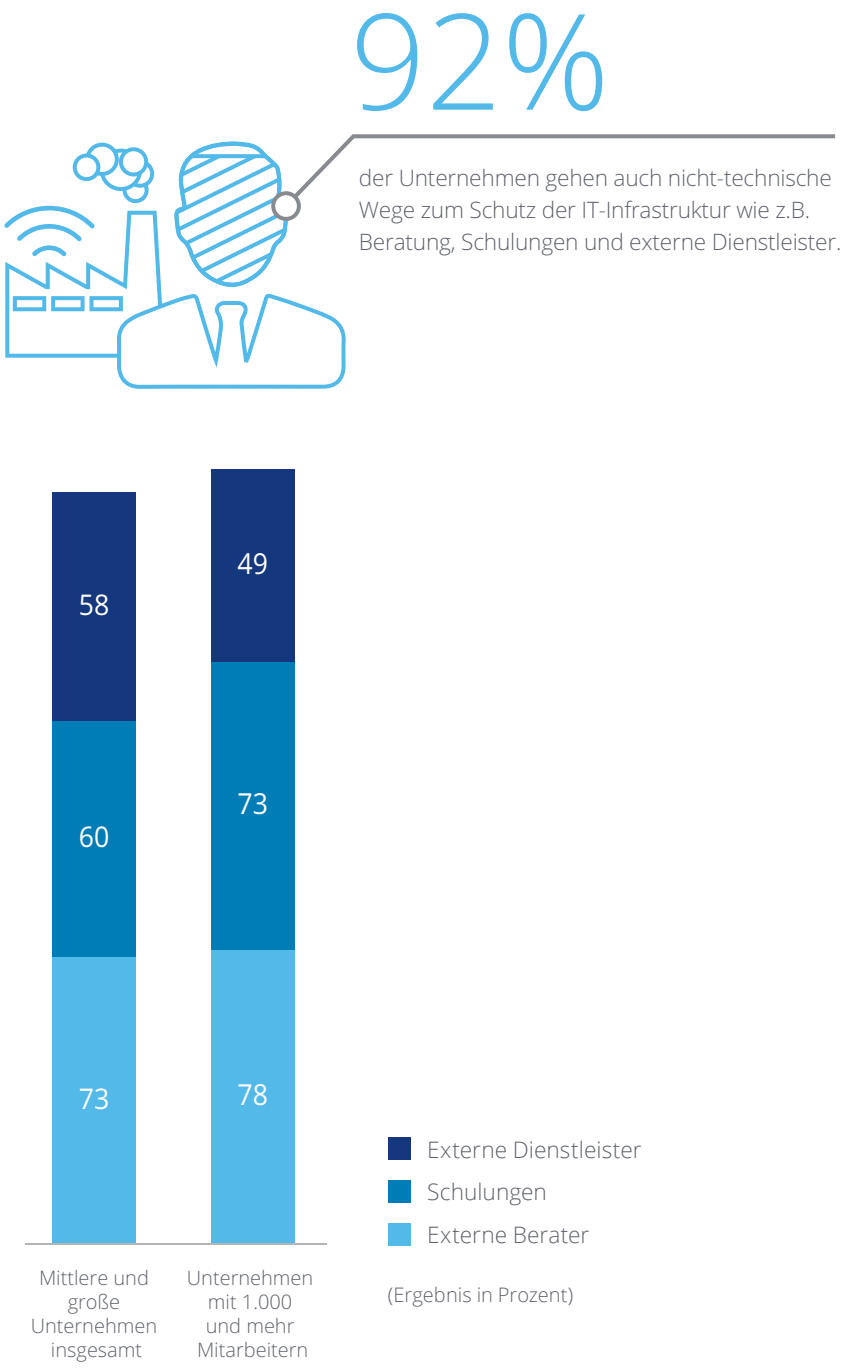
[3] BSI (2017): https://www.bsi.bund.de, abgerufen am 21.11.2017

Abb. 9 – Sind die Unternehmen in Deutschland auf IT-Angriffe vorbereitet?



Mit 92 Prozent ergreift eine große Mehrheit der Unternehmen nicht-technische Maßnahmen zum Schutz der IT-Infrastruktur. Mittlere und große Unternehmen mit 1.000 und mehr Mitarbeitern setzen hierbei alle in erster Linie auf externe Berater. Auf diese Weise beschaffen sich Unternehmen Kompetenz, Know-how, Manpower und Objektivität. Die überwiegende Anzahl der Unternehmen nutzt Schulungen, um Mitarbeiter über Informationssicherheit zu informieren. Die Mehrheit der Unternehmen beauftragt externe Dienstleister, die sich um das Thema Cyber-Security im Unternehmen kümmern, beispielsweise durch sogenannte Managed Security Services.

Abb. 10 – Einsatz nicht-technischer Schutzmaßnahmen



Aufgrund von Mehrfachnennungen ist die Summe anteiliger Antworten größer als 100 Prozent.

In den Unternehmen, die nach eigener Aussage „so gut wie möglich" auf IT-Gefahren vorbereitet sind, zeigt sich bei genauerer Analyse, dass diese Einschätzung zum Teil kritisch zu hinterfragen ist. Denn in genau diesen Unternehmen

- beschäftigt sich in mehr als jedem fünften Fall die Geschäftsleitungsebene nur anlassbezogen oder kaum bzw. gar nicht mit dem Thema Cyber-Security,
- verfügt nur in der Hälfte der Fälle die Geschäftsleitungsebene nach Einschätzung der befragten Führungskraft über ausreichend Kompetenz in dem Themenfeld,
- ist nur knapp der Hälfte der Führungskräfte bekannt, dass es gesetzliche oder regulatorische Anforderungen an ihr Unternehmen im Bereich IT-Sicherheit gibt, und
- gibt es in mehr als jedem Vierten keinen Notfallplan für den Fall eines erfolgreichen Cyber-Angriffs.

Abb. 11 – Angaben bezüglich Informationssicherheitsmaßnahmen sind kritisch zu bewerten

Für die Unternehmen, die nach eigener Aussage „so gut wie möglich" auf mögliche Gefahren für die IT-Sicherheit vorbereitet sind, gilt:

50%

von ihnen geben an, dass die Geschäftsleitungsebene ausreichende Kompetenz im Bereich Cyber-Security hat.

Bei 28%
gibt es keinen Notfallplan für den Fall eines erfolgreichen Cyber-Angriffs.

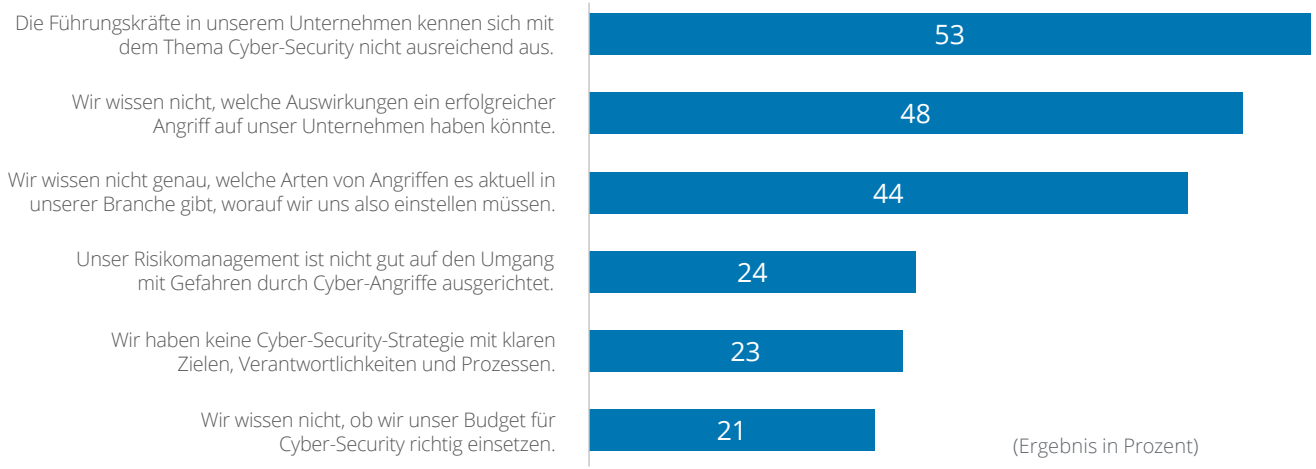
Nur 46%
ist bekannt, dass es gesetzliche/regulatorische Anforderungen an ihr Unternehmen im Bereich Cyber-Security gibt.

In 22%
der Fälle beschäftigt sich die Geschäftsleitungsebene nur anlassbezogen oder kaum bzw. gar nicht mit dem Thema Cyber-Security.

Verbreitet geben die Wirtschaftsführer insgesamt Unsicherheiten und Defizite im Umgang mit Cyber-Risiken zu Protokoll. So räumt jeweils die Mehrheit der Führungskräfte aus mittleren und großen Unternehmen ein, dass man in der eigenen Organisation nicht genau wisse, welche Arten von Angriffen es aktuell in der eigenen Branche gibt und worauf man sich einstellen müsse, welche Auswirkungen ein erfolgreicher Angriff auf das Unternehmen haben könnte, und auch, dass sich die Führungskräfte im eigenen Unternehmen mit dem Thema Cyber-Security nicht ausreichend auskennen. Und in immerhin rund jeder dritten Firma gibt es keine Cyber-Security-Strategie mit klaren Zielen, Verantwortlichkeiten und Prozessen. Bemerkenswerterweise bestehen solche Unsicherheiten und Defizite verbreitet auch bei Unternehmen, die täglich IT-Angriffen ausgesetzt sind, sowie in solchen, die nach eigener Aussage so gut wie möglich auf IT-Angriffe vorbereitet sind.

Abb. 12 – Know-how und Angriffshäufigkeiten driften weit auseinander

Aussagen von Führungskräften in mittleren und großen Unternehmen, die täglich IT-Angriffen ausgesetzt sind:



„Neben allen intern zu ergreifenden Maßnahmen wünschen Unternehmen auch den Austausch mit staatlichen Stellen. Den Einsatz eines übergeordneten Warnsystems oder Informationen über neue Angriffs- sowie Schutzmöglichkeiten empfänden Unternehmen als wertvollen Beitrag, ebenso die konkrete Unterstützung im Angriffsfall."

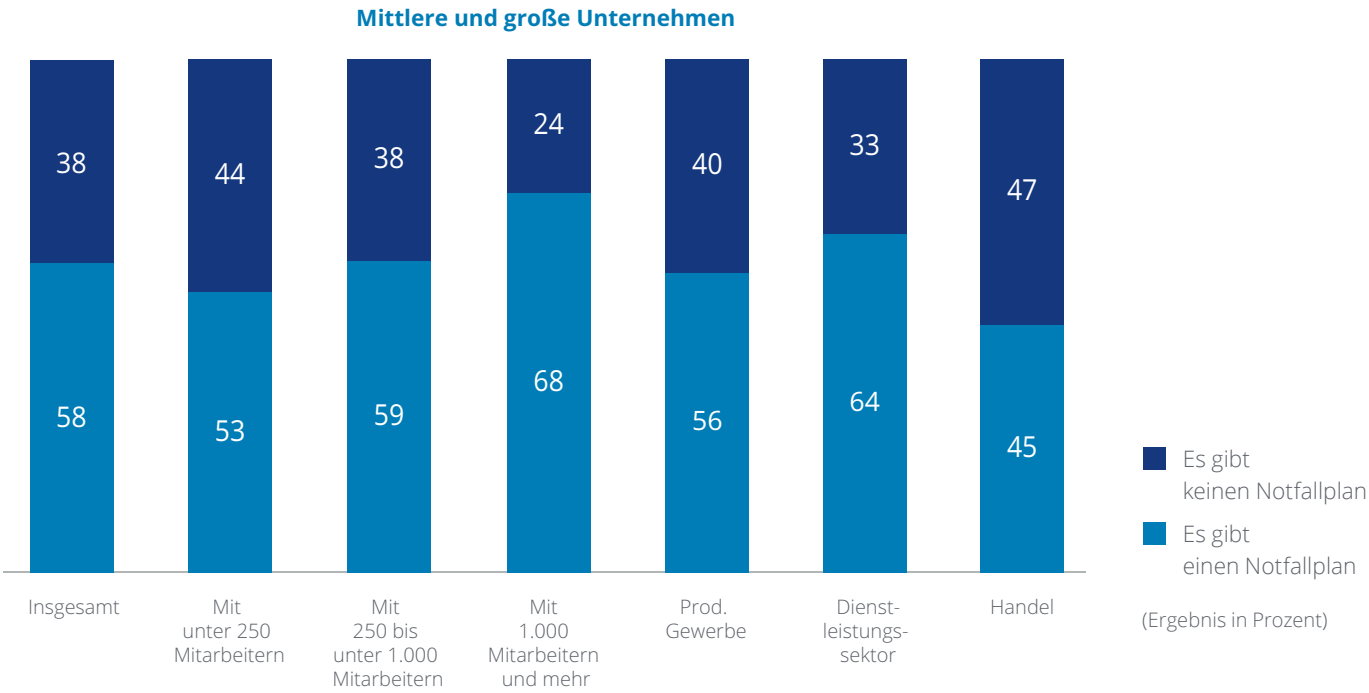
Katrin Rohmann, Public Sector Leader

Die Ausgaben für die Informationssicherheit sind in 42 Prozent der großen und mittleren Unternehmen in den letzten Jahren deutlich gestiegen, in weiteren 40 Prozent etwas gestiegen. Aber Notfallpläne oder ein Krisenmanagementsystem für den Fall eines erfolgreichen Cyber-Angriffs gegen das eigene Unternehmen gibt es in mehr als jedem dritten Unternehmen nicht. Selbst unter großen Unternehmen mit 1.000 und mehr Mitarbeitern besteht hier in rund jedem vierten Fall ein Defizit.

Ein Notfallplan, besonders ein Cyber-Incident-Response-Plan, hilft Unternehmen, bei Cyber-Angriffen angemessen auf die Bedrohungen zu reagieren. Der Notfallplan hat die Wiederherstellung von Daten und IT-Infrastrukturen nach einem Vorfall zum Ziel, was ohne einen solchen oftmals problematisch ist. Unsere Umfrage zeigt, dass derartige Pläne in 38 Prozent der Unternehmen nicht vorhanden sind.

Abb. 13 – Oftmals gibt es keine Notfallpläne für den Fall eines Cyber-Angriffs

Notfallpläne
Bei über einem Drittel der Unternehmen gibt es keine Notfallpläne für den Fall eines Cyber-Angriffs.



5. Verantwortung und Kompetenz im Unternehmen

Mit dem seit Juli 2015 gültigen Informationssicherheitsgesetz (IT-SiG) leistete die Bundesregierung einen Beitrag, die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit zu machen.[4] Insbesondere für Unternehmen, die kritische Infrastrukturen betreiben, gilt das Informationssicherheitsgesetz. Demnach müssen die Betreiber effektive Sicherheitsmaßnahmen etablieren. Doch auch Unternehmen, die nicht unter das IT-Sicherheitsgesetz fallen, sollten sich um Cyber-Security und ein IT-Risikomanagement kümmern. Die Aussagen der Befragten zu Häufigkeit der Angriffe und möglichen Schadenspotenzialen belegen, dass diese Risiken in vielen Unternehmen zu den identifizierten Gefahren gehören, denen im Rahmen eines internen Kontrollsystems und Risikomanagements zu begegnen ist.

Die Notwendigkeit, angemessene Maßnahmen zur Informationssicherheit zu implementieren und sich auf IT-Sicherheitsvorfälle vorzubereiten, wird nach wie vor in den meisten Unternehmen als Expertenaufgabe gesehen. Cyber-Angriffe jedoch bergen Risiken, die ein Unternehmen in seiner Existenz gefährden oder wesentlich in seiner Entwicklung beeinträchtigen können. Damit liegt die Verantwortung nicht allein bei den IT-Experten, sondern ausdrücklich auch bei der Unternehmensführung und dem Aufsichtsrat.

„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."

(§ 91 Abs. 2 AktG)

[4] BSI (2017): https://www.bsi.bund.de, abgerufen am 21.11.2017.

Der Deutsche Corporate Governance Kodex empfiehlt international und national anerkannte Standards guter und verantwortungsvoller Unternehmensführung und regt auch dazu an, dass die Unternehmensführung für ein angemessenes Risikomanagement und Risikocontrolling sorgen sollte. Darunter ist auch ein angemessenes Cyber-Security-Management zu verstehen.

Je nach gewählter Rechtsform des Unternehmens sind verschiedene Rechtsgrundlagen aus haftungsrechtlicher Sicht einschlägig, um diese Sorgfaltspflicht der Unternehmensführung herzuleiten. § 91 Abs. 2 AktG entfaltet Ausstrahlungswirkung auch auf andere Rechtsformen.

IT-Risiken gehören, wenn sie für ein Unternehmen als bedeutend eingestuft werden, zu den in ein umfassendes Risikomanagement einzubindenden Risikoarten. Die Implementierung eines Risikomanagementsystems gehört unabdingbar zu den Sorgfaltspflichten eines Vorstandes oder einer Geschäftsführung.

Konkret für die Informationssicherheit eines Unternehmens heißt das, basierend auf einer Risikostrategie ein funktionierendes IT- und Informationssicherheitsmanagement einzurichten. Die Risikoidentifikation durch eine regelmäßige und systematische Analyse interner und externer Faktoren bildet hierbei die Basis einer Risikobewertung. Weitere Bestandteile sind eine Risikokommunikation im Rahmen einer regelmäßigen Berichterstattung und die Etablierung einer Risikokultur sowie eines Risikobewusstseins im Unternehmensalltag.

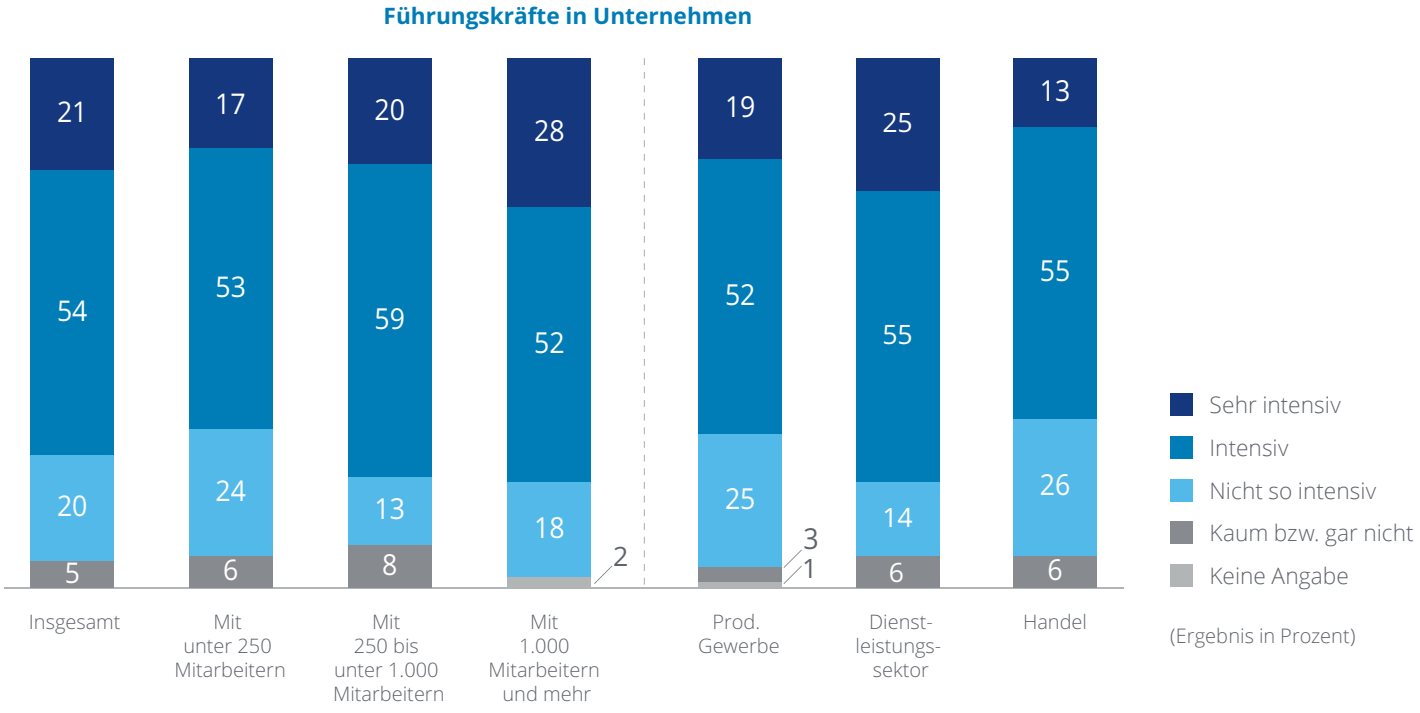
Herauszustellen ist, dass eine effektive Cyber-Security wie alle Maßnahmen zur Risikoerkennung und zum Risikomanagement eine fortlaufende Tätigkeit der Unternehmensführung erfordert. Es sollten nicht nur einmalig Sicherheitsmaßnahmen entwickelt, implementiert und durchgeführt werden, sondern vielmehr müssen diese Maßnahmen vor dem Hintergrund der Entwicklung der Risiken und sich verändernder Abläufe und Unternehmensprozesse stetig auf ihre Effizienz überprüft, angepasst und verbessert werden.

Fortlaufende Überwachung und Verbesserung können von der Unternehmensführung nicht allein erfüllt werden. Vielmehr kann sie diese Aufgaben ordnungsgemäß auch an fachkundige Personen delegieren, diese einweisen und überwachen.
In vielen Unternehmen wird die Funktion des Chief Information Security Officer (CISO) mit dem Thema Cyber-Security betraut. Ein Datenschutzbeauftragter hat sein spezielles Themenfeld im Blick. Mit der Verantwortung für die physische Sicherheit ist in der Regel die Corporate Security betraut. Alle diese Funktionen müssen effektiv zusammenwirken, um die erforderliche Informationssicherheit im Unternehmen zu gewährleisten.

Die Unternehmensführung ist ebenso dafür verantwortlich, dass eine angemessene und wirksame interne Revision implementiert ist. Dabei sollte sichergestellt sein, dass auch die interne Revision regelmäßig die umgesetzten Maßnahmen für Cyber-Sicherheit auf Aktualität, Relevanz und Effektivität überprüft.

In drei Viertel der befragten Unternehmen beschäftigt sich die Unternehmensführung intensiv oder sogar sehr intensiv mit dem Thema Cyber-Security. Das bedeutet aber allerdings im Umkehrschluss, dass in jedem vierten Unternehmen die Unternehmensführung weniger intensiv bis gar nicht mit dem Thema befasst ist. Unter großen Unternehmen mit 1.000 und mehr Mitarbeitern liegt dieser Anteil bei immerhin rund einem Fünftel. In zwei Dritteln der Unternehmen beschäftigt sich die Unternehmensführung regelmäßig mit dem Thema Cyber-Security, in mehr als jedem vierten Fall allerdings nur anlassbezogen.

Abb. 14 – Cyber-Sicherheit Chefsache?
Grundsätzlich intensive Beschäftigung der Geschäftsleitungsebene mit dem Thema Cyber-Security

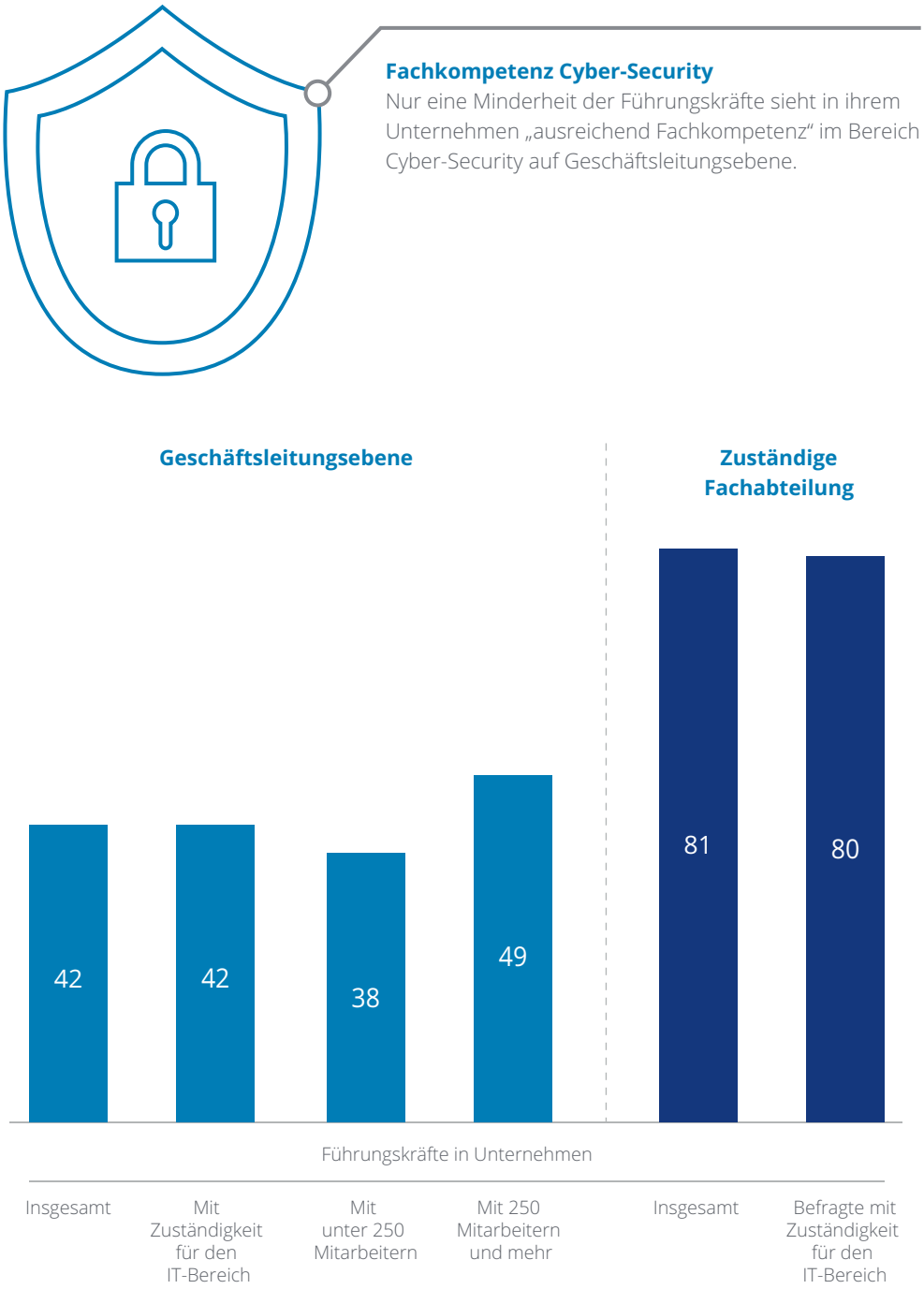


jedoch in **33%** der Unternehmen nur anlassbezogen oder gar nicht!

Die Kompetenz von Vorstand oder Geschäftsführung für Cyber-Security wird von den Führungskräften aber eher skeptisch gesehen. Nur 42 Prozent halten die Fachkompetenz in diesem Thema auf Geschäftsleitungsebene für ausreichend.

Den eigenen Fachabteilungen wird dagegen deutlich größeres Vertrauen entgegengebracht. 81 Prozent der befragten Führungskräfte bescheinigen ihnen ausreichende Kompetenz.

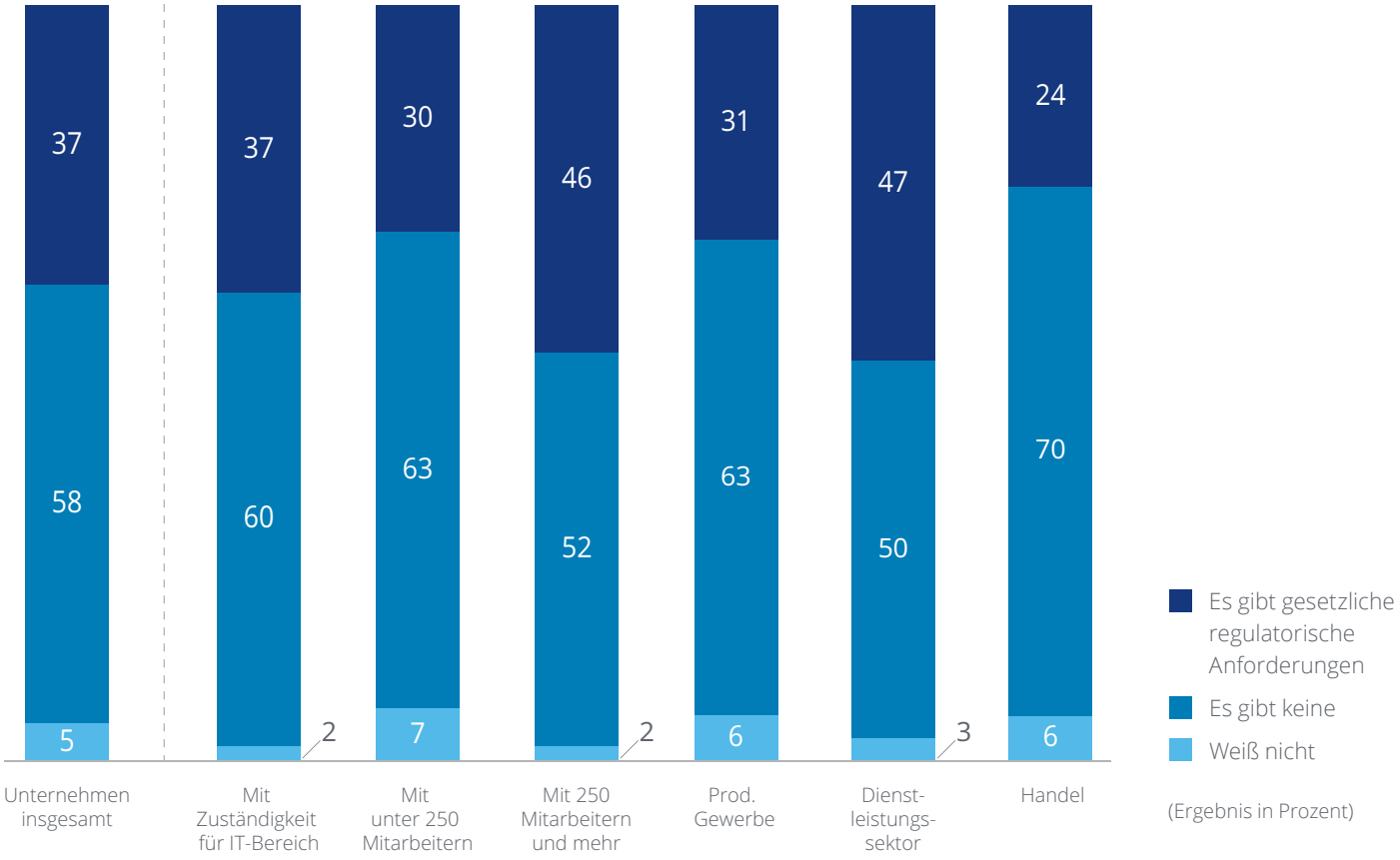
Abb. 15 – Fachkompetenz auf der Geschäftsleitungsebene ausbaufähig



(Ergebnis in Prozent)

Von gesetzlichen oder regulatorischen Anforderungen an ihr Unternehmen im Bereich Informationssicherheit berichten 37 Prozent der Führungskräfte. Die Mehrheit – auch die Mehrheit der Führungskräfte, die für den IT-Bereich in ihrem Unternehmen zuständig sind, – ist überzeugt, dass solche für sie nicht gelten.

Abb. 16 – Wissen um gesetzliche/regulatorische Anforderungen



„Es ist beachtenswert, dass einem Großteil der Führungskräfte die regulatorischen Anforderungen an ihr Unternehmen im Bereich Cyber-Security häufig unbekannt sind. Das macht es Entscheidern schwierig, in Anlehnung an den IT-Grundschutz systematisch vorzugehen und notwendige Informationssicherheitsmaßnahmen zu erkennen und umzusetzen."

Peter J. Wirnsperger, Cyber Risk Leader

Dem Aufsichtsrat obliegt die regelmäßige und proaktive Überwachung der Unternehmensführung und der von ihr implementierten Maßnahmen zur Umsetzung der Unternehmensstrategie inklusive der Risikostrategie.

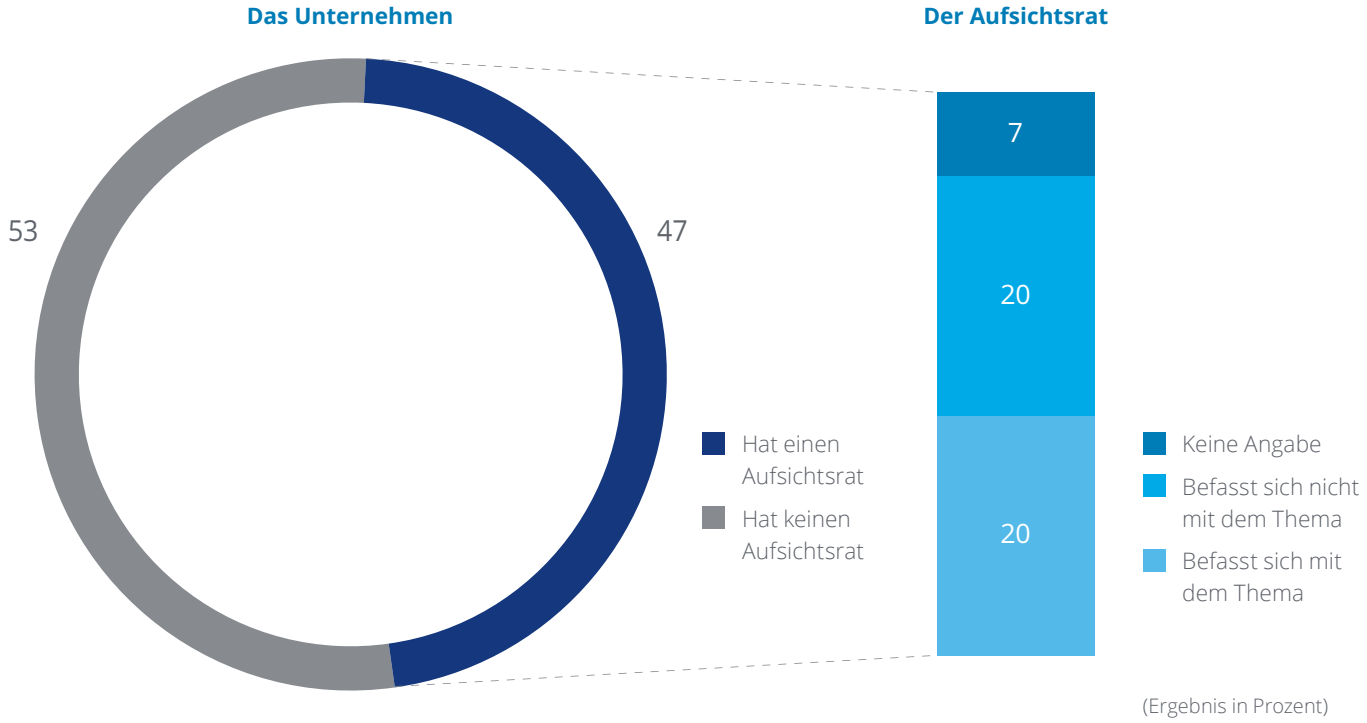
Somit spielt er eine wichtige Rolle bei der Überwachung der Wirksamkeit des internen Kontrollsystems und des Risikomanagementsystems auch auf dem Gebiet der Cyber-Security und bei der Beurteilung der Wirksamkeit der hierzu ergriffenen Managementmaßnahmen. Der Aufsichtsrat ist auch für die Überwachung der Wirksamkeit des internen Revisionssystems zuständig.

In den befragten Unternehmen, die über einen Aufsichtsrat verfügen, nimmt sich dieser nur in rund der Hälfte der Fälle auch das Thema Cyber Risks in den Blick.

„Der Aufsichtsrat hat die Geschäftsführung zu überwachen."

(§ 111 Abs. 1 AktG)

Abb. 17 – Aufsichtsräte und das Thema Cyber-Risiken
Aufsichtsräte befassen sich nur in etwa der Hälfte der Fälle mit dem Thema "Cyber-Risiken"



6. Handlungsempfehlungen

Umsetzen der gesetzlichen Verpflichtungen
Die Unternehmensführung sollte Maßnahmen zur Cyber-Security als integralen Bestandteil ihrer Verpflichtung zur Schaffung einer effizienten sowie angemessenen Risikofrüherkennung und Überwachung aufnehmen und die entsprechenden Maßnahmen als wichtigen Bestandteil in das Risikomanagementsystem des Unternehmens integrieren. Bei Gefährdungen, die als bedeutend eingestuft werden, ist Cyber-Security eindeutig Chefsache!

Risikofaktor Mensch
Die Stärkung der Eigenverantwortung von Mitarbeitern und die Schaffung eines Risikobewusstseins sollten einen hohen Stellenwert genießen. Neben den technischen Maßnahmen ist das Sicherheitswissen der Mitarbeiter stets aufzufrischen und sie so zu sensibilisieren, dass eine hohe Motivation zur Anwendung aller nicht-technischen Maßnahmen erreicht werden kann.

Cyber-Kompetenz der Unternehmensführung und des Aufsichtsrates
Steht die Unternehmensführung für das Thema operativ in der Verantwortung und wird dies durch den Aufsichtsrat überwacht, müssen beide Gremien über die dafür notwendige Kompetenz verfügen. Die Unternehmensführung sollte ein Grundverständnis über die Wirkungsketten von Cyber-Bedrohungen haben und stets über Risiken im Cyber-Raum und die Effizienz der Sicherheitsmaßnahmen unterrichtet werden. Der Aufsichtsrat sollte proaktiv die ergriffenen Maßnahmen der Unternehmensführung überwachen.

Richtlinien, Anweisungen und Notfallpläne aufstellen und umsetzen
Angesichts der großen Unsicherheit bei möglichen Sicherheitsvorfällen sind Richtlinien, Anweisungen und Notfallpläne in schriftlicher Form festzuhalten, fortlaufend zu aktualisieren und jedem verfügbar zu machen. Insbesondere ein Cyber-Incident-Response-Plan hilft Unternehmen, Bedrohungen zu erkennen und auf Cyber-Angriffe angemessen zu reagieren. Er ermöglicht die Wiederherstellung von Daten sowie IT-Infrastrukturen und somit die schelle Wiederaufnahme des Geschäftsbetriebs nach einem Vorfall.
Das Vorgehen für den Notfall muss geübt werden, moderne Methoden wie Red Teaming oder War Gaming können helfen, sicher und routiniert im Ernstfall zu agieren.

Diskrepanz zwischen Bedrohungslage und Schutzniveau begegnen
Die sich stets erhöhende Zahl an Cyber-Angriffen steht einer großen Zahl an Wirtschaftsführern und Politikern gegenüber, die an den Vorbereitungen auf Sicherheitsvorfälle zweifeln. Unternehmen müssen kontinuierlich ihre Gefährdung analysieren und jederzeit ihren Mix von technischen sowie nicht-technischen Maßnahmen der Bedrohungslage anpassen. Diese Maßnahmen zur Informationssicherheit müssen in ein funktionsfähiges Gesamtrisikomanagement integriert sein.

Ansprechpartner

Katrin Rohmann
Public Sector Leader
Tel: +49 (0)30 25468 127
krohmann@deloitte.de

Peter J. Wirnsperger
Cyber Risk Leader
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Deloitte.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen des Einzelfalls gerecht zu werden, und ist nicht dazu bestimmt, Grundlage für wirtschaftliche oder sonstige Entscheidungen zu sein. Weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited, noch ihre Mitgliedsunternehmen oder deren verbundene Unternehmen (insgesamt das „Deloitte Netzwerk") erbringen mittels dieser Veröffentlichung professionelle Beratungs- oder Dienstleistungen. Keines der Mitgliedsunternehmen des Deloitte Netzwerks ist verantwortlich für Verluste jedweder Art, die irgendjemand im Vertrauen auf diese Veröffentlichung erlitten hat.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL"), eine „private company limited by guarantee" (Gesellschaft mit beschränkter Haftung nach britischem Recht), ihr Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen. DTTL und jedes ihrer Mitgliedsunternehmen sind rechtlich selbstständig und unabhängig. DTTL (auch „Deloitte Global" genannt) erbringt selbst keine Leistungen gegenüber Mandanten. Eine detailliertere Beschreibung von DTTL und ihren Mitgliedsunternehmen finden Sie auf www.deloitte.com/de/UeberUns.

Deloitte erbringt Dienstleistungen in den Bereichen Wirtschaftsprüfung, Risk Advisory, Steuerberatung, Financial Advisory und Consulting für Unternehmen und Institutionen aus allen Wirtschaftszweigen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Mit einem weltweiten Netzwerk von Mitgliedsgesellschaften in mehr als 150 Ländern verbindet Deloitte herausragende Kompetenz mit erstklassigen Leistungen und unterstützt Kunden bei der Lösung ihrer komplexen unternehmerischen Herausforderungen. Making an impact that matters – für rund 263.900 Mitarbeiter von Deloitte ist dies gemeinsames Leitbild und individueller Anspruch zugleich.

Stand 12/2017