CYBER SECURITY REPORT 2015

ERGEBNISSE EINER REPRÄSENTATIVEN BEFRAGUNG
VON ABGEORDNETEN SOWIE TOP-FÜHRUNGSKRÄFTEN
IN MITTLEREN UND GROSSEN UNTERNEHMEN

INHALT

Herausgeber
Deutsche Telekom/T-Systems

Konzeption und Durchführung der Studie
Institut für Demoskopie Allensbach
Allensbach am Bodensee

Centrum für Strategie und Höhere Führung
Bodman am Bodensee

Ansprechpartner
Harald Lindlar
harald.lindlar@telekom.de

Prof. Dr. Klaus Schweinsberg
klaus.schweinsberg@glh-online.com

IfD Allensbach
Institut für Demoskopie Allensbach

glh CENTRUM FÜR STRATEGIE UND HÖHERE FÜHRUNG

VORBEMERKUNGEN

Bereits im fünften Jahr in Folge hat das **INSTITUT FÜR DEMOSKOPIE ALLENSBACH** im Auftrag von **T-SYSTEMS** sowie in Kooperation mit dem **CENTRUM FÜR STRATEGIE UND HÖHERE FÜHRUNG** Topentscheider aus Politik und Wirtschaft nach ihrer allgemeinen Risikoeinschätzung sowie ausgewählten Themen im Bereich „Cyber Security" befragt. Die inzwischen fünfte Welle des Cyber Security Reports erlaubt damit für zahlreiche Fragen eine Betrachtung im Zeitverlauf. Diese unterstreicht, dass Cyber- und Datenrisiken aus Sicht der Entscheider in Politik und Wirtschaft weiterhin ein hohes Gefahrenpotenzial für Deutschland, seine Bürger und die Unternehmen darstellen.

Neben den Trendfortschreibungen in Bezug auf die Einschätzung von Risiken aus verschiedenen Lebensbereichen, dem Stellenwert der IT-Sicherheit im eigenen Unternehmen, der Bedrohung durch IT-Angriffe, der Bewertung der staatlichen Fachkompetenz im Bereich IT-Sicherheit sowie der Bedeutung unternehmensübergreifender Initiativen für IT-Sicherheit stellt das Thema „Industrie 4.0" einen großen Schwerpunkt in diesem Jahr dar. Die intelligente Vernetzung von Menschen, Maschinen und industriellen Prozessen gilt als eine der derzeit tiefgreifendsten Veränderungen im verarbeitenden Gewerbe und in den damit zusammenhängenden Wirtschaftsbereichen wie der Logistik. Nach der Erfindung der Dampfmaschine, der Massenfertigung mithilfe von Fließbändern und elektrischer Energie sowie dem Einsatz von Elektronik und IT zur weiteren Automatisierung der Produktion soll mit dem Begriff „Industrie 4.0" die Dimension dieser Veränderung signalisiert werden.

Der diesjährige Cyber Security Report liefert auf breiter statistischer Basis ein repräsentatives Meinungsbild von Entscheidern aus Wirtschaft und Politik zur Einschätzung des Potenzials von Industrie 4.0, der Chancen und Risiken sowie des Umsetzungsstands in den Unternehmen. Da die Veränderungen in den Produktionsprozessen vor allem für Industrieunternehmen von Bedeutung sind, wurden Unternehmen aus dem verarbeitenden Gewerbe überproportional in der Stichprobe berücksichtigt. Konkret wurden 293 Führungskräfte aus dem verarbeitenden Gewerbe befragt. Eine faktorielle Gewichtung stellte sicher, dass die Unternehmen des verarbeitenden Gewerbes in den Gesamtergebnissen entsprechend ihrem tatsächlichen Anteil berücksichtigt wurden. Die Gesamtergebnisse sind damit also weiterhin repräsentativ für die Gesamtheit der mittleren und großen Unternehmen aus allen Branchen.

Die Studie stützt sich auf insgesamt 645 telefonisch zwischen Ende August bis Anfang Oktober durchgeführte Interviews mit einem repräsentativen Querschnitt von Politikern sowie Top-Führungskräften aus mittleren und großen Unternehmen. Als Entscheider aus der Politik wurden 113 Abgeordnete aus dem Bundestag, den Landtagen und deutsche Abgeordnete aus dem Europaparlament befragt. Bei den Entscheidern in der Wirtschaft wurden insgesamt 532 Führungskräfte aus großen und mittleren Unternehmen befragt, darunter 247 Führungskräfte aus großen Unternehmen und 285 Führungskräfte aus mittleren Unternehmen. Zu den großen Unternehmen zählen gemäß Definition der EU-Kommission Unternehmen mit 250 und mehr Beschäftigten und/oder mehr als 50 Mio. Euro Jahresumsatz. Mittlere Unternehmen sind als Unternehmen definiert, die zwischen 50 und 249 Mitarbeitern haben und/oder einen Jahresumsatz von 10 bis höchstens 50 Mio. Euro erzielen. Die befragten Unternehmen repräsentieren aufgrund ihrer Größenordnung zwar gut rund 2 Prozent aller Unternehmen in Deutschland, erwirtschaften aber rund 80 Prozent aller umsatzsteuerpflichtigen Waren und Dienstleistungen und beschäftigen circa zwei Drittel aller sozialversicherungspflichtig Arbeitnehmer in Deutschland.

Die Exklusivität der befragten Führungskräfte leitet sich aber nicht nur aus der Größe ihrer Unternehmen, sondern auch aus ihrer Stellung in diesen Unternehmen ab. Gut zwei Drittel, und damit der überwiegende Teil, gehörte der ersten Führungsebene (Vorstände, Geschäftsführer, Inhaber) an. Knapp ein Drittel, vorrangig in den Großunternehmen, verfügt – beispielsweise als Bereichsleiter – ebenfalls über eine herausgehobene Position im eigenen Unternehmen.

IT- UND DATENRISIKEN ALS GESELLSCHAFTLICHE RISIKEN AUS SICHT DER ENTSCHEIDER

Aus Sicht der Entscheider aus Politik und Wirtschaft stellen Cybergefahren und Datenschutzverletzungen unter 20 Risiken aus allen Lebensbereichen das größte Risikopotenzial für die Bevölkerung in Deutschland dar. Unter den sieben größten Risiken finden sich erneut fünf wieder, die mit IT- und Datensicherheit zusammenhängen: 70 Prozent der Entscheider sehen Computerviren als großes Risiko an, 67 Prozent den Datenbetrug im Internet, 63 Prozent den Missbrauch von persönlichen Daten durch andere Nutzer in sozialen Netzwerken, 52 Prozent den Missbrauch von persönlichen Daten durch Unternehmen. Eine andere Facette der IT- und Datensicherheit ist die staatliche Überwachung der Bürger, insbesondere der Internet- oder Telefonverbindungen: 49 Prozent der Entscheider sehen in der Überwachung deutscher Bürger durch ausländische Staaten ein großes Risiko für die Bevölkerung, 19 Prozent in der Überwachung durch den deutschen Staat.

Im Vergleich zu den einzelnen IT- und Datenrisiken werden von den Politikern und Führungskräften in mittleren und großen Unternehmen nur Risiken im Kontext von Alter und demografischem Wandel als ähnlich bedeutsam eingestuft: So sehen 66 Prozent der Entscheider die Pflegebedürftigkeit im Alter, 52 Prozent das Thema Altersarmut als großes Risiko für die Bevölkerung an.

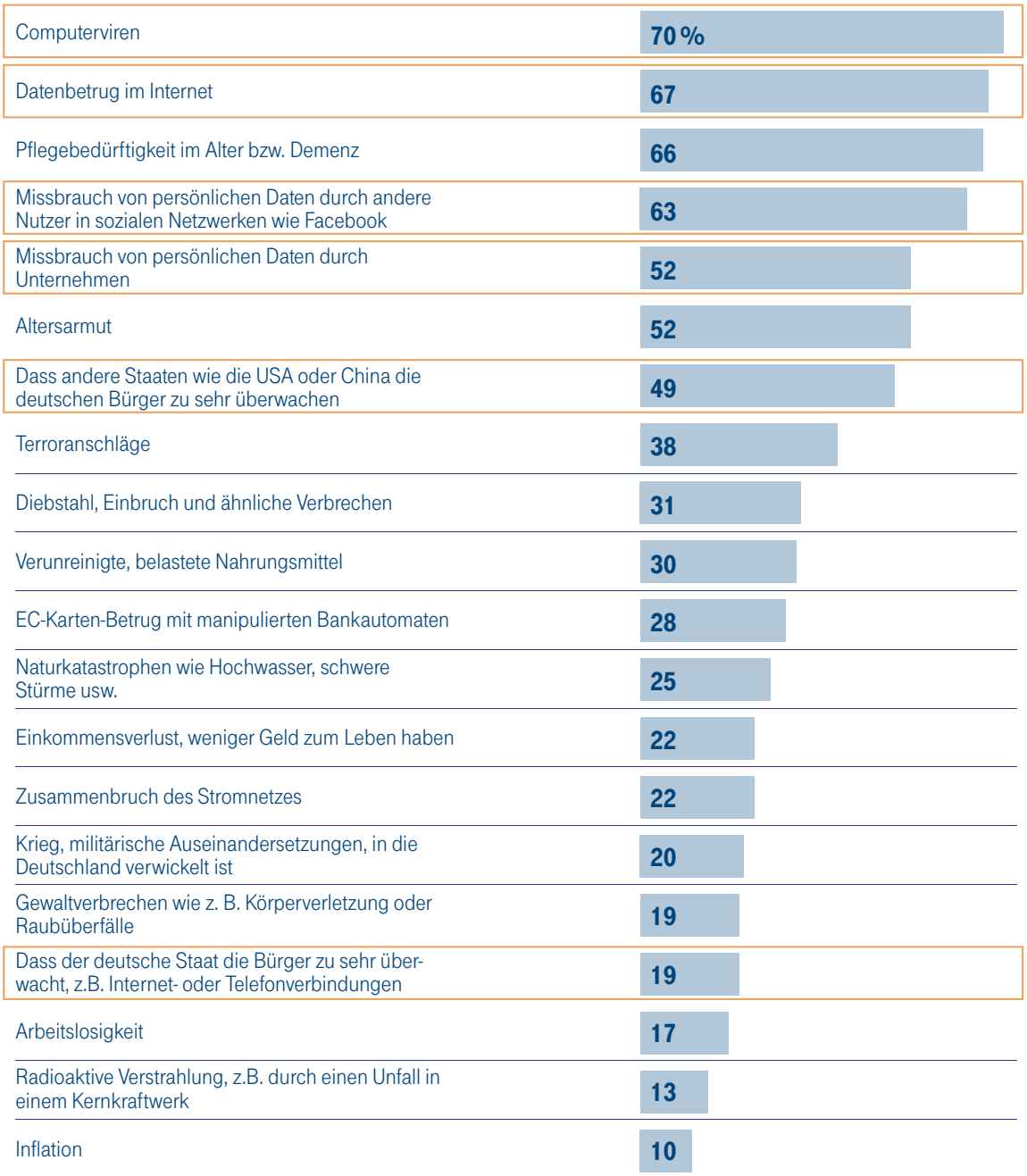
Andere Risiken folgen erst mit deutlichem Abstand: Terroranschläge stellen für 38 Prozent der Entscheider ein großes Risiko dar; Diebstahl, Einbruch und ähnliche Straftaten folgen mit 31 Prozent. Materielle Risiken wie Einkommensverlust, Arbeitslosigkeit und Inflation spielen mit 22, 17 bzw. 10 Prozent aus Sicht der Entscheider eine eher nachrangige Rolle für die Menschen in Deutschland **(Schaubild 1)**.

Schaubild 1

DIE RISIKOWAHRNEHMUNG VON ENTSCHEIDERN AUS POLITIK UND WIRTSCHAFT

Frage: „Ich lese Ihnen jetzt mögliche Risiken und Gefahren für die Menschen in Deutschland vor und Sie sagen mir bitte jeweils, ob das Ihrer Meinung nach für die Menschen in Deutschland ein großes Risiko, eine große Gefahr oder ein weniger großes Risiko oder nur ein geringes Risiko bzw. gar kein Risiko darstellt."

Das stellt für die Menschen in Deutschland ein großes Risiko dar –

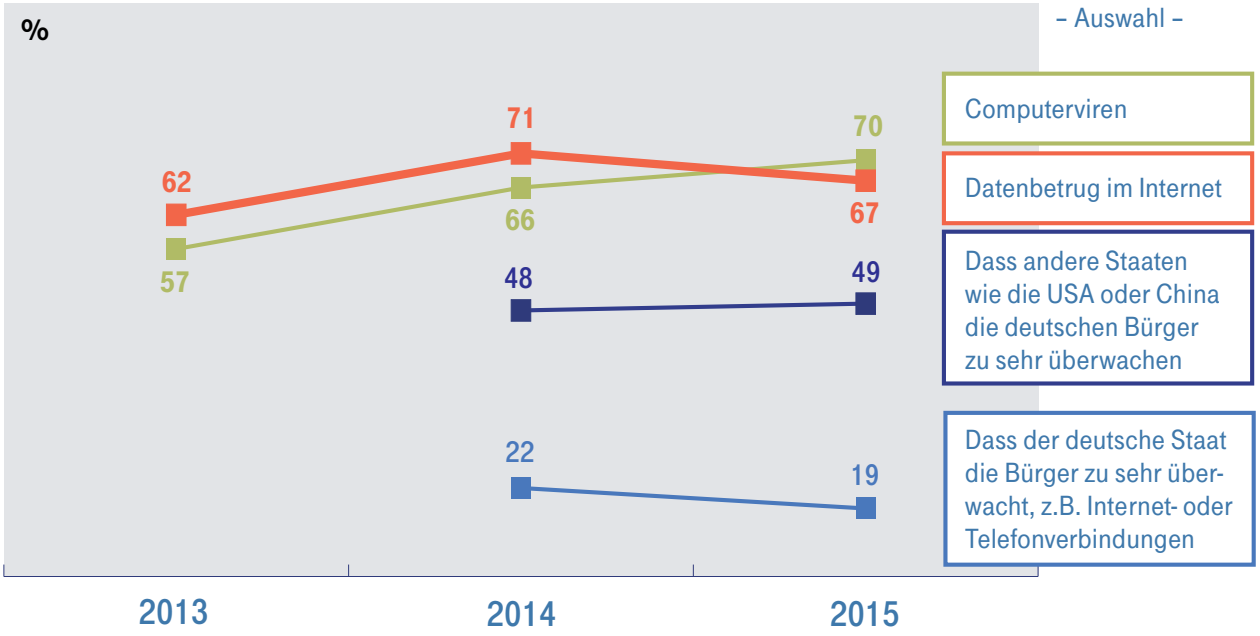


Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Schaubild 2

ENTWICKLUNG DES GESELLSCHAFTLICHEN RISIKOPOTENZIALS VON CYBER- UND DATENRISIKEN IN DEN LETZTEN JAHREN

Das stellt aus der Sicht der Entscheider ein
großes Risiko für die Menschen in Deutschland dar –



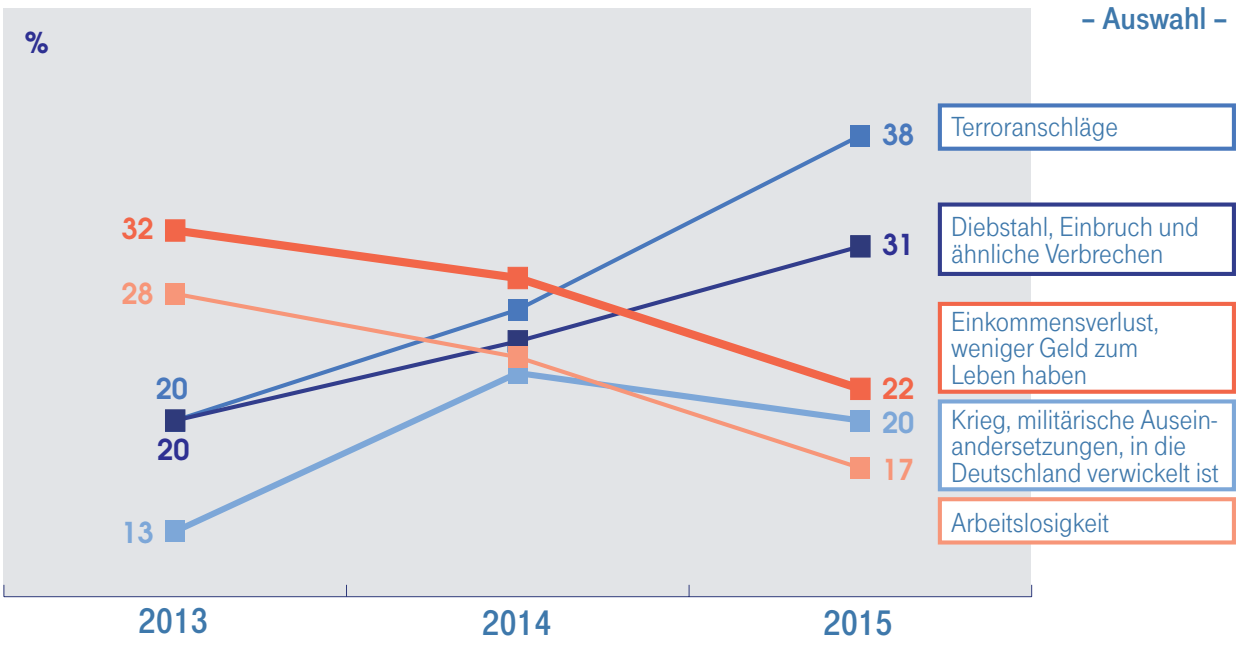
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7231(September 2015)

Die Entscheider stufen Cyberrisiken damit als unvermindert hoch ein. Bei Computerviren ist sogar ein weiterer Anstieg des Risikopotenzials erkennbar. So stufen 70 Prozent der Entscheider Computerviren als große Bedrohung für Deutschland ein, im vergangenen Jahr waren es erst 66 Prozent, vor zwei Jahren 57 Prozent. Andere Cyber- und Datenrisiken werden, auf teilweise hohem Niveau, ähnlich eingeschätzt wie in den letzten zwei Jahren. Die Sicherheitsgefährdung, die von Datenbetrug im Internet ausgeht, wird mit 67 Prozent ähnlich hoch eingestuft wie 2014. Gleiches gilt für das Überwachungsrisiko durch andere Staaten wie die USA oder China. Waren es vor einem Jahr 48 Prozent der Entscheider, die dieses Risiko als hoch einstuften, sind es aktuell 49 Prozent **(Schaubild 2)**.

Schaubild 3

ENTWICKLUNG ANDERER RISIKEN IN DEN LETZTEN JAHREN AUS SICHT DER ENTSCHEIDER

Das stellt aus der Sicht der Entscheider ein
großes Risiko für die Menschen in Deutschland dar –



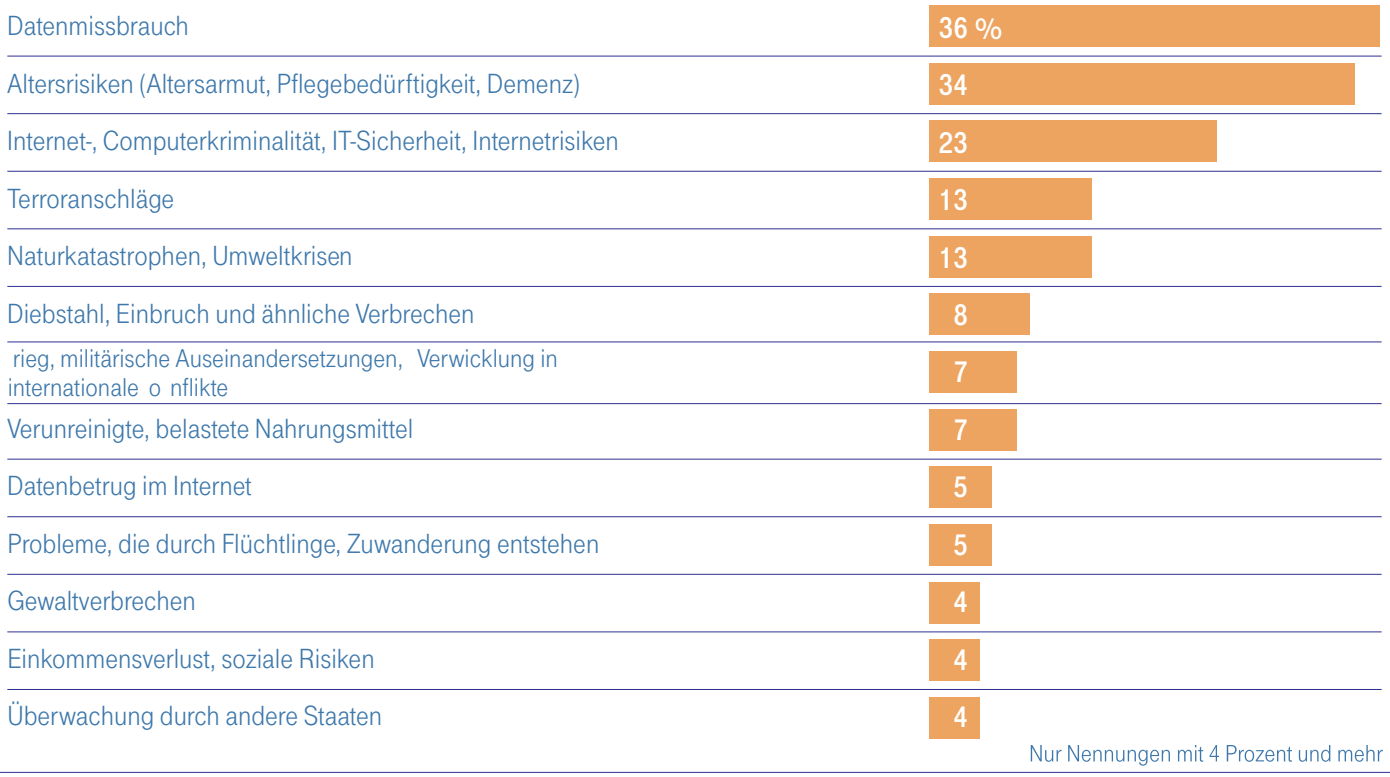
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7231(September 2015)

Materielle Risiken haben hingegen vor dem Hintergrund der guten gesamtwirtschaftlichen Entwicklung erneut an Bedeutung verloren. So sehen aktuell beispielsweise nur 17 Prozent der Entscheider in der Arbeitslosigkeit ein großes Risiko für die Bevölkerung in Deutschland, in den beiden Jahren zuvor waren es 24 Prozent bzw. 28 Prozent. Demgegenüber ist die Einschätzung des Gefährdungspotenzials durch Diebstahl, Einbruch und ähnliche Verbrechen ebenso wie durch Terroranschläge seit 2013 kontinuierlich gestiegen. Knapp jeder dritte Entscheider sieht inzwischen Diebstahl- und Einbruchsdelikte als großes gesellschaftliches Risiko an, vor zwei Jahren waren es lediglich 20 Prozent. Mit Blick auf die Gefährdung durch Terroranschläge hat sich das Risikopotenzial in den letzten beiden Jahren sogar fast verdoppelt. 2013 stellten Terroranschläge für 20 Prozent der Entscheider ein großes Risiko für die Menschen in Deutschland dar, aktuell sind es 38 Prozent **(Schaubild 3)**.

Schaubild 4

RISIKEN, DIE AUS SICHT DER ENTSCHEIDER AUS POLITIK UND WIRTSCHAFT STARK ZUNEHMEN WERDEN

Frage: „Wie ist Ihre Einschätzung: Welche der genannten Risiken werden in Zukunft besonders stark zunehmen?“ (offene Ermittlung, ohne Antwortvorgaben)



Nur Nennungen mit 4 Prozent und mehr

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

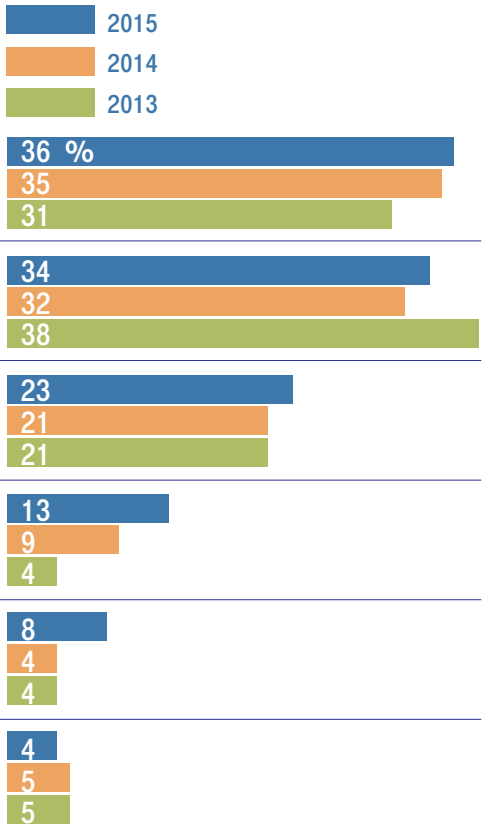
Die Entscheider aus Politik und Wirtschaft wurden nicht nur um ihre derzeitige Risikobewertung gebeten, sondern auch um eine Einschätzung, welche Risiken aus ihrer Sicht künftig besonders stark zunehmen werden. Da die Abfrage zur künftigen Risikoentwicklung als offene, ungestützte Frage (also ohne konkrete Antwortvorgaben) erfolgte, ist ein Vergleich der absoluten Werte mit der derzeitigen Risikobewertung nicht möglich. Umso bemerkenswerter ist dafür die Deutlichkeit, mit der die Politiker und Führungskräfte aus mittleren und großen Unternehmen Cyber- und Datenrisiken ganz spontan als herausragende Zukunftsgefahren benennen. 36 Prozent verweisen auf den Datenmissbrauch als wachsende Gefahrenquelle, 23 Prozent auf Internet- und Computerkriminalität sowie die IT-Sicherheit generell, 5 Prozent rechnen mit einer besonders starken Zunahme von Datenbetrug im Internet. Dass mindestens eines dieser drei Risiken künftig stark zunehmen wird, wird von 56 Prozent der Entscheider erwartet. Damit werden aus Sicht von Abgeordneten und Führungskräften in der Wirtschaft IT- und Datenrisiken künftig noch stärker zunehmen als Altersrisiken wie Altersarmut und Pflegebedürftigkeit, die nach Meinung von 34 Prozent der Entscheider stark zunehmen werden **(Schaubild 4)**.

Auch die Erwartungen zu künftigen Risikoentwicklungen unterstreichen die zuvor beschriebenen Trends. So gehen mit 36 Prozent erneut mehr Entscheider als in den Vorjahren davon aus, dass das Risiko von Datenmissbrauch künftig stark zunehmen wird. Gleiches gilt – auf insgesamt niedrigerem Niveau – für Terroranschläge und Diebstahl- bzw. Einbruchskriminalität. Erwarteten im Jahr 2013 lediglich 4 Prozent der Entscheider ein steigendes Risiko durch Terroranschläge, waren es 2014 9 Prozent und aktuell sind es 13 Prozent. Für Diebstahl, Einbruch und ähnliche Verbrechen sahen vor zwei Jahren ebenfalls erst 4 Prozent ein zunehmendes Risiko, derzeit sind es 8 Prozent **(Schaubild 5)**.

Schaubild 5

RISIKEN, DIE AUS SICHT DER ENTSCHEIDER STARK ZUNEHMEN WERDEN – VERGLEICH ZU DEN VORJAHREN

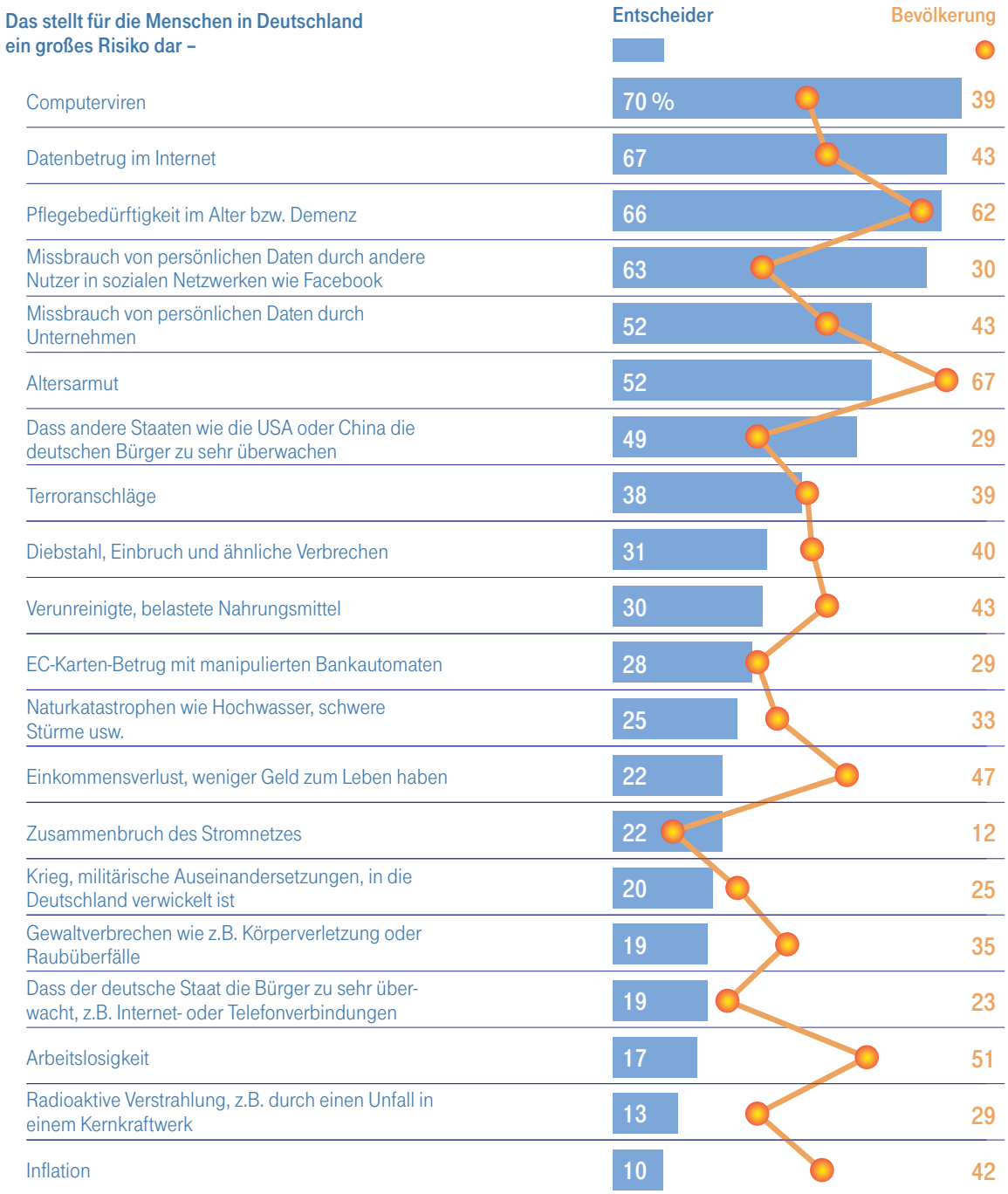
Diese Risiken werden nach Einschätzung der Entscheider stark zunehmen
(offene Ermittlung, ohne Antwortvorgaben)
– Auswahl –



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7231

Schaubild 6

RISIKOWAHRNEHMUNG VON BEVÖLKERUNG UND ENTSCHEIDERN IM VERGLEICH



Basis: Bundesrepublik Deutschland, Bevölkerung ab 16 Jahren, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen

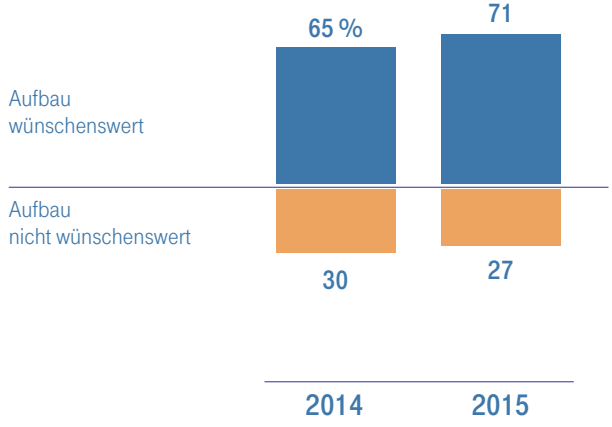
Quelle: Allensbacher Archiv, IfD-Umfragen 11040 (Juni 2015), 7231 (September 2015)

Wie in früheren Jahren unterscheiden sich die Entscheider in ihrer Einschätzung gesellschaftlich relevanter Risiken teilweise erheblich vom Bevölkerungsdurchschnitt. Dies zeigt der direkte Vergleich der Einschätzungen von Entscheidern und Bevölkerung. Die Entscheider aus Politik und Wirtschaft messen Cyber- und Datenrisiken mehr Bedeutung bei als die Bevölkerung, die Bevölkerung sieht hingegen vor allem in materiellen Risiken, aber auch der klassischen Kriminalität das höhere Bedrohungspotenzial. So stellen Computerviren für 70 Prozent der Entscheider, aber nur für 39 Prozent der Bevölkerung ein großes gesellschaftliches Risiko dar. Dass andere Staaten wie die USA oder China deutsche Bürger überwachen, sehen 49 Prozent der Entscheider, aber nur 29 Prozent der Bürger als Gefahr an. Umgekehrt halten 51 Prozent der Bevölkerung, aber nur 17 Prozent der Entscheider Arbeitslosigkeit für ein großes Risiko in Deutschland. Ähnliches lässt sich bei Einkommensverlust (Bevölkerung: 47 Prozent; Entscheider: 22 Prozent) oder Inflation (Bevölkerung: 42 Prozent, Entscheider: 10 Prozent) beobachten **(Schaubild 6)**.

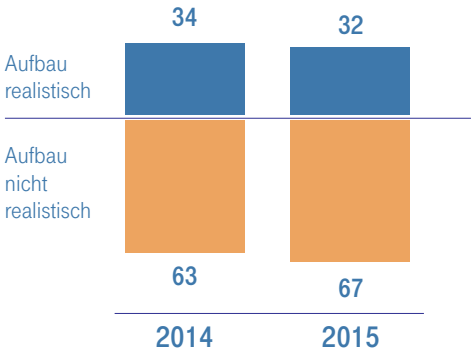
Schaubild 7

AUFBAU EINES INNERDEUTSCHEN BZW. INNEREUROPÄISCHEN INTERNETS: WEITERHIN WÜNSCHENSWERT, UMSETZUNG ALLERDINGS WENIG REALISTISCH

Frage: „Im Zuge des NSA-Abhörskandals gibt es ja Pläne zum Aufbau eines innerdeutschen bzw. innereuropäischen Internets, also dass der Datenverkehr nicht mehr über die USA läuft. Halten Sie es für wünschenswert, ein solches innerdeutsches bzw. innereuropäisches Internet aufzubauen, oder halten Sie das für nicht wünschenswert?“



Frage: „Halten Sie den Aufbau eines solchen innerdeutschen bzw. innereuropäischen Internets für realistisch oder nicht realistisch?“



Auf 100 fehlende Prozent: unentschieden oder keine Angabe
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen 6289, 7231

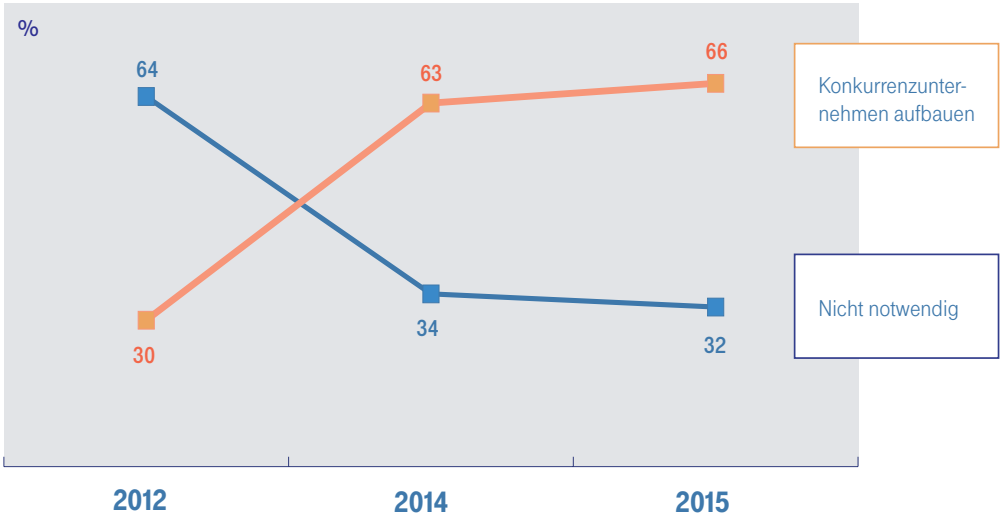
Im Kontext der Berichte über Abhörmaßnahmen des US-amerikanischen Geheimdienstes NSA kam mitunter der Vorschlag auf, über den Aufbau eines innerdeutschen bzw. innereuropäischen Internets das Überwachungsrisiko zu minimieren. Der Aufbau eines solchen nationalen bzw. europäischen Internets gilt den Entscheidern in Politik und Wirtschaft zwar nach wie vor als wünschenswert: 71 Prozent unterstützen den Aufbau eines innerdeutschen bzw. innereuropäischen Internets, vor einem Jahr waren es 65 Prozent. Gleichzeitig hält aber mit 32 Prozent nach wie vor nur eine Minderheit ein solches Vorhaben für realistisch, 2014 waren es 34 Prozent **(Schaubild 7)**.

Auch der Aufbau von europäischen Konkurrenzunternehmen zu Google, Facebook oder Apple wurde in diesem Zusammenhang, aber auch mit Blick auf die Marktführerschaft im digitalen Zeitalter diskutiert. Hier hat sich der Stimmungswandel, der sich infolge des NSA-Abhörskandals vollzogen hat, verfestigt. Im Cyber Security Report 2012 – also ein Jahr vor dem NSA-Abhörskandal – hielt die Mehrheit (64 Prozent) der Entscheider den Aufbau von europäischen Gegenspielern für nicht erforderlich. Nach Bekanntwerden des NSA-Abhörskandals hat sich das Meinungsbild vollständig umgekehrt: 63 Prozent hielten vor einem Jahr den Aufbau von Konkurrenzunternehmen für geboten, aktuell sind es 66 Prozent. Nur 32 Prozent halten den Aufbau von Wettbewerbern für nicht erforderlich **(Schaubild 8)**.

Schaubild 8

GRUNDLEGENDER MEINUNGSWANDEL VERFESTIGT SICH: MEHRHEIT DER ENTSCHEIDER HÄLT DEN AUFBAU EUROPÄISCHER KONKURRENZ-UNTERNEHMEN ZU GOOGLE, FACEBOOK UND APPLE FÜR NOTWENDIG ...

Frage: „Sollten sich die Europäer Ihrer Ansicht nach darum bemühen, verstärkt eigene Konkurrenzunternehmen zu Google, Facebook oder Apple aufzubauen, oder halten Sie das nicht für notwendig?“



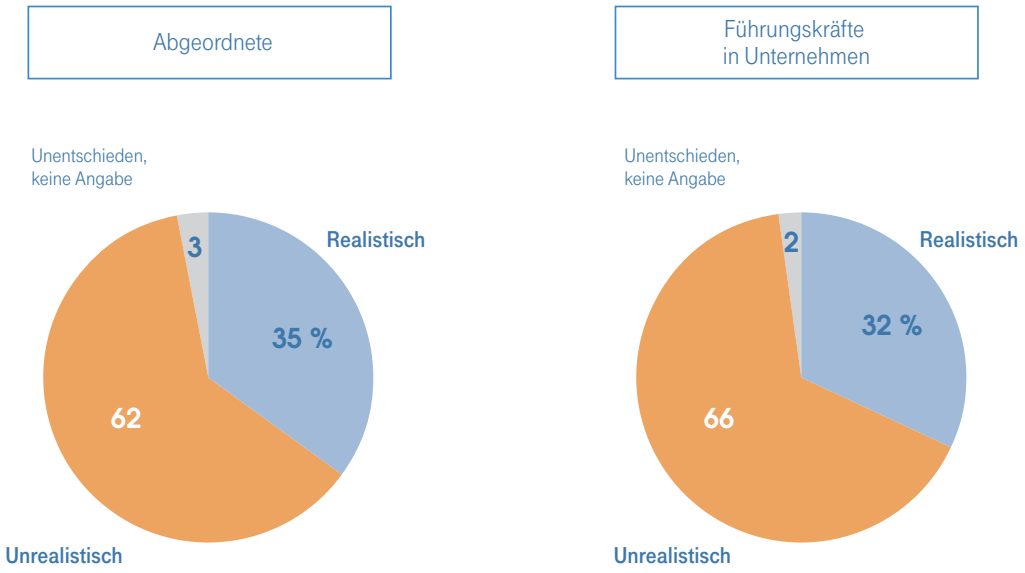
Auf 100 fehlende Prozent: unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7231

Schaubild 9

… ABER FÜR WENIG REALISTISCH

Frage: „Halten Sie es für realistisch, dass in Europa solche Konkurrenzunternehmen aufgebaut werden können, oder halten Sie das für unrealistisch?“



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

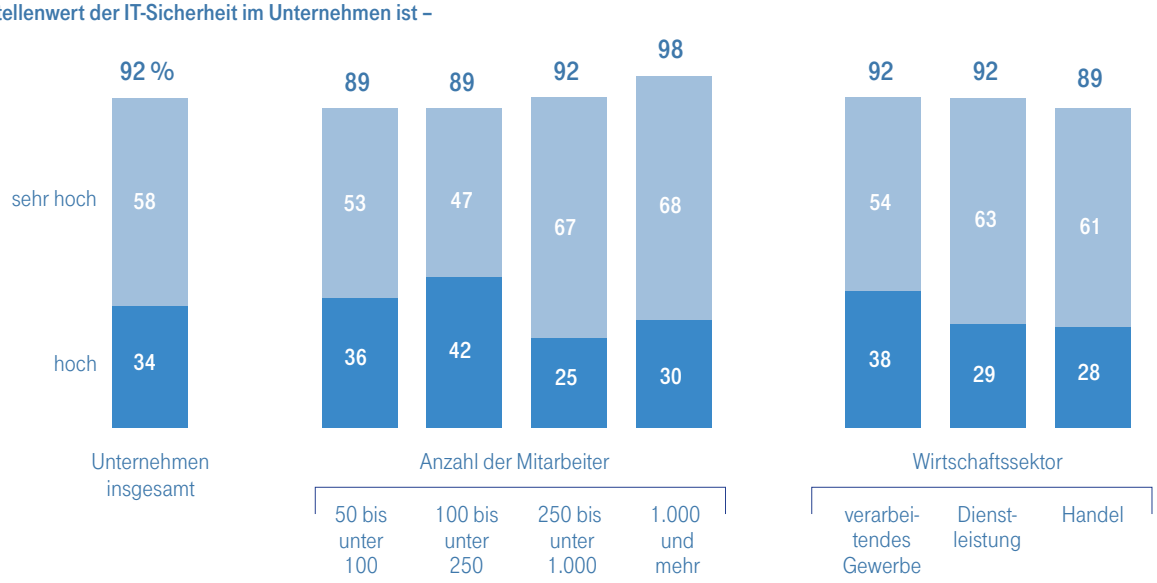
Allerdings zeigt sich das gleiche Bild wie beim Aufbau eines innerdeutschen bzw. innereuropäischen Internets: Die Mehrheit der Entscheider hält ein solches Bestreben zwar für wünschenswert, aber für wenig erfolgversprechend. Nur rund jeder dritte Entscheider räumt dem Vorhaben Aussicht auf Erfolg ein, wobei sich Abgeordnete und Führungskräfte aus der Wirtschaft kaum in ihren Einschätzungen unterscheiden **(Schaubild 9)**.

HOHER STELLENWERT VON IT-SICHERHEIT IN DEUTSCHEN UNTERNEHMEN

Schaubild 10

HOHER STELLENWERT DER IT-SICHERHEIT FÜR DEUTSCHE UNTERNEHMEN

Frage: „Welchen Stellenwert hat IT-Sicherheit in Ihrem Unternehmen, also dass Ihr Unternehmensnetzwerk vor Zugriffen von außen geschützt ist? Hat IT-Sicherheit bei Ihnen einen sehr hohen, hohen, nicht so hohen oder nur einen geringen Stellenwert?“



Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Weitgehend unabhängig von Branche und Unternehmensgröße messen deutsche Unternehmen der IT-Sicherheit heute eine große Bedeutung bei: 92 Prozent der Führungskräfte in mittleren und großen Unternehmen geben zu Protokoll, dass die IT-Sicherheit in ihrem Unternehmen einen hohen oder sogar hohen Stellenwert hat. Große Unternehmen messen der IT-Sicherheit dabei eine noch ausgeprägtere Bedeutung bei als mittlere Unternehmen. So stufen von den Unternehmen mit 50 bis unter 100 Mitarbeitern 53 Prozent den Stellenwert der IT-Sicherheit als sehr hoch ein, von den Unternehmen mit 1.000 und mehr Mitarbeitern sind es 68 Prozent **(Schaubild 10)**.

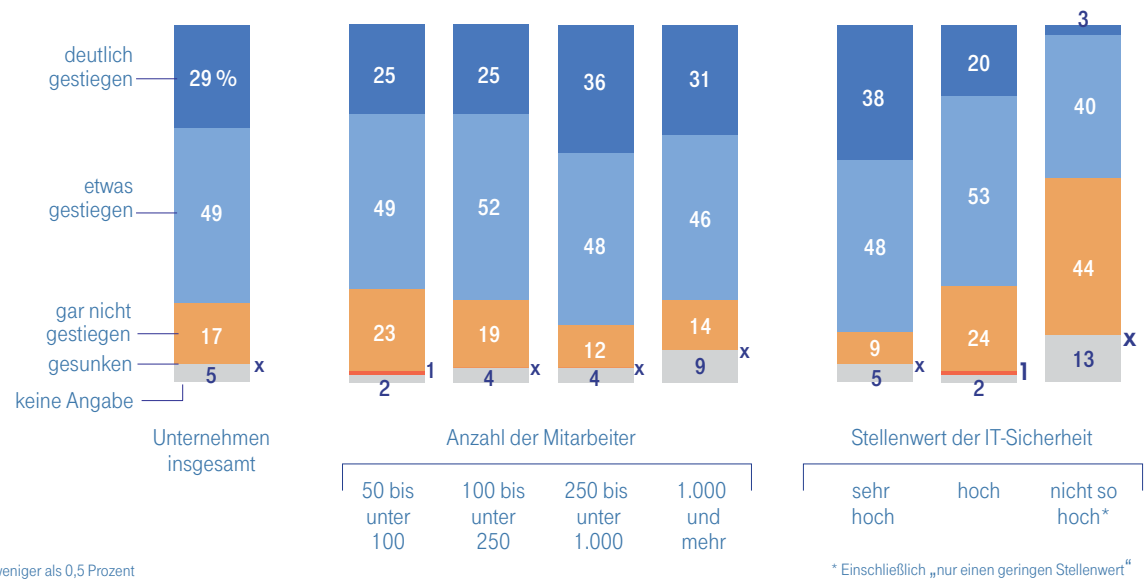
Damit einher gehen häufig auch steigende Kosten. Mit Blick auf die letzten zwei, drei Jahre berichten 29 Prozent der Unternehmen von deutlich gestiegenen Kosten für die IT-Sicherheit, 49 Prozent von etwas gestiegenen Kosten. Lediglich 17 Prozent berichten von konstanten Kosten. Dabei spielt die Unternehmensgröße eine vergleichsweise untergeordnete Rolle. Der Anteil der Unternehmen mit stark gestiegenen Kosten für die IT-Sicherheit liegt – ohne systematischen Zusammenhang mit der Unternehmensgröße – zwischen 25 und 36 Prozent; der Anteil der Unternehmen mit moderaten Kostensteigerungen zwischen 46 und 52 Prozent. Ausschlaggebender für die Kostenentwicklung ist eher der Stellenwert, welcher der IT-Sicherheit im eigenen Unternehmen eingeräumt wird: In Unternehmen, in denen die IT-Sicherheit einen hohen Stellenwert hat, sind die Kosten deutlich häufiger stark gestiegen als in Unternehmen, in denen die IT-Sicherheit lediglich eine hohe oder sogar nur eine nachrangige Bedeutung hat. 38 Prozent der Unternehmen, in denen die IT-Sicherheit einen sehr hohen Stellenwert hat, verzeichneten in den letzten zwei, drei Jahren stark steigende Kosten, von den Unternehmen, in denen die IT-Sicherheit einen hohen Stellenwert hat, waren es 20 Prozent **(Schaubild 11)**.

Schaubild 11

ENTWICKLUNG DER KOSTEN FÜR DIE IT-SICHERHEIT

Frage: „Darf ich fragen, wie sich die Kosten für IT-Sicherheit, für den Schutz vor Hackerangriffen in den letzten 2, 3 Jahren bei Ihnen entwickelt haben?“

Die Kosten für die IT-Sicherheit gegen Hackerangriffe sind –



x = weniger als 0,5 Prozent

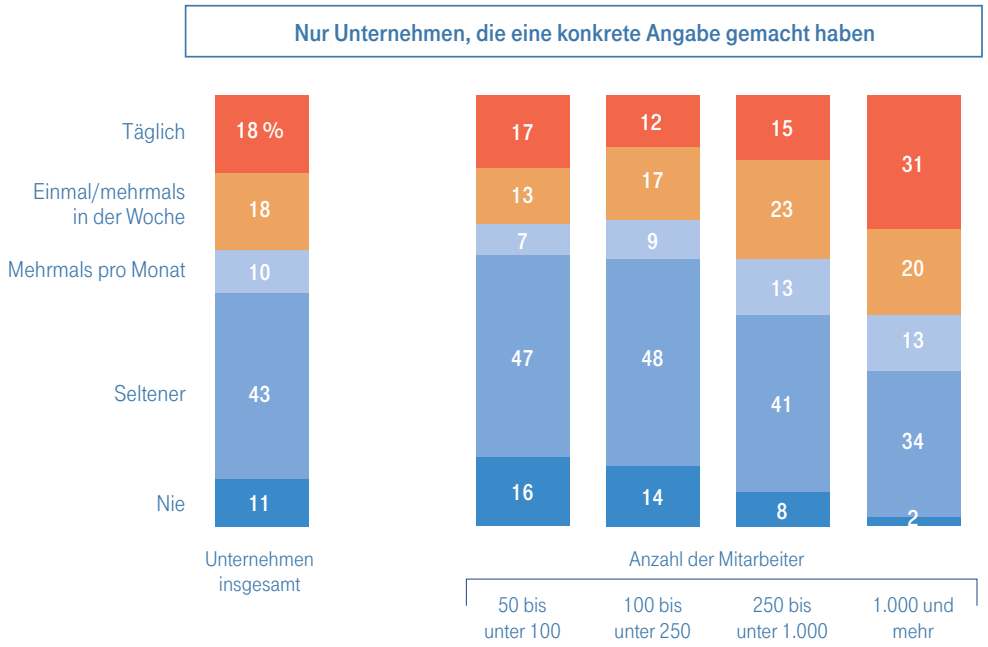
* Einschließlich „nur einen geringen Stellenwert“

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Schaubild 12

DEUTSCHE UNTERNEHMEN ALS ZIEL VON IT-ANGRIFFEN

Frage: „Wie häufig ist Ihr Unternehmen IT-Angriffen ausgesetzt, durch die Ihr Unternehmen ausspioniert oder geschädigt werden soll?“



Basis: Bundesrepublik Deutschland; Führungskräfte in mittleren und großen Unternehmen, die eine konkrete Angabe zur Häufigkeit von IT-Angriffen gemacht haben

Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Der hohe Stellenwert der IT-Sicherheit in deutschen Unternehmen ist nicht ohne Grund: Rund neun von zehn Unternehmen haben bereits IT-Angriffe auf ihr Unternehmen registriert. 18 Prozent haben täglich, weitere 18 Prozent ein- oder mehrmals pro Woche mit externen Angriffen zu kämpfen, 10 Prozent mehrmals im Monat, 43 Prozent seltener als einmal im Monat. Die Häufigkeit der (wahrgenommenen) Angriffe hängt stark von der Größe des Unternehmens ab. So registrieren von den Unternehmen, die zwischen 50 und unter 100 Mitarbeiter haben, 17 Prozent täglich Angriffe, von den Unternehmen mit 1.000 und mehr Mitarbeitern sind es 31 Prozent. Umgekehrt geben 16 Prozent der Unternehmen mit 50 bis unter 100 Mitarbeitern zu Protokoll, bislang noch nicht Ziel von IT-Angriffen gewesen zu sein; von den Unternehmen mit 1.000 und mehr Mitarbeitern ist es nur jedes 50. Unternehmen, das noch nie Ziel von IT-Angriffen war **(Schaubild 12)**.[1]

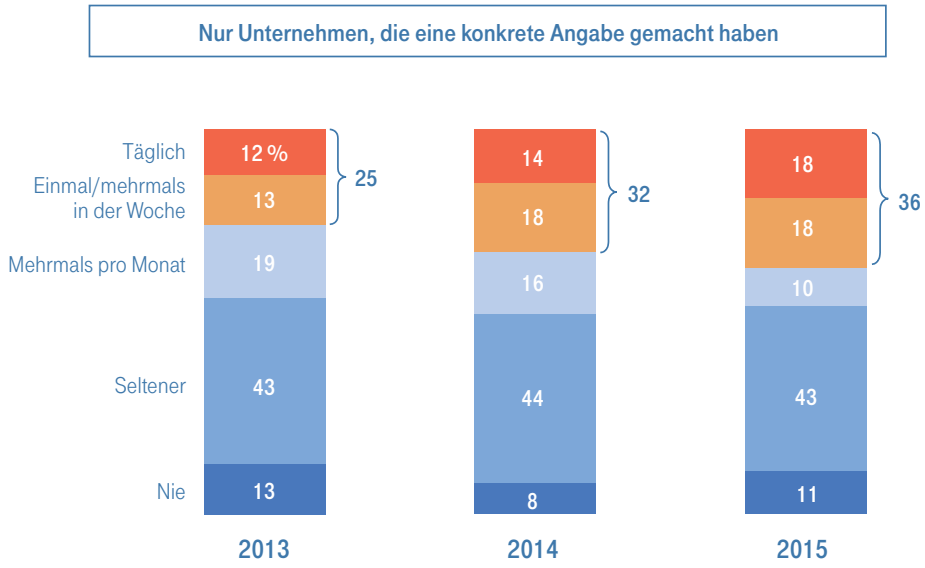
[1] 15 Prozent der Führungskräfte machten zur Häufigkeit der IT-Angriffe auf ihr Unternehmen keine konkrete Angabe, wobei es keine nennenswerten Strukturunterschiede z. B. hinsichtlich der Mitarbeiterzahl oder des Umsatzes zwischen denjenigen Befragten, die konkrete Angaben gemacht haben, und denjenigen ohne konkrete Angaben gibt. Deshalb ist es methodisch vertretbar, für diejenigen, die keine konkrete Angabe gemacht haben, die gleiche Häufigkeitsverteilung zu unterstellen wie für die Unternehmen, die eine konkrete Angabe gemacht haben. Die Originaldaten (ohne Basiswechsel) lauten wie folgt: Tägliche IT-Angriffe: 16 Prozent; mehrmals in der Woche: 7 Prozent; etwa einmal in der Woche: 8 Prozent; 2- bis 3-mal im Monat: 9 Prozent; etwa einmal im Monat: 9 Prozent; seltener: 28 Prozent; nie: 9 Prozent; Unmöglich zu sagen, keine Angabe: 15 Prozent.

Die Häufigkeit von IT-Angriffen auf deutsche Unternehmen ist im Vergleich zu den Vorjahren erneut leicht gestiegen. In der aktuellen Befragung berichten 36 Prozent der Unternehmen, mindestens einmal pro Woche Ziel von IT-Angriffen zu sein, im letzten Jahr waren es 32 Prozent, 2013 erst 25 Prozent. Tägliche Angriffe beobachten aktuell 18 Prozent im Vergleich zu 14 Prozent im Vorjahr und 12 Prozent im Jahr 2013 **(Schaubild 13)**.

Schaubild 13

HÄUFIGKEIT VON IT-ANGRIFFEN ERNEUT LEICHT GESTIEGEN

Frage: „Wie häufig ist Ihr Unternehmen IT-Angriffen ausgesetzt, durch die Ihr Unternehmen ausspioniert oder geschädigt werden soll?“



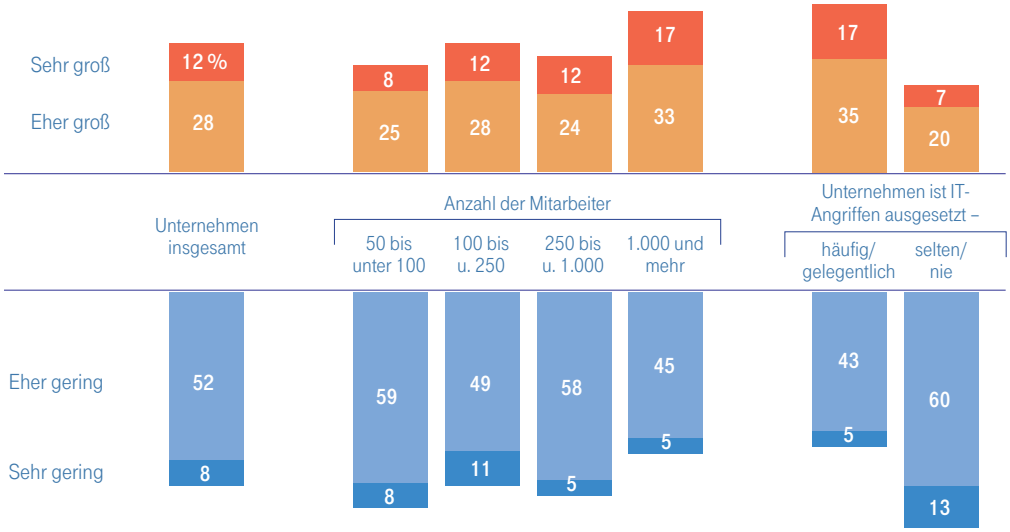
Basis: Bundesrepublik Deutschland; Führungskräfte in mittleren und großen Unternehmen, die eine konkrete Angabe zur Häufigkeit von IT-Angriffen gemacht haben

Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7231

Schaubild 14

NUR EINE MINDERHEIT DER UNTERNEHMEN STUFT DAS SCHADENS-RISIKO DURCH EINEN HACKERANGRIFF ALS (EHER) GROSS EIN

Frage: „Was glauben Sie: Wie groß ist das Risiko für Ihr Unternehmen, durch einen Hackerangriff gravierend geschädigt zu werden? Ist das Risiko sehr groß, eher groß, eher gering oder sehr gering?“



Auf 100 fehlende Prozent: Unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Obwohl die überwältigende Mehrheit der mittleren und großen Unternehmen aller Branchen bereits Ziel von IT-Angriffen war, stuft nur eine Minderheit das Risiko, durch einen Hackerangriff gravierend geschädigt zu werden, als eher oder sogar sehr groß ein. Nur 12 Prozent erkennen darin ein sehr großes, 28 Prozent ein eher großes Risiko. Die große Mehrheit, 60 Prozent, stuft das Schadensrisiko für das eigene Unternehmen als eher oder sehr gering ein. Lediglich in sehr großen Unternehmen mit 1.000 und mehr Mitarbeitern gehen mit 50 Prozent gleich viele Unternehmen von einem großen Schadenspotenzial wie von einem begrenzten Risiko aus. Die Risikoeinschätzung hängt deutlich davon ab, wie häufig das Unternehmen IT-Angriffe registriert.[2] Von den Unternehmen, die über häufige oder gelegentliche IT-Angriffe berichten, stufen 52 Prozent das Risiko gravierender Schäden durch solche Angriffe als groß bzw. sehr groß ein. Von den Unternehmen, die selten oder nie Ziel externer Angriffe sind, gehen mit 27 Prozent deutlich weniger davon aus, durch einen Hackerangriff gravierend geschädigt werden zu können **(Schaubild 14)**.

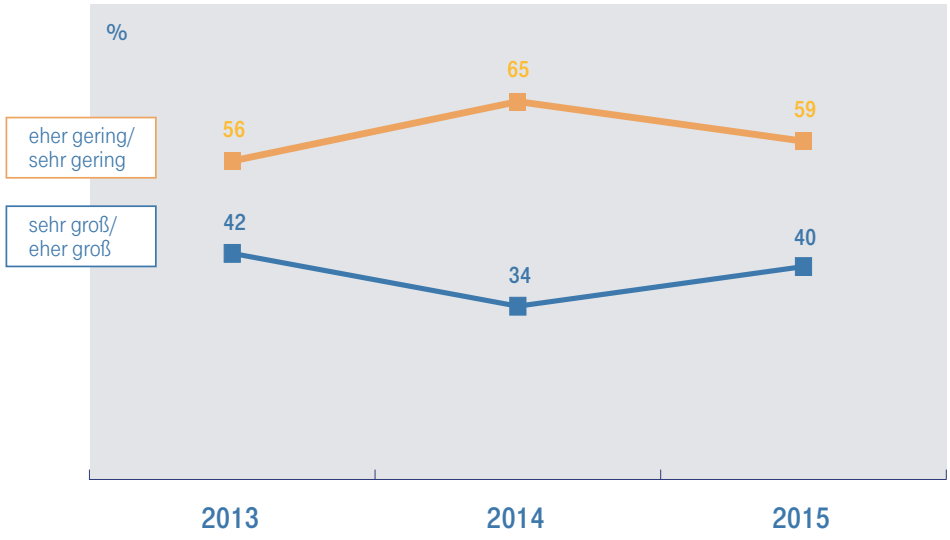
[2] Als „häufig“ oder „gelegentlich“ sind Unternehmen subsumiert, die mindestens einmal im Monat Angriffe registrieren. Unternehmen, die seltener oder nie attackiert werden, sind unter der Bezeichnung „selten/nie“ zusammengefasst.

Trotz der vielen Berichte über Hackerangriffe und Fälle von Industriespionage zeigt die subjektive Einschätzung der Führungskräfte hinsichtlich des eigenen Schadensrisikos keine klaren Entwicklungslinien. Zwar ist der Anteil der Führungskräfte, die für das eigene Unternehmen ein großes Schadensrisiko durch Hackerangriffe sehen, binnen der letzten zwölf Monate von 34 Prozent auf 40 Prozent gestiegen, liegt aber weiterhin knapp unter dem Niveau von 2013, als 42 Prozent der mittleren und großen Unternehmen in IT-Angriffen ein großes Schadenspotenzial für das eigene Unternehmen erkannten. Umgekehrt ist der Anteil derjenigen, die ein geringes Risiko für das eigene Unternehmen konstatieren, zwar von 65 Prozent im Vorjahr auf nun 59 Prozent gesunken, liegt aber weiterhin leicht über dem Niveau von 2013 **(Schaubild 15)**.

Schaubild 15

SUBJEKTIVE EINSCHÄTZUNG DES SCHADENSRISIKOS DURCH HACKERANGRIFFE IM ZEITVERLAUF

Es halten das Risiko, dass ihr Unternehmen durch einen Hackerangriff geschädigt wird, für –

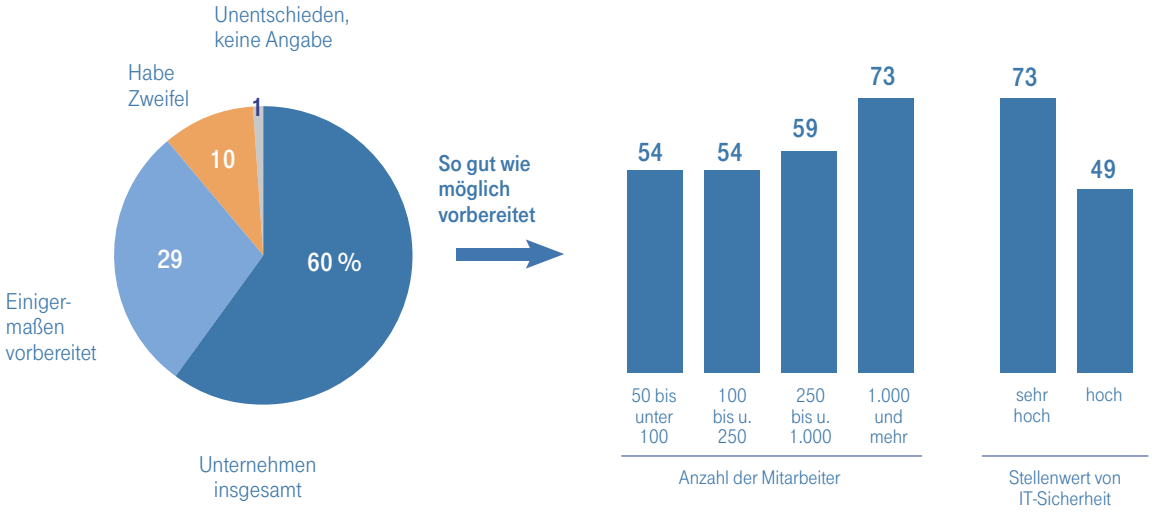


Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7231

Schaubild 16

MEHRHEIT DER FÜHRUNGSKRÄFTE SIEHT IHR UNTERNEHMEN AUF MÖGLICHE GEFAHREN FÜR DIE IT-SICHERHEIT BESTMÖGLICH VORBEREITET

Frage: „Haben Sie das Gefühl, dass Ihr Unternehmen alles in allem so gut wie möglich oder zumindest einigermaßen auf mögliche Gefahren für die IT-Sicherheit wie z. B. Hackerangriffe vorbereitet ist, oder haben Sie da Zweifel?“



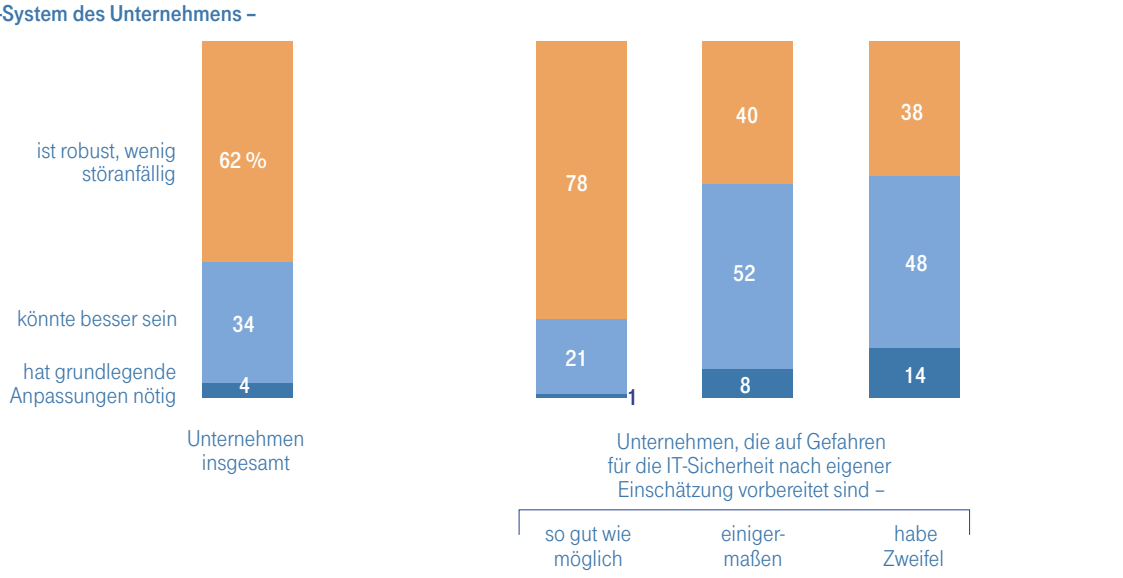
Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Die Einschätzung, dass sich das Schadensrisiko durch Hackerangriffe in Grenzen hält, hängt teilweise auch damit zusammen, dass sich mit 60 Prozent die deutliche Mehrheit der Führungskräfte in mittleren und großen Unternehmen davon überzeugt zeigt, dass ihr Unternehmen gut auf mögliche Gefahren hinsichtlich der IT-Sicherheit vorbereitet ist. Weitere 29 Prozent sehen sich zumindest einigermaßen gerüstet. Lediglich 10 Prozent äußern dezidierte Zweifel, dass ihr Unternehmen ausreichend auf mögliche Gefahren für die IT-Sicherheit vorbereitet ist. Je größer das Unternehmen, desto eher herrscht die Meinung vor, dass man so gut wie möglich aufgestellt ist. Allerdings sind die Unterschiede weniger groß, als man zunächst vermuten könnte, denn auch von den Unternehmen mit 50 bis unter 100 Mitarbeitern ist mehr als die Hälfte überzeugt, bestmöglich gegen potenzielle Gefahren bei der IT-Sicherheit gewappnet zu sein; von den Unternehmen mit 1.000 und mehr Mitarbeitern sind es 73 Prozent. Besonders gut fühlen sich Unternehmen vorbereitet, für welche die IT-Sicherheit im Unternehmen einen sehr hohen Stellenwert hat. Von ihnen sehen sich 73 Prozent sehr gut gegen mögliche Gefahren für die IT-Sicherheit aufgestellt **(Schaubild 16)**.

Schaubild 17

MEHRHEIT DER FÜHRUNGSKRÄFTE BESCHREIBT DAS EIGENE IT-SYSTEM ALS WENIG STÖRANFÄLLIG

Frage: „Wie würden Sie das IT-System Ihres Unternehmens generell beschreiben: Würden Sie Ihr IT-System als robust, also wenig stör- bzw. fehleranfällig bezeichnen oder würden Sie sagen ‚es funktioniert zwar, könnte aber besser sein' oder sind Sie mit dem IT-System Ihres Unternehmens unzufrieden, sind aus Ihrer Sicht grundlegende Anpassungen notwendig?"



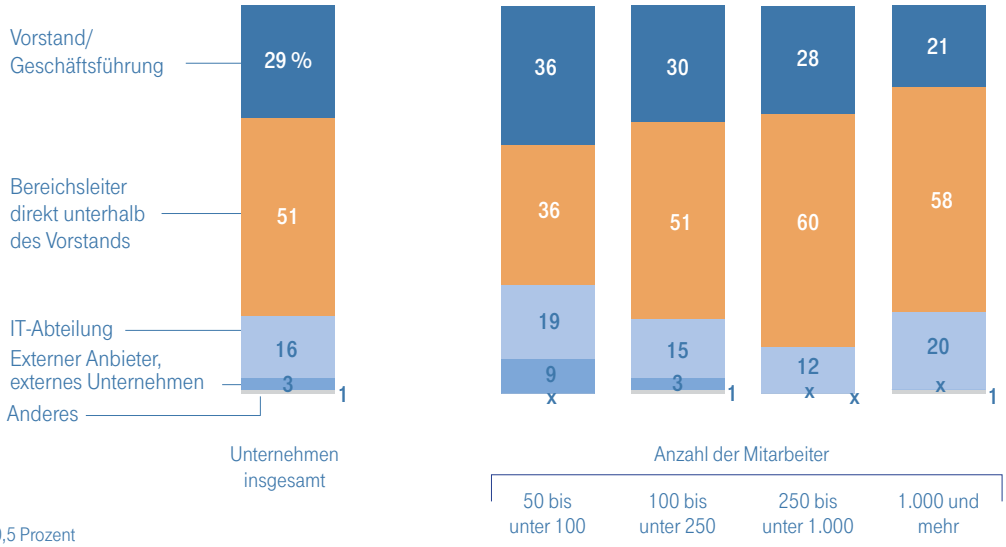
Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Einen engen Zusammenhang gibt es dabei zwischen der generellen Stabilität des eigenen IT-Systems und der Einschätzung, auf IT-Angriffe bestmöglich vorbereitet zu sein. Insgesamt bewerten 62 Prozent der Führungskräfte das IT-System ihres Unternehmens als wenig stör- bzw. fehleranfällig. 34 Prozent berichten zwar von Optimierungsmöglichkeiten, sind aber grundsätzlich mit der Funktionsweise zufrieden. Lediglich 4 Prozent äußern einen grundlegenden Anpassungsbedarf. Diejenigen Unternehmen, die sich so gut wie möglich auf die Gefahren eines IT-Angriffs vorbereitet sehen, beschreiben mit 78 Prozent auch überdurchschnittlich häufig ihr IT-System generell als robust. Von denjenigen, die sich als einigermaßen auf IT-Angriffe vorbereitet sehen, stufen nur 40 Prozent das eigene IT-System als wenig störanfällig ein, 52 Prozent sehen dagegen auch beim allgemeinen IT-System des Unternehmens Verbesserungspotenzial **(Schaubild 17)**.

Schaubild 18

VERANTWORTUNG FÜR DIE VERSORGUNGSSICHERHEIT DER INFORMATIONS- UND KOMMUNIKATIONSINFRASTRUKTUR

Frage: „Wer ist bei Ihnen im Unternehmen für die Versorgungssicherheit der Informations- und Kommunikationsinfrastruktur verantwortlich, also dass IT- und Kommunikationssysteme zuverlässig und uneingeschränkt verfügbar sind? Ist das die Geschäftsführung bzw. der Vorstand, ein Bereichsleiter direkt unterhalb des Vorstands oder die IT-Abteilung ohne direkte Anbindung an die Geschäftsführung bzw. den Vorstand oder wer sonst?“



x = weniger als 0,5 Prozent

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

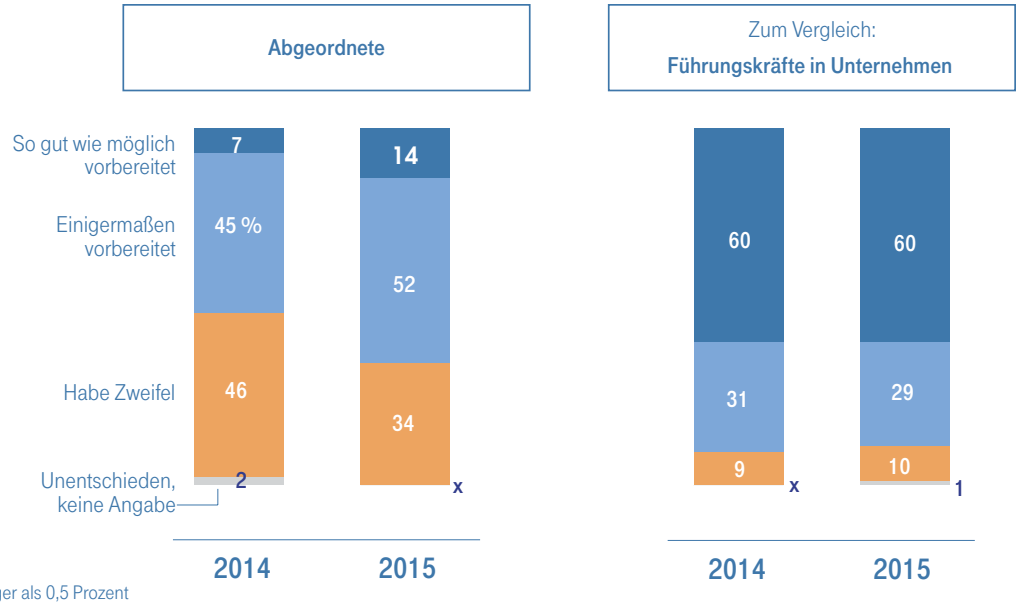
Die Verantwortung für die Versorgungssicherheit der Informations- und Kommunikationsinfrastruktur liegt dabei mit 51 Prozent mehrheitlich bei Bereichsleitern unmittelbar unterhalb der Vorstands- bzw. Geschäftsführungsebene. In 29 Prozent der Unternehmen zeichnen Vorstand und Geschäftsführer selbst verantwortlich dafür, dass die IT- und Kommunikationssysteme zuverlässig und uneingeschränkt verfügbar sind. Eine IT-Abteilung ohne direkte Anbindung an Geschäftsführung bzw. Vorstand ist nur in 16 Prozent der Fälle für die Versorgungssicherheit federführend verantwortlich **(Schaubild 18)**.

Während die Führungskräfte von einer ausreichenden Vorbereitung des eigenen Unternehmens auf IT-Angriffe berichten, äußern sich die Politiker eher skeptisch, sehen die Unternehmen insgesamt aber besser als noch vor einem Jahr auf IT-Angriffe vorbereitet. 14 Prozent der Abgeordneten sind der Meinung, dass die Unternehmen in Deutschland bestmöglich auf Gefahren bezüglich ihrer IT-Systeme vorbereitet sind; 52 Prozent sehen die Unternehmen zumindest einigermaßen vorbereitet. Vor einem Jahr lagen die Werte bei 7 Prozent bzw. 45 Prozent. Die Diskrepanz zwischen der Bewertung der Führungskräfte in Unternehmen einerseits und der Politiker andererseits ist damit deutlich zurückgegangen, bleibt aber weiterhin – vor allem bei der Einschätzung einer bestmöglichen Vorbereitung – beträchtlich **(Schaubild 19)**.

Schaubild 19

POLITIKER SEHEN DEUTSCHE UNTERNEHMEN BESSER AUF IT-RISIKEN VORBEREITET ALS VOR EINEM JAHR

Frage: „Haben Sie das Gefühl, dass die Unternehmen in Deutschland alles in allem so gut wie möglich oder zumindest einigermaßen auf mögliche Gefahren für die IT-Sicherheit wie z.B. Hackerangriffe vorbereitet sind, oder haben Sie da Zweifel?“



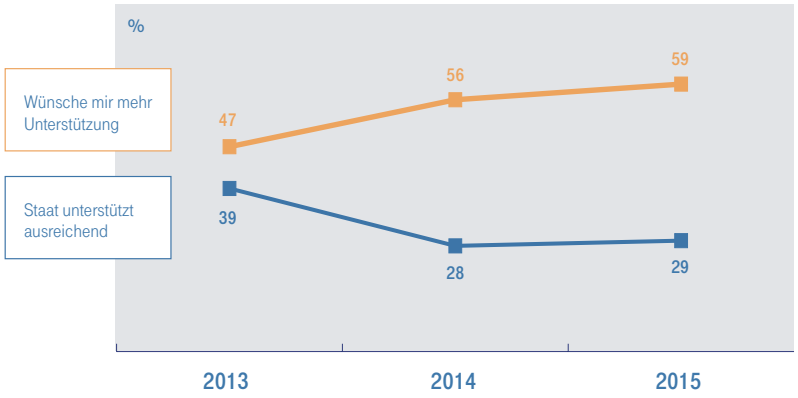
x = weniger als 0,5 Prozent

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen 6289, 7231

Schaubild 20

VERSTÄRKTER WUNSCH NACH MEHR UNTERSTÜTZUNG DURCH DEN STAAT BEI DER BEKÄMPFUNG VON IT-ANGRIFFEN

Frage: „Wie sehen Sie das: Werden deutsche Unternehmen bei der Bekämpfung von IT-Angriffen ausreichend durch den Staat unterstützt, oder fühlen Sie sich bei diesem Thema von der Politik alleingelassen, wünschen Sie sich da mehr Unterstützung durch den Staat?“



Auf 100 fehlende Prozent: Unentschieden, keine Angabe

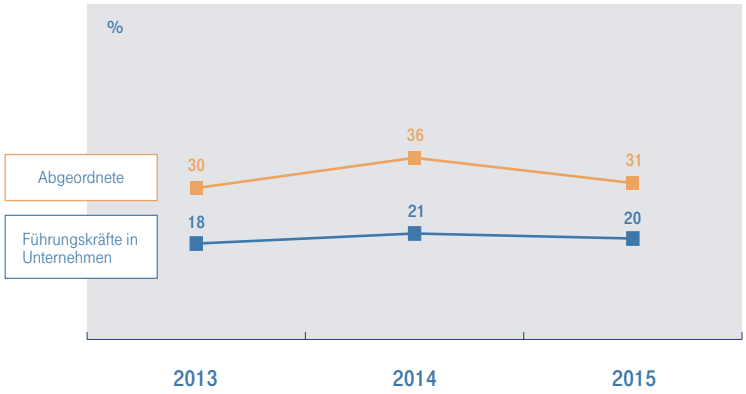
Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7231

Zu der (noch) besseren Vorbereitung auf IT-Angriffe kann der Staat aus Sicht der Unternehmen durchaus beitragen. Der Ruf nach einem stärkeren staatlichen Engagement ist dabei nochmals etwas lauter geworden. Inzwischen wünschen sich 59 Prozent der mittleren und großen Unternehmen mehr Unterstützung durch den Staat, 2013 waren es noch 47 Prozent. Nur 29 Prozent sind der Auffassung, dass der Staat die deutschen Unternehmen bei der Bekämpfung von IT-Angriffen ausreichend unterstützt (Schaubild 20).

Schaubild 22

KEINE STEIGENDE FACHKOMPETENZ IN POLITIK UND VERWALTUNG ERKENNBAR

„Für die Schaffung gesetzlicher Rahmenbedingungen bei der IT-Sicherheit ist in Politik und Verwaltung ausreichend Kompetenz vorhanden.“

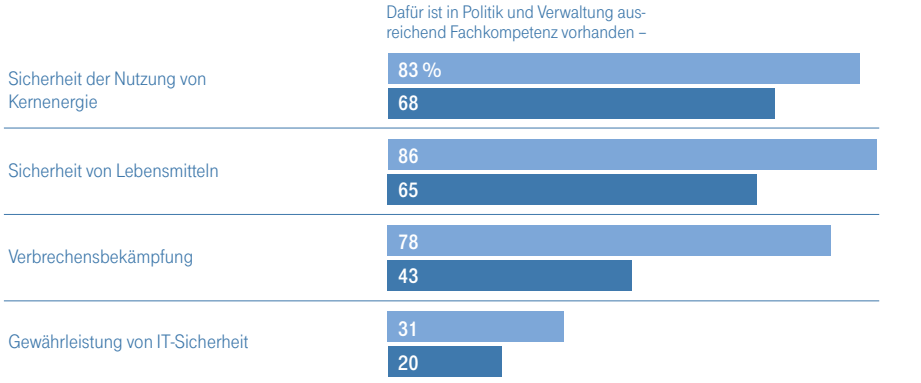


Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7231

Schaubild 21

EINSCHÄTZUNG DER FACHKOMPETENZ IN POLITIK UND VERWALTUNG

Frage: „Wie ist Ihr Eindruck: Ist für die Schaffung gesetzlicher Rahmenbedingungen bei der Verbrechensbekämpfung / bei der IT-Sicherheit / für die Sicherheit von Lebensmitteln/für eine sichere Nutzung der Kernenergie ausreichend Fachkompetenz in Politik und Verwaltung vorhanden oder haben Sie da Zweifel?“



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Dabei steht die Unterstützung durch den Staat vor einem Dilemma. Denn sowohl die Führungskräfte aus der Wirtschaft als auch die Abgeordneten selbst zweifeln daran, dass in Legislative wie Exekutive ausreichend Fachkompetenz beim Thema IT-Sicherheit vorhanden ist. Während in anderen Bereichen wie der Nutzung der Kernenergie oder der Sicherheit von Lebensmitteln eine deutliche Mehrheit von Unternehmensentscheidern wie von Abgeordneten Politik und Verwaltung eine hohe Fachkompetenz zubilligt, hinkt die IT-Sicherheit deutlich hinterher. Von den Führungskräften in den Unternehmen sind gerade einmal 20 Prozent davon überzeugt, dass es auf staatlicher Seite ausreichende Fachkompetenz für die Schaffung gesetzlicher Rahmenbedingungen zur Gewährleistung von IT-Sicherheit gibt. Auch von den Abgeordneten geht nur eine Minderheit (31 Prozent) davon aus, dass es in Politik und Verwaltung genug Know-how für dieses Thema gibt **(Schaubild 21)**.

Über die letzten Jahre ist aus Sicht der Entscheider auch kein Aufbau von weiterer Fachkompetenz erkennbar. Seit 2013 bewegt sich der Anteil derjenigen, die in Politik und Verwaltung ausreichend Fachkompetenz für die Schaffung gesetzlicher Rahmenbedingungen bei der IT-Sicherheit verorten, bei den Abgeordneten zwischen 30 und 36 Prozent, bei den Führungskräften in Unternehmen zwischen 18 und 21 Prozent **(Schaubild 22)**.

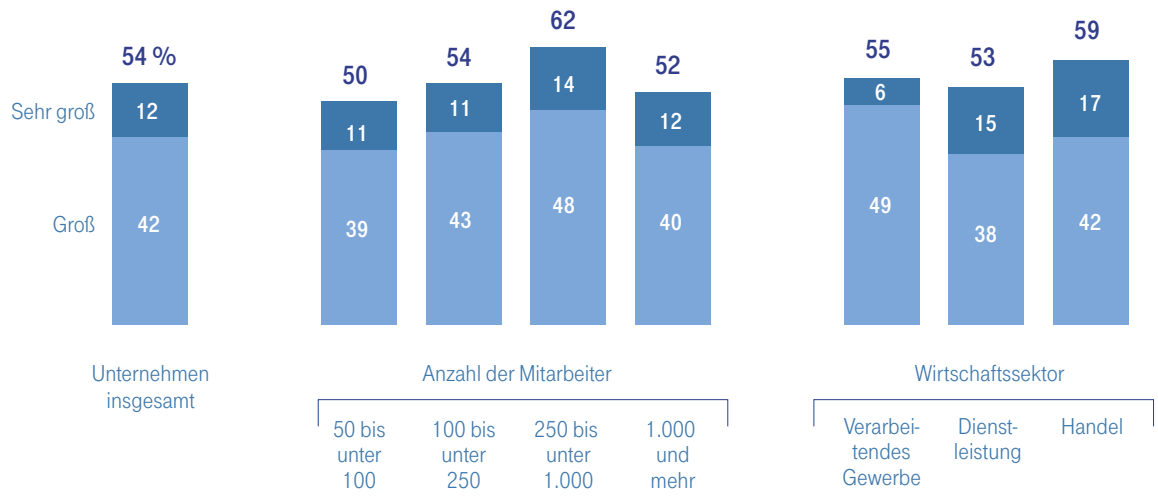
ZUNEHMENDE DIGITALISIERUNG ALS FINANZIELLE HERAUSFORDERUNG

Nicht nur die IT-Sicherheit geht mit erheblichem Aufwand und steigenden Kosten für die Unternehmen einher, auch die Digitalisierung insgesamt stellt für viele Unternehmen eine (finanzielle) Herausforderung dar. 54 Prozent der mittleren und großen Unternehmen in Deutschland sehen die zunehmende Digitalisierung und die damit einhergehenden Investitionskosten als große oder sogar sehr große finanzielle Herausforderung. Unternehmen verschiedener Größe wie auch Branchen sehen sich dabei in ähnlichem Maße herausgefordert. Jeweils zwischen 50 Prozent und 62 Prozent sehen die zunehmende Digitalisierung als große Aufgabe für das eigene Unternehmen **(Schaubild 23)**.

Schaubild 23

FINANZIELLE HERAUSFORDERUNGEN BEI DEN INVESTITIONSKOSTEN DURCH DIE ZUNEHMENDE DIGITALISIERUNG

Frage: „Wie groß sind für Sie die finanziellen Herausforderungen, die durch die zunehmende Digitalisierung und die damit verbundenen Investitionskosten entstehen: Würden Sie sagen, das stellt Sie vor sehr große, große, weniger große oder kaum, gar keine finanzielle Herausforderungen?“



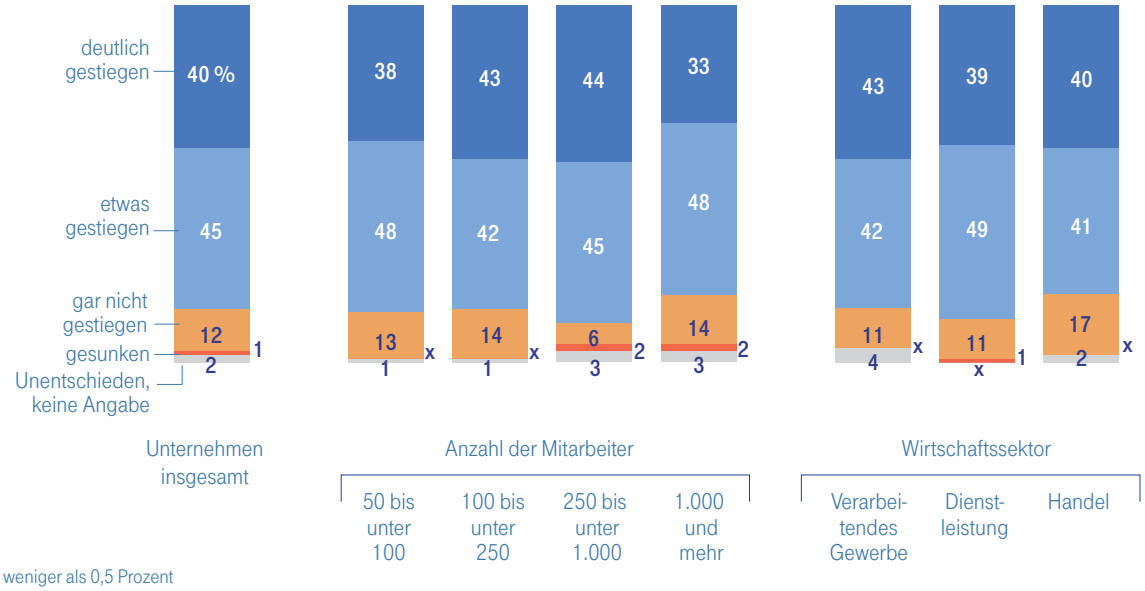
Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Schaubild 24

GENERELLE ENTWICKLUNG DER IT-KOSTEN

Frage: „Darf ich fragen, wie sich die IT-Kosten insgesamt in Ihrem Unternehmen in den letzten 2, 3 Jahren entwickelt haben?“

Die IT-Kosten insgesamt sind in den letzten 2, 3 Jahren –



x = weniger als 0,5 Prozent

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

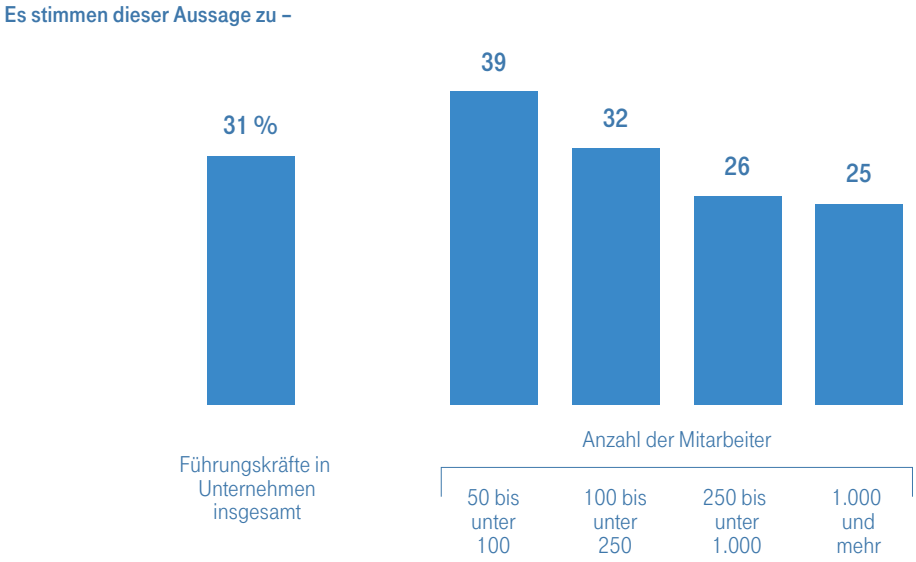
Die zunehmende Digitalisierung spiegelt sich auch in steigenden IT-Kosten wider. 85 Prozent der mittleren und großen Unternehmen berichten von deutlich oder moderat gestiegenen IT-Kosten insgesamt mit Blick auf die letzten zwei, drei Jahre. In 40 Prozent der Unternehmen sind die IT-Kosten deutlich, in 45 Prozent etwas gestiegen. Lediglich 12 Prozent hatten keinen Kostenanstieg im IT-Bereich zu verzeichnen. Die Kostenentwicklung lässt sich dabei weitgehend unabhängig von Unternehmensgröße und Branche beobachten **(Schaubild 24)**.

Die Dynamik der Entwicklungen und Innovationen im IT-Bereich ist aber nicht nur Auslöser für steigende Kosten, sondern kann auch, gerade bei weniger großen Unternehmen, zu Unsicherheiten bei Investitionsentscheidungen führen. So stimmen 31 Prozent der Unternehmen insgesamt der Aussage zu: „Die Entwicklungen und Innovationen im IT-Bereich sind so dynamisch, da weiß ich gar nicht, in was ich investieren soll, was für unser Unternehmen jeweils das Beste ist." Von den Unternehmen mit 50 bis 100 Mitarbeitern sagen dies sogar 39 Prozent. Aber auch von Führungskräften in sehr großen Unternehmen mit mehr als 1.000 Mitarbeitern bekundet jeder Vierte eine entsprechende Unsicherheit **(Schaubild 25)**.

Schaubild 25

UNSICHERHEIT BEI IT-INVESTITIONEN?

Frage: „Wenn jemand sagt ‚Die Entwicklungen und Innovationen im IT-Bereich sind so dynamisch, da weiß ich gar nicht, in was ich investieren soll, was für unser Unternehmen jeweils das Beste ist.' Würden Sie dem zustimmen oder nicht zustimmen?"



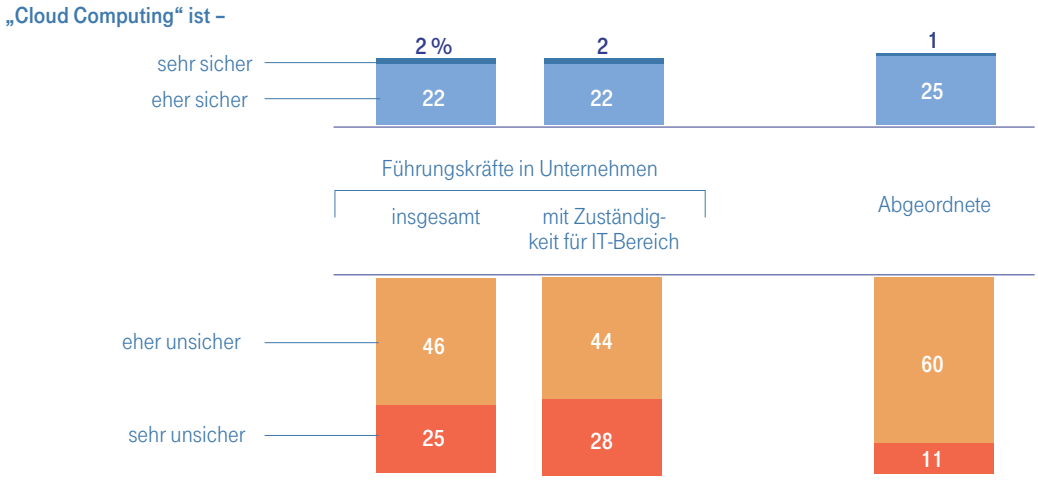
Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Zu den besonders bekannten IT-Trends gehört das „Cloud Computing“, also die Möglichkeit, eigene Daten und Programme extern im Internet statt auf dem eigenen Computer oder Firmenserver zu speichern. Obwohl die Nutzung von Cloud Services durch Unternehmen weiterhin stark zunimmt, stößt diese Form der Datenspeicherung bei den Entscheidern auf erhebliche Sicherheitsbedenken und – damit einhergehend – vermutlich auch auf Unsicherheit bei der Investitionsentscheidung. Von den Führungskräften in den mittleren und großen Unternehmen halten diese Art der Datenverarbeitung nur 2 Prozent für sehr sicher, 22 Prozent für eher sicher. Die überwiegende Mehrheit hält das Cloud Computing dagegen für eher unsicher (46 Prozent) oder sehr unsicher (25 Prozent). Führungskräfte, die in ihrem Unternehmen für den IT-Bereich verantwortlich sind, sehen das Cloud Computing ähnlich kritisch. Bei den Abgeordneten stößt das Cloud Computing ebenfalls auf Skepsis. 26 Prozent der Politiker sehen das Cloud Computing als sicher an, 71 Prozent dagegen als unsicher **(Schaubild 26)**.

Schaubild 26

VERBREITET ZWEIFEL AN DER SICHERHEIT VON „CLOUD COMPUTING“

Frage: „Es gibt ja die Möglichkeit, eigene Daten und Programme im Internet zu speichern, statt auf dem eigenen Computer oder Firmenserver. Für wie sicher halten Sie diese Art der Datenverarbeitung, das sogenannte ‚Cloud Computing‘?“



Auf 100 fehlende Prozent: Kommt darauf an, keine Angabe

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Im Vergleich zu früheren Jahren bewegt sich das Vertrauen in Cloud-Services damit weiterhin auf niedrigem Niveau. Nimmt man Abgeordnete und Führungskräfte aus großen Unternehmen, für die seit 2011 Daten vorliegen, als Basis, so schwankt der Anteil derjenigen, die das Cloud Computing für sicher halten, in den letzten fünf Jahren stabil zwischen 18 Prozent und 27 Prozent, während sich der Anteil derjenigen, die das Cloud Computing als unsicher einstufen, im gleichen Zeitraum zwischen 68 Prozent und 73 Prozent bewegte **(Tabelle 1)**.

Tabelle 1

ABGEORDNETE UND FÜHRUNGSKRÄFTE IN GROSSEN UNTERNEHMEN

	2011 %	2012 %	2013 %	2014 %	2015 %
„Cloud Computing“ ist –					
sehr sicher	2	2	2	1	1
eher sicher	19	21	25	17	22
eher unsicher	47	49	48	51	55
sehr unsicher	26	19	20	22	18

Auf 100 fehlende Prozent: Kommt darauf an, keine Angabe

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in großen Unternehmen

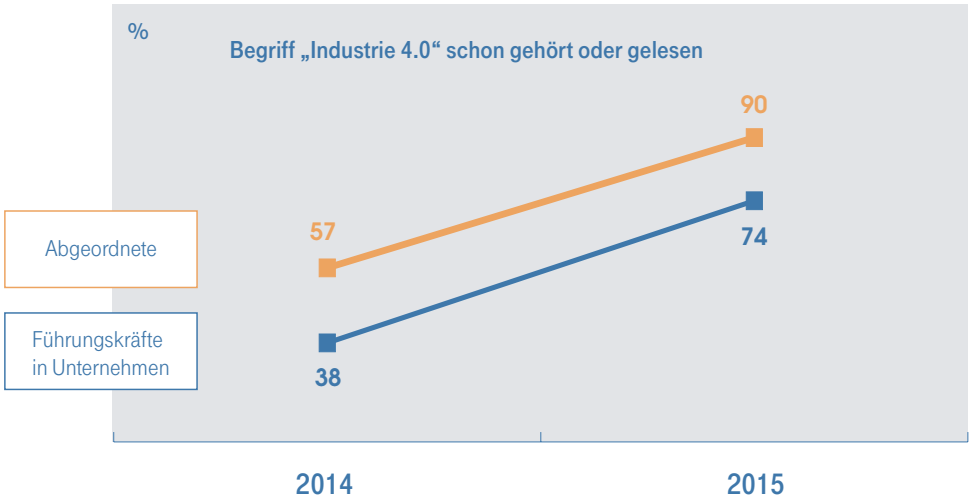
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7231

INDUSTRIE 4.0: GROSSE BEDEUTUNG FÜR DEUTSCHLAND

Schaubild 27

„INDUSTRIE 4.0“ IST INZWISCHEN DER ÜBERWIEGENDEN MEHRHEIT DER ENTSCHEIDER EIN BEGRIFF

Frage: „Haben Sie schon einmal von dem Begriff ‚Industrie 4.0‘ gehört oder gelesen, oder ist das nicht der Fall?“



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen 6269, 7231

„Industrie 4.0“ ist von Bundesregierung und Branchenverbänden als Begriff für die Verzahnung von Produktion mit modernster Informations- und Kommunikationstechnik geprägt worden. Wie sehr das Thema in den letzten zwölf Monaten an Bedeutung und Präsenz gewonnen hat, lässt sich an der Bekanntheit des Begriffs ablesen. Während beim letzten Cyber Security Report 2014 erst 38 Prozent der Führungskräfte in der Wirtschaft und 57 Prozent der Abgeordneten den Begriff Industrie 4.0 gehört oder gelesen hatten, ist der Begriff der überwiegenden Mehrheit der Entscheider inzwischen geläufig. 74 Prozent der Führungskräfte in Unternehmen und 90 Prozent der Abgeordneten ist der Begriff mittlerweile bekannt **(Schaubild 27)**.

Schaubild 28

BEKANNTHEIT MIT „INDUSTRIE 4.0“ VERWANDTER BEGRIFFE

Frage: „Welchen dieser Begriffe haben Sie bereits gehört oder gelesen? War das der Begriff vernetzte oder intelligente Fabrik, Smart Factory, Internet der Dinge oder war das ein anderer Begriff?“

	Entscheider insgesamt	Führungskräfte in Unternehmen %	Abgeordnete %
Ja, schon einmal gehört oder gelesen	**84 %**	**82**	**89**
und zwar –			
vernetzte bzw. intelligente Fabrik	66	64	72
Smart Factory	61	59	70
Internet der Dinge	48	46	59
Anderes	x	1	x
Nein, noch nicht gehört	**16**	**18**	**11**

x = weniger als 0,5 Prozent

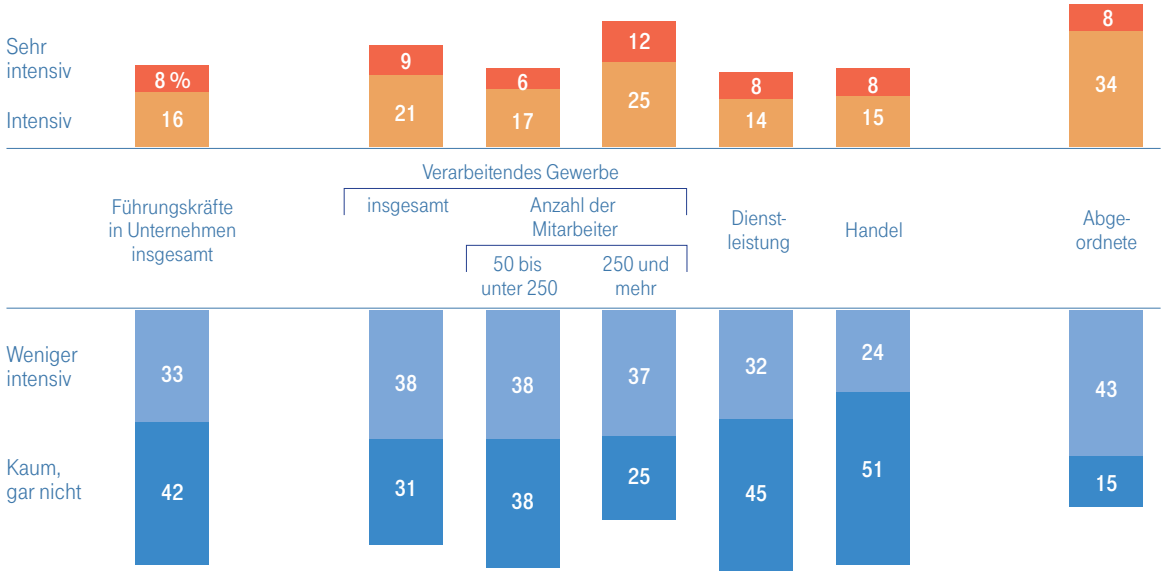
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Auch andere, mit Industrie 4.0 verwandte Begriffe sind vielen Entscheidern bekannt. 66 Prozent haben bereits von vernetzten bzw. intelligenten Fabriken gehört, 61 Prozent von der Smart Factory, 48 Prozent vom Internet der Dinge. 84 Prozent ist mindestens einer dieser Begriffe bekannt. Den Abgeordneten sind die Begriffe durchweg geläufiger als den Führungskräften in Unternehmen. So haben beispielsweise 72 Prozent der Abgeordneten schon den Begriff Smart Factory gehört, von den Führungskräften in Unternehmen sind es 64 Prozent **(Schaubild 28)**.

Schaubild 29

NUR EINE MINDERHEIT HAT SICH BISLANG INTENSIVER MIT DEM THEMA „INDUSTRIE 4.0“ BESCHÄFTIGT

Frage: „Wie intensiv haben Sie sich bisher mit dem Thema ‚Industrie 4.0‘ beschäftigt?“



Auf 100 fehlende Prozent: Unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Nur eine Minderheit hat sich mit den Konzepten allerdings schon intensiver auseinandergesetzt. 24 Prozent der Führungskräfte in Unternehmen haben sich näher mit dem Thema befasst. Im verarbeitenden Gewerbe, das von Industrie 4.0 in besonderem Maße betroffen ist, hat sich mit 30 Prozent rund jede dritte Führungskraft schon eingehender damit beschäftigt, wobei es deutliche Unterschiede in Abhängigkeit von der Unternehmensgröße gibt. In den großen Unternehmen des verarbeitenden Gewerbes haben sich schon 37 Prozent, in den mittleren Unternehmen erst 23 Prozent mit dem Thema befasst **(Schaubild 29)**.

Diejenigen, denen der Begriff Industrie 4.0 bekannt ist, wurden in einer offenen Nachfrage – also ohne die Vorgabe von Antwortalternativen – gebeten, ihr Verständnis von Industrie 4.0 zu erläutern. Die Antworten wurden anschließend ausgewertet und zu aussagekräftigen Kategorien zusammengefasst. 35 Prozent derjenigen, denen der Begriff Industrie 4.0 bekannt war, haben diesen mit der Digitalisierung und dem Einsatz neuer digitaler Techniken in Verbindung gebracht. 34 Prozent haben einen Bezug zur Vernetzung in der Produktion hergestellt. 13 Prozent haben Veränderungen in den Produktionsabläufen wie Individualisierung oder Flexibilisierung genannt **(Schaubild 30)**.

Schaubild 30

WAS ENTSCHEIDER UNTER „INDUSTRIE 4.0“ VERSTEHEN

Frage: „Können Sie mir ungefähr sagen, was der Begriff ‚Industrie 4.0‘ Ihrem Verständnis nach bezeichnet?“ (offene Frage, ohne Antwortvorgabe)

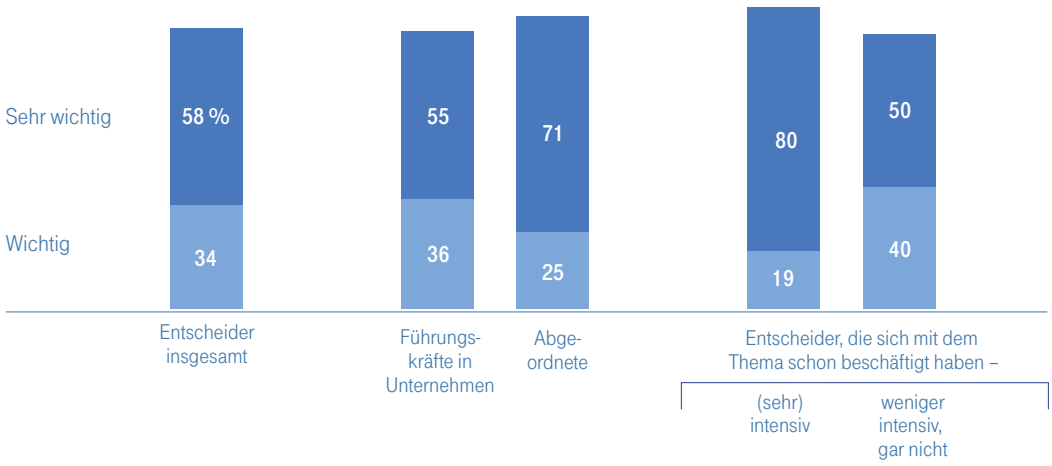
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen, die bereits von „Industrie 4.0“ gehört oder gelesen haben

Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Schaubild 31

GROSSE BEDEUTUNG VON „INDUSTRIE 4.0“ FÜR DEN WIRTSCHAFTSSTANDORT DEUTSCHLAND

Frage: „Einmal ganz allgemein gefragt: Wie wichtig ist das Projekt ‚Industrie 4.0‘ für den Wirtschaftsstandort Deutschland? Ist es Ihrer Meinung nach sehr wichtig, wichtig, weniger wichtig oder kaum, gar nicht wichtig?“*



*Zusätzliche Erläuterung für Befragte, die sich bisher weniger intensiv oder kaum, gar nicht mit dem Thema „Industrie 4.0“ beschäftigt haben: „Mit ‚Industrie 4.0‘ bzw. den anderen Begriffen wird die Neuorganisation der Wertschöpfungskette von Unternehmen durch Digitalisierung und Vernetzung der Produktionssysteme beschrieben. Wesentliche Bestandteile sind beispielsweise teilautonome Maschinen, die sich ohne menschliche Steuerung bewegen und selbstständig Entscheidungen treffen, sowie die Möglichkeit einer starken Individualisierung von Produkten auch im Rahmen von Großserien. Durch die Vernetzung kann die Produktion zudem nahezu in Echtzeit gesteuert und optimiert werden."

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

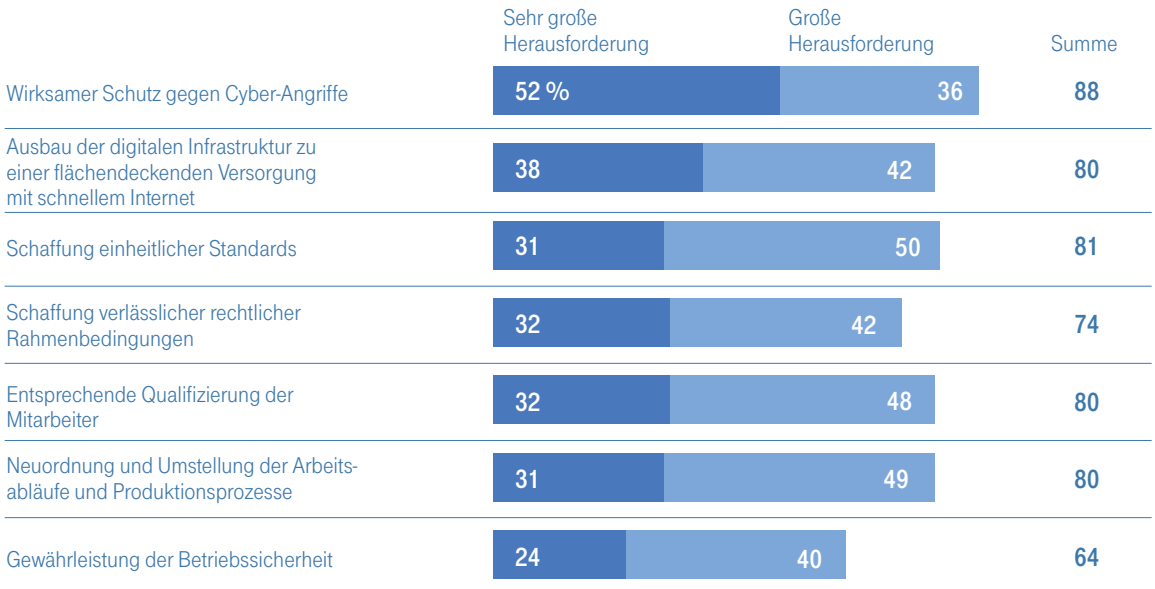
Weitgehende Einigkeit besteht unter den Entscheidern über die große Bedeutung von Industrie 4.0 für den Wirtschaftsstandort Deutschland. 58 Prozent halten das Projekt für sehr wichtig, weitere 34 Prozent für wichtig. Abgeordnete sehen dabei im Vergleich zu Unternehmensführungskräften Industrie 4.0 häufiger als besonders wegweisend für den Wirtschaftsstandort Deutschland an. 71 Prozent halten das Projekt für sehr wichtig, von den Führungskräften in Unternehmen sind es 55 Prozent. Zudem sind Entscheider, die sich schon intensiver mit dem Thema befasst und damit über einen tieferen Einblick in die Chancen von Industrie 4.0 haben, von der Tragweite des Projekts besonders überzeugt: 80 Prozent von ihnen halten Industrie 4.0 für sehr wichtig, wenn es um die Zukunft des Wirtschaftsstandorts Deutschland geht **(Schaubild 31)**.

Die Umsetzung eines derart umfassenden Konzepts wie Industrie 4.0 steht naturgemäß vor einer Vielzahl von Herausforderungen. Als größte Herausforderung wird von den Führungskräften aus dem verarbeitenden Gewerbe, die die einzelnen Aspekte angesichts ihres Branchenhintergrunds besonders gut einschätzen können, der wirksame Schutz gegen Cyberangriffe eingestuft. 52 Prozent sehen darin eine sehr große, weitere 36 Prozent eine große Herausforderung. Aber auch der Ausbau der digitalen Infrastruktur zu einer flächendeckenden Versorgung mit schnellem Internet, die Schaffung einheitlicher Standards, die Schaffung verlässlicher rechtlicher Rahmenbedingungen, die Qualifizierung von Mitarbeitern sowie die Neuordnung und Umstellung der Arbeitsabläufe und Produktionsprozesse gelten jeweils rund einem Drittel der Führungskräfte aus dem verarbeitenden Gewerbe als sehr große Herausforderung, zwischen 42 Prozent und 50 Prozent sehen darin jeweils eine große Herausforderung **(Schaubild 32)**.

Schaubild 32

HERAUSFORDERUNGEN BEI DER UMSETZUNG VON „INDUSTRIE 4.0“

Frage: „Nach dem, was Sie wissen oder vermuten: Was sind die größten Hürden bzw. Herausforderungen bei der Umsetzung von ‚Industrie 4.0‘? Wie ist es mit ...: Ist das Ihrer Meinung nach eine sehr große, große, weniger große oder kaum eine bzw. keine Herausforderung für Unternehmen?“

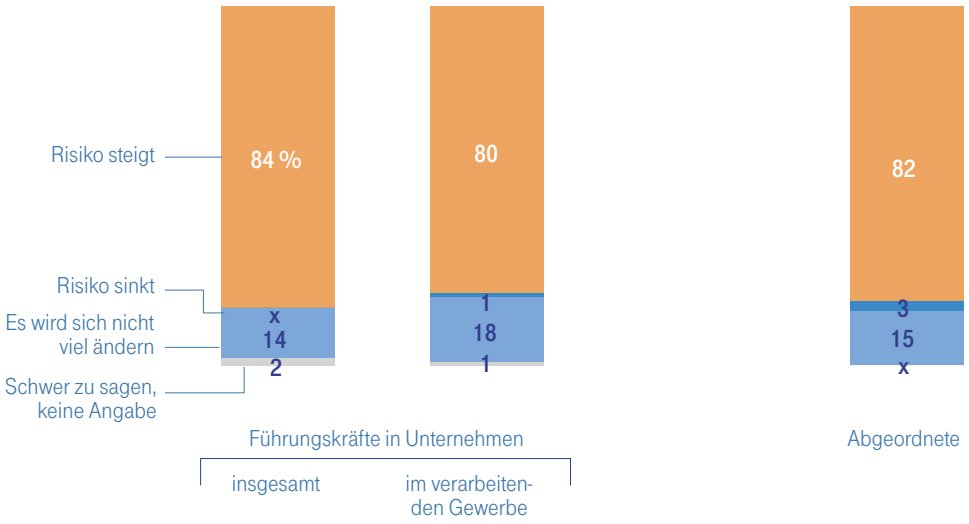


Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen des verarbeitenden Gewerbes
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Schaubild 33

STEIGENDES RISIKO VON CYBERANGRIFFEN AUF UNTERNEHMEN DURCH „INDUSTRIE 4.0“

Frage: „Glauben Sie, mit der Umsetzung des Projekts ‚Industrie 4.0‘, also der Automatisierung und Vernetzung des Produktionsprozesses, steigt das Risiko von Cyberangriffen auf Unternehmen oder wird das Risiko sinken oder glauben Sie, da wird sich nicht viel ändern?“



x = weniger als 0,5 Prozent

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

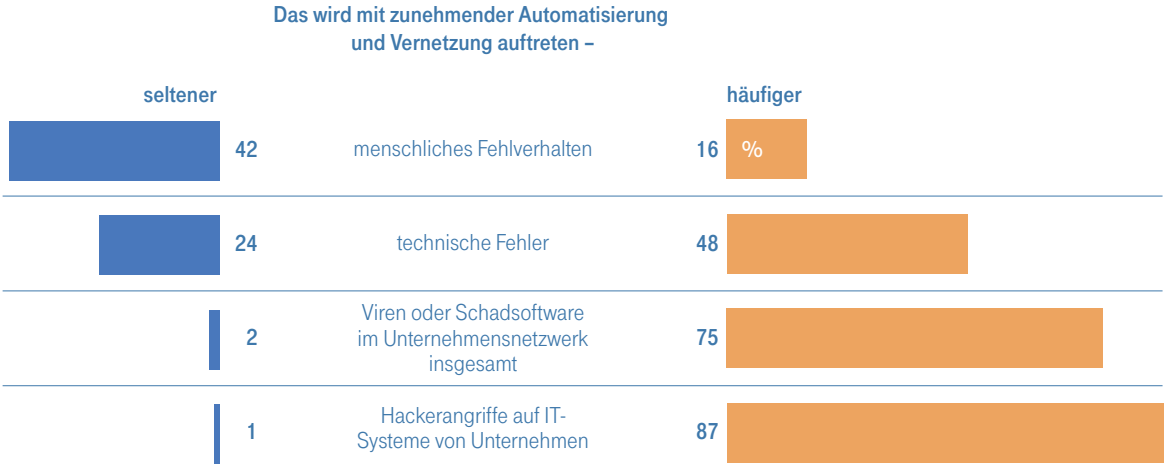
Die Relevanz von Cyber Security im Kontext von Industrie 4.0 zeigt sich auch darin, dass 84 Prozent der Führungskräfte in Unternehmen aufgrund der Automatisierung und Vernetzung der Produktionsprozesse von einem steigenden Risiko von Cyberangriffen auf Unternehmen ausgehen. 14 Prozent erwarten ein gleichbleibendes Risiko. Diese Einschätzung wird in gleicher Größenordnung auch von Führungskräften aus dem verarbeitenden Gewerbe wie von Abgeordneten geteilt **(Schaubild 33)**.

Auch ein Vergleich mit anderen Gefahrenquellen unterstreicht die Bedeutung von Cyberrisiken, die mit der Umsetzung von Maßnahmen im Zusammenhang mit Industrie 4.0 einhergehen. 87 Prozent der Führungskräfte in Unternehmen erwarten durch die verstärkte Verzahnung von Produktion und digitalen Informations- und Kommunikationstechnologien vermehrte Hackerangriffe, 75 Prozent gehen von einer Zunahme von Viren oder Schadsoftware im Unternehmensnetzwerk aus. Seltener wird aus Sicht der Führungskräfte hingegen menschliches Fehlverhalten werden. 42 Prozent der Führungskräfte rechnen mit einem Rückgang menschlichen Fehlverhaltens **(Schaubild 34)**. Für Führungskräfte aus dem verarbeitenden Gewerbe zeigt sich ein ähnliches Meinungsbild.

Schaubild 34

ERWARTETE FOLGEN VON „INDUSTRIE 4.0“

Frage: „Die Automatisierung und Vernetzung von Produktionssystemen in Unternehmen kann ja neben Vorteilen auch verschiedene Gefahren bzw. Risiken mit sich bringen, die den Produktionsprozess gefährden können. Ich lese Ihnen jetzt einige Risiken vor und Sie sagen mir bitte, ob diese mit einer zunehmenden Automatisierung und Vernetzung Ihrer Meinung nach häufiger auftreten werden oder ob sie seltener auftreten werden oder ob sich an der Häufigkeit vermutlich nichts ändert.“



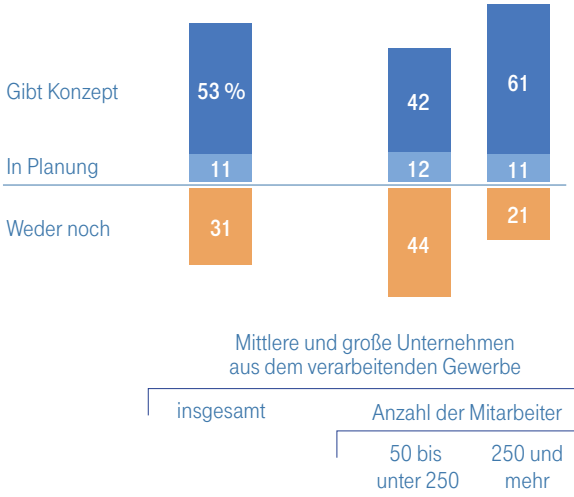
Auf 100 fehlende Prozent: „Nicht viel ändern“ bzw. „Schwer zu sagen“, keine Angabe

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

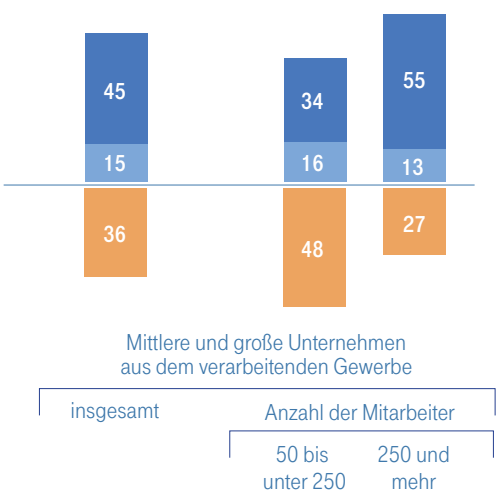
Schaubild 35

SPEZIELLES IT-SICHERHEITSKONZEPT FÜR PRODUKTIONS-BEREICH UND -STEUERUNG

Frage: „Gibt es in Ihrem Unternehmen ein IT-Sicherheitskonzept speziell für den Produktionsbereich bzw. für die Produktionsmaschinen oder ist so ein IT-Sicherheitskonzept in Planung oder weder noch?“



Frage: „Gibt es ein spezielles Sicherheitskonzept für den Datenaustausch zwischen Produktionssteuerung und Produktion oder planen Sie ein Sicherheitskonzept oder weder noch?"



Auf 100 fehlende Prozent: Weiß nicht, keine Angabe

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen des verarbeitenden Gewerbes
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

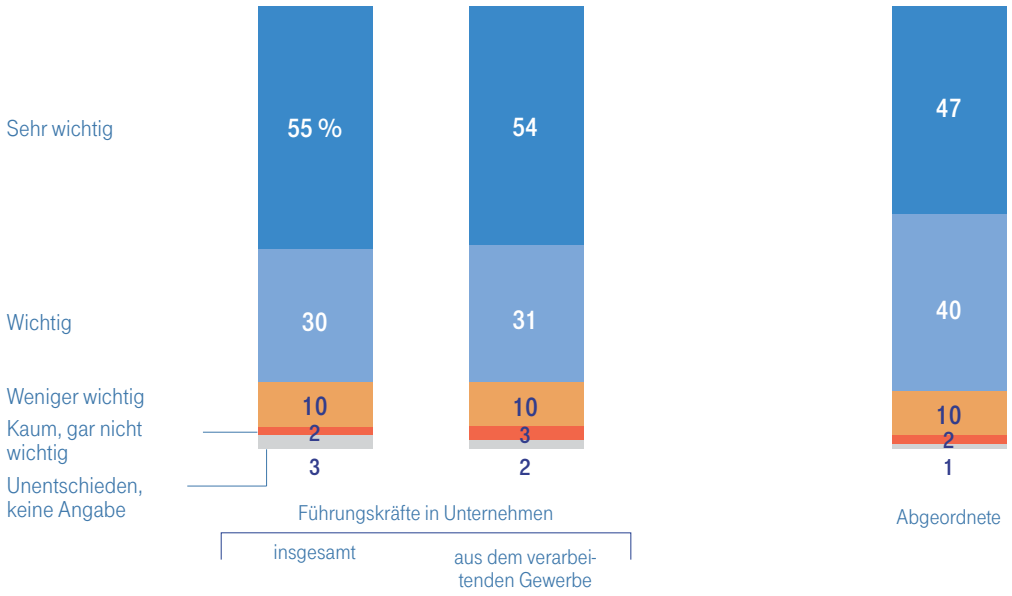
Angesichts der erwarteten Zunahme von Cyberrisiken sind entsprechende Vorkehrungen der Unternehmen eine wichtige Voraussetzung für eine erfolgreiche Umsetzung von Industrie 4.0. Wichtige Bestandteile solcher Sicherheitsmaßnahmen können IT-Sicherheitskonzepte zum einen speziell für den Produktionsbereich, zum anderen für den Datenaustausch zwischen Produktionssteuerung und Produktion sein. 53 Prozent der mittleren und großen Unternehmen aus dem verarbeitenden Gewerbe verfügen bereits über ein IT-Sicherheitskonzept für den Produktionsbereich, bei weiteren 11 Prozent befindet sich ein solches in Planung. Für den Datenaustausch zwischen Produktionssteuerung und Produktion haben 45 Prozent der Unternehmen aus dem verarbeitenden Gewerbe ein Sicherheitskonzept entwickelt, bei 15 Prozent ist ein solches in Planung. Große Unternehmen besitzen dabei häufiger als mittlere Unternehmen ein Sicherheitskonzept für den jeweiligen Bereich. So haben beispielsweise 61 Prozent der großen Unternehmen aus dem verarbeitenden Gewerbe ein IT-Sicherheitskonzept speziell für den Produktionsbereich, von den mittleren Unternehmen sind es 42 Prozent **(Schaubild 35)**.

In der Diskussion über die Umsetzung von Industrie 4.0 werden immer wieder einheitliche Standards als erfolgskritische Voraussetzung eingefordert. Die Entscheider teilen diese Forderung. 85 Prozent der Führungskräfte sowohl in Unternehmen insgesamt als auch im verarbeitenden Gewerbe und 87 Prozent der Abgeordneten halten unternehmensübergreifende Standards für den Erfolg von Industrie 4.0 für wichtig oder sogar sehr wichtig **(Schaubild 36)**.

Schaubild 36

BREITER KONSENS: UNTERNEHMENSÜBERGREIFENDE STANDARDS SIND WICHTIG FÜR DEN ERFOLG VON „INDUSTRIE 4.0“

Frage: „Was meinen Sie: Wie wichtig ist es für die erfolgreiche Umsetzung des Projekts ‚Industrie 4.0‘, dass es einheitliche, unternehmensübergreifende Standards, z.B. bei Softwareprogrammen, gibt?“

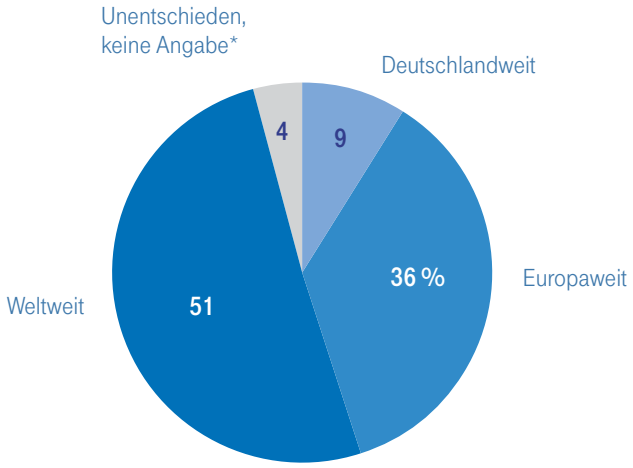


Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Schaubild 37

INTERNATIONALE STANDARDISIERUNG ERFORDERLICH

Frage: „Auf welcher Ebene sollten Ihrer Meinung nach einheitliche, unternehmensübergreifende Standards festgelegt werden: Sollten die Standards deutschlandweit vereinheitlicht werden oder europaweit oder sollten weltweit einheitliche Standards gelten?“



*Einschließlich der Entscheider, die eine Standardisierung grundsätzlich für nicht wichtig halten.

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

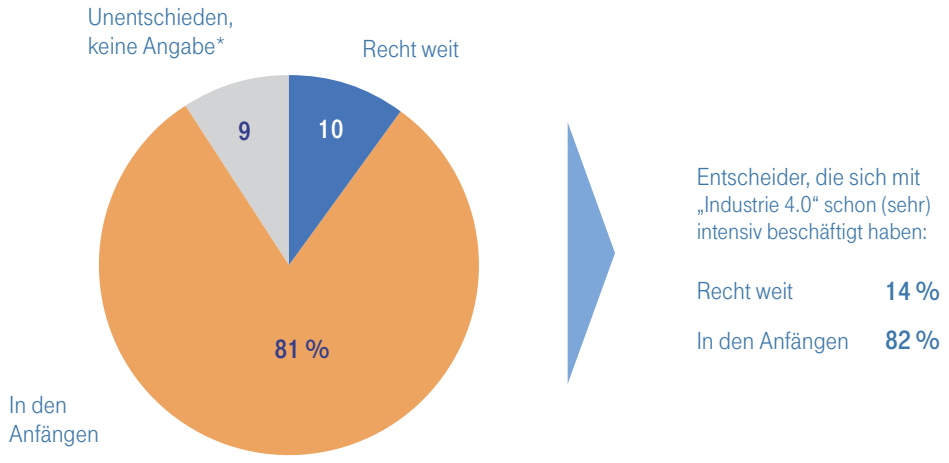
Dabei spricht sich die überwältigende Mehrheit für weltweite, zumindest aber europaweite Standards aus. 51 Prozent sind der Meinung, dass die Standards weltweit definiert werden sollten, 36 Prozent sprechen sich für eine europaweite Normierung aus. Eine nationale Lösung halten hingegen nur 9 Prozent für den richtigen Weg **(Schaubild 37)**.

So wichtig die Festlegung von Standards für den Fortschritt und den Erfolg von Industrie 4.0 ist, sosehr befindet sich dieser Prozess aus Sicht der Entscheider noch in den Anfängen. Nur 10 Prozent haben den Eindruck, dass man mit der Definition von Standards bereits recht weit ist. 81 Prozent sind dagegen der Ansicht, dass die Festlegung von unternehmensübergreifenden Normen noch in den Anfängen steckt. Entscheider, die sich schon intensiver mit dem Thema Industrie 4.0 befasst haben, teilen diese kritische Einschätzung. Von ihnen sind ebenfalls lediglich 14 Prozent der Auffassung, dass man bei der Entwicklung einheitlicher Standards schon recht weit ist, 82 Prozent haben dagegen den Eindruck, dass diese noch am Anfang stehen **(Schaubild 38)**.

Schaubild 38

STANDARDISIERUNG BEFINDET SICH NOCH IN DEN ANFÄNGEN

Frage: „Wie ist Ihr Eindruck: Wie weit ist man bei der Festlegung von Standards? Würden Sie sagen, dass man dabei schon recht weit ist oder ist man hier eher noch in den Anfängen?“



*Einschließlich der Entscheider, die eine Standardisierung grundsätzlich für nicht wichtig halten.

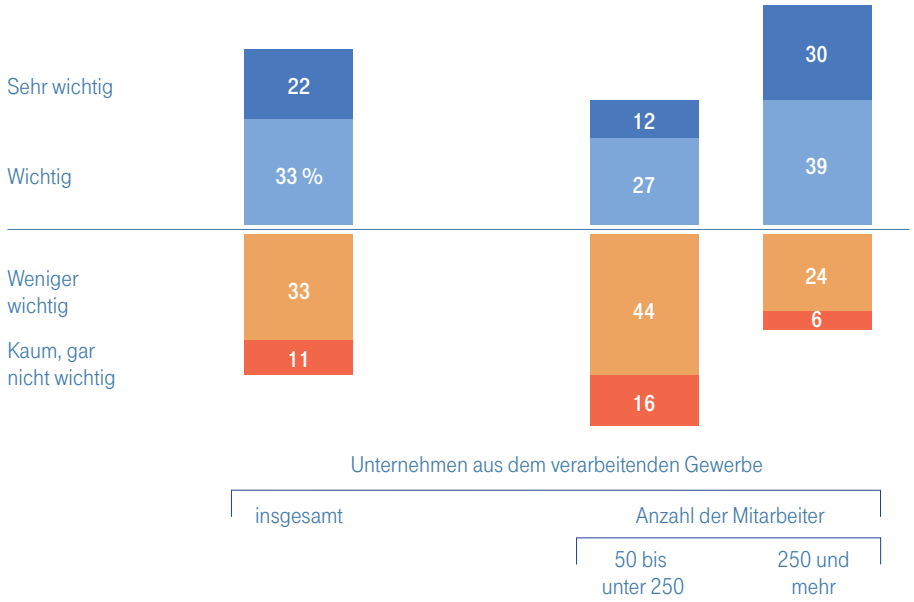
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

INDUSTRIE 4.0 IM EIGENEN UNTERNEHMEN

Schaubild 39

BEDEUTUNG VON „INDUSTRIE 4.0“ FÜR DAS EIGENE UNTERNEHMEN

Frage: „Wie wichtig ist ‚Industrie 4.0‘ für die Zukunft Ihres eigenen Unternehmens?“



Auf 100 fehlende Prozent: Unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen des verarbeitenden Gewerbes
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

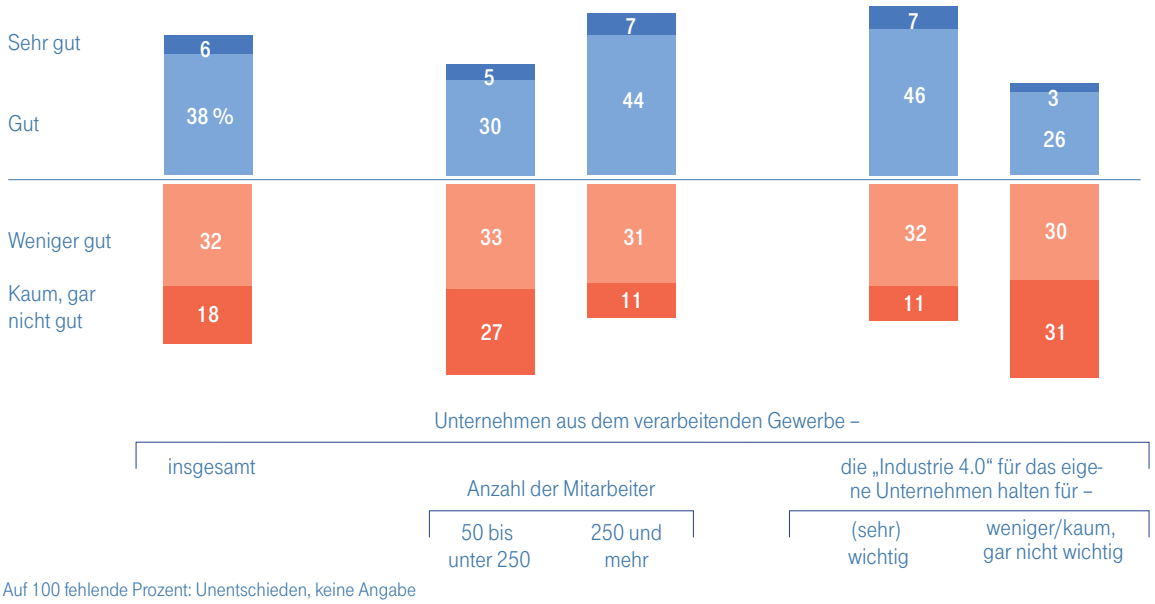
Die große Bedeutung der Neuorganisation der Wertschöpfungskette durch Digitalisierung und Vernetzung der Produktionssysteme wird auch von der Mehrheit der Führungskräfte im verarbeitenden Gewerbe, also in der deutschen Industrie, mit Blick auf das eigene Unternehmen bestätigt. 22 Prozent der Führungskräfte im verarbeitenden Gewerbe halten Industrie 4.0 mit Blick auf die Zukunft des eigenen Unternehmens für sehr wichtig, weitere 33 Prozent für wichtig. Dabei gibt es deutliche Unterschiede in Abhängigkeit von der Unternehmensgröße. Von den mittleren Unternehmen des verarbeitenden Gewerbes stufen 39 Prozent Industrie 4.0 für die Zukunft des eigenen Unternehmens als wichtig oder sehr wichtig ein, von den großen Unternehmen sind es mit 69 Prozent mehr als zwei Drittel **(Schaubild 39)**.

Es sind auch eher die großen als die mittleren Unternehmen, die sich auf Industrie 4.0 gut vorbereitet fühlen. Von allen Unternehmen des verarbeitenden Gewerbes haben 38 Prozent den Eindruck, gut auf die Veränderungen durch Industrie 4.0 vorbereitet zu sein, 6 Prozent sehr gut. Umgekehrt fühlen sich aber 50 Prozent weniger oder gar nicht gut vorbereitet. In den großen Unternehmen haben 51 Prozent, in den mittleren Unternehmen 35 Prozent das Gefühl, gut bzw. sehr gut auf die Veränderungen vorbereitet zu sein. Unterdurchschnittlich vorbereitet zeigen sich die Unternehmen, für deren Zukunft Industrie 4.0 nach eigener Einschätzung eine untergeordnete Bedeutung hat, während sich diejenigen, die Industrie 4.0 als wichtig oder sogar sehr wichtig für das eigene Unternehmen bewerten, mit 53 Prozent auch mehrheitlich gut vorbereitet fühlen **(Schaubild 40)**.

Schaubild 40

GUT AUF „INDUSTRIE 4.0“ VORBEREITET?

Frage: „Haben Sie das Gefühl, dass Ihr Unternehmen gut auf die Veränderungen durch die Umsetzung von ‚Industrie 4.0‘ vorbereitet ist? Würden Sie sagen, Ihr Unternehmen ist da sehr gut, gut, weniger gut oder kaum bzw. gar nicht vorbereitet?“



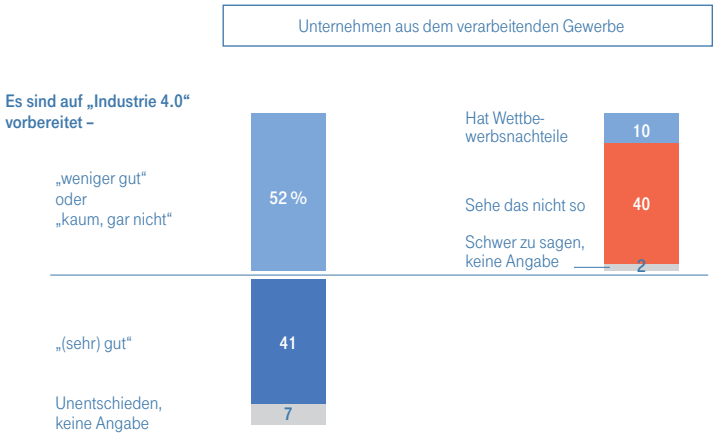
Auf 100 fehlende Prozent: Unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen des verarbeitenden Gewerbes
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Schaubild 41

BEGRENZTE VORBEREITUNG AUF „INDUSTRIE 4.0“ WIRD KAUM ALS WETTBEWERBSNACHTEIL ANGESEHEN

Frage an Unternehmen, die „weniger gut“ oder „kaum, gar nicht“ auf „Industrie 4.0“ vorbereitet sind:
„Glauben Sie, dass Ihr Unternehmen dadurch einen Wettbewerbsnachteil hat, oder glauben Sie das nicht?“



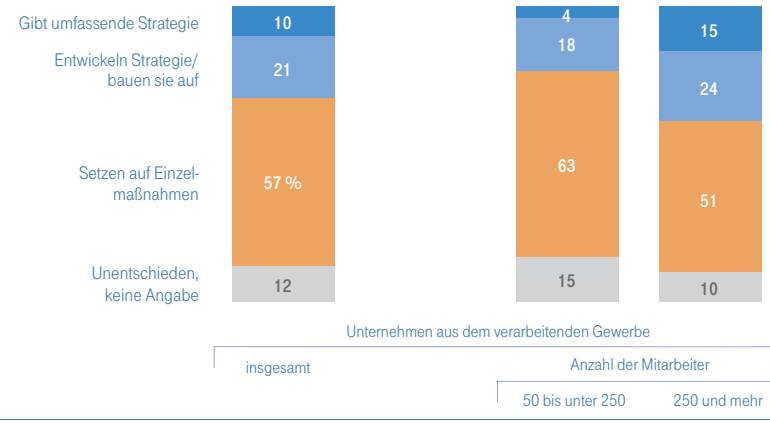
Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen des verarbeitenden Gewerbes
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Die unzureichende Vorbereitung auf die durch Industrie 4.0 induzierten Veränderungen wird von den betroffenen Unternehmen kaum als Wettbewerbsnachteil gesehen. Unter den 52 Prozent der Unternehmen aus dem verarbeitenden Gewerbe, die sich weniger oder gar nicht gut auf Industrie 4.0 vorbereitet sehen, erwarten nur 10 Prozent – bezogen auf alle Unternehmen des verarbeitenden Gewerbes – Wettbewerbsnachteile; 40 Prozent glauben nicht an Wettbewerbsnachteile aufgrund der schlechten Vorbereitung auf die Veränderungen durch Industrie 4.0 **(Schaubild 41)**.

Schaubild 42

UMSETZUNG VON „INDUSTRIE 4.0“ IN DEN UNTERNEHMEN: EHER EINZELMASSNAHMEN STATT UMFASSENDE STRATEGIE

Frage: „Gibt es in Ihrem Unternehmen eine umfassende Strategie zur Umsetzung von ‚Industrie 4.0‘, also zur Automatisierung und Vernetzung der Produktionssysteme oder sind Sie gerade dabei, eine solche umfassende Strategie zu entwickeln und aufzubauen, oder setzen Sie in Ihrem Unternehmen auf einzelne Maßnahmen, um ‚Industrie 4.0‘ einzuführen, statt auf eine umfassende Strategie?“



Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen des verarbeitenden Gewerbes
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

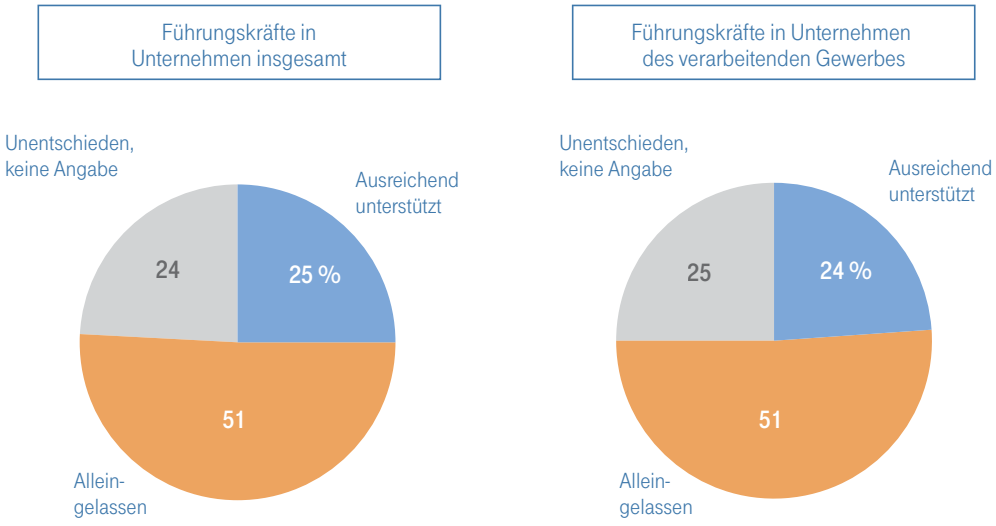
Die große Mehrheit der Unternehmen aus dem verarbeitenden Gewerbe setzt bei der Umsetzung von Industrie 4.0 auf Einzelmaßnahmen. Nur jedes zehnte Unternehmen verfügt derzeit schon über eine umfassende Strategie für die Automatisierung und Vernetzung der Produktionssysteme, 21 Prozent planen die Entwicklung einer solchen umfassenden Strategie. Auch von den großen Unternehmen des verarbeitenden Gewerbes besitzt mit 15 Prozent nur eine Minderheit eine umfassende Strategie, 24 Prozent arbeiten gerade an einer entsprechenden Strategie **(Schaubild 42)**.

Mit Blick auf die staatliche Unterstützung bei der Umsetzung und Bewältigung der Veränderungen aufgrund von Industrie 4.0 hat die Mehrheit der Führungskräfte aus den Unternehmen den Eindruck, dass die Unternehmen von der Politik nicht ausreichend unterstützt werden. Nur rund jeder Vierte ist der Meinung, dass die Politik hier genug Hilfestellungen und Förderung bietet **(Schaubild 43)**.

Schaubild 43

MEHRHEIT SIEHT DIE UNTERNEHMEN BEI DER UMSETZUNG VON „INDUSTRIE 4.0“ NICHT AUSREICHEND VON DER POLITIK UNTERSTÜTZT

Frage: „Wie sehen Sie das: Werden die deutschen Unternehmen bei der Umsetzung von ‚Industrie 4.0‘ ausreichend durch den Staat unterstützt oder haben Sie nicht diesen Eindruck, werden die Unternehmen bei der Umsetzung von der Politik alleingelassen?“



Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

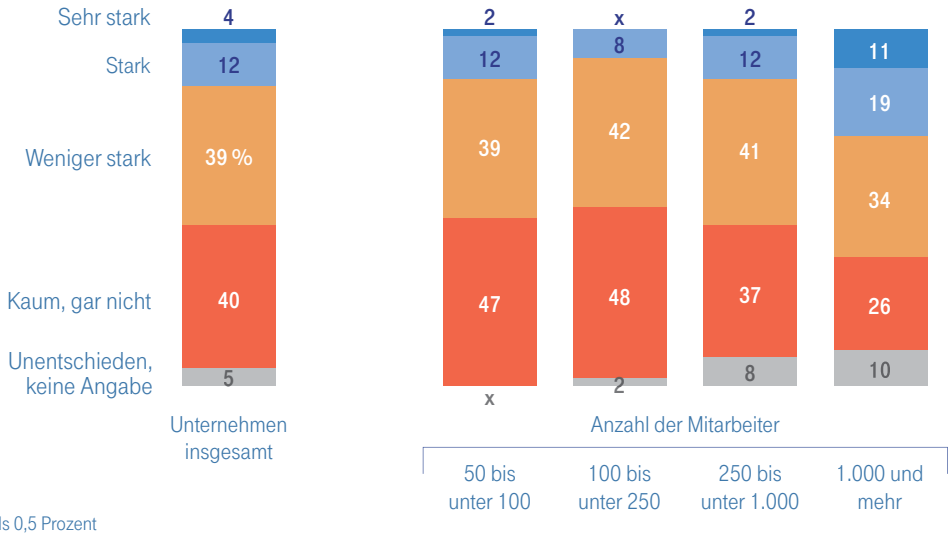
UNTERNEHMENSÜBERGREIFENDE INITIATIVEN ZUR IT-SICHERHEIT

Schaubild 44

NUR EINE KLEINE MINDERHEIT DER UNTERNEHMEN IST IN INITIATIVEN ZUM THEMA IT-SICHERHEIT EINGEBUNDEN

Frage: „Es gibt ja verschiedene Initiativen von Unternehmen, von Unternehmensverbänden oder vom Staat, um sich beim Thema IT-Sicherheit besser auszutauschen. Wie stark ist Ihr Unternehmen in solche Initiativen eingebunden?“

Es sind in Initiativen eingebunden –



x = weniger als 0,5 Prozent

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

In den letzten Cyber Security Reports wurde von den Führungskräften in Unternehmen wie auch von den Abgeordneten die Notwendigkeit eines unternehmensübergreifenden Austauschs zu Themen der IT-Sicherheit betont.[3] Gleichwohl ist derzeit nur ein kleiner Teil der mittleren und großen Unternehmen in Initiativen zum Thema IT-Sicherheit eingebunden. 4 Prozent der Unternehmen sind sehr stark, 12 Prozent stark in die verschiedenen Initiativen von Unternehmen, Unternehmensverbänden oder staatlichen Stellen involviert. Am ehesten noch sind große Unternehmen mit 1.000 und mehr Mitarbeitern Teil solcher Initiativen. Von ihnen ist gut jedes dritte Unternehmen stark oder sogar sehr stark in eine derartige Initiative involviert **(Schaubild 44)**.

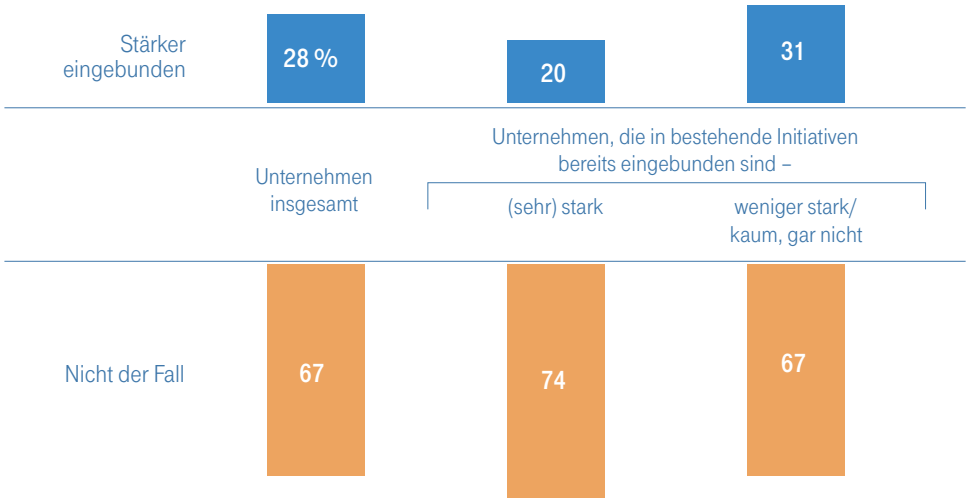
[3] Vgl. Cyber Security Report 2014, Schaubild 36.

Die Mehrheit der Unternehmen wünscht sich aktuell auch keine stärkere Einbindung in bestehende Initiativen. Insgesamt würden sich nur 28 Prozent der Unternehmen wünschen, (noch) stärker in solche Initiativen zur IT-Sicherheit eingebunden zu sein; 67 Prozent sehen hier keinen Bedarf. Von den bislang weniger stark oder gar nicht involvierten Unternehmen würde sich nur rund jedes dritte Unternehmen (31 Prozent) künftig eine stärkere Einbindung wünschen, gut zwei Drittel sehen keinen Bedarf. Von den Unternehmen, die derzeit bereits sehr stark oder stark eingebunden sind, sind 20 Prozent an einer noch stärkeren Einbindung interessiert **(Schaubild 45)**.

Schaubild 45

WUNSCH NACH EINER STÄRKEREN EINBINDUNG IN INITIATIVEN ZUM THEMA IT-SICHERHEIT

Frage: „Würden Sie sich wünschen, (noch) stärker in solche Initiativen eingebunden zu sein, oder ist das nicht der Fall?“



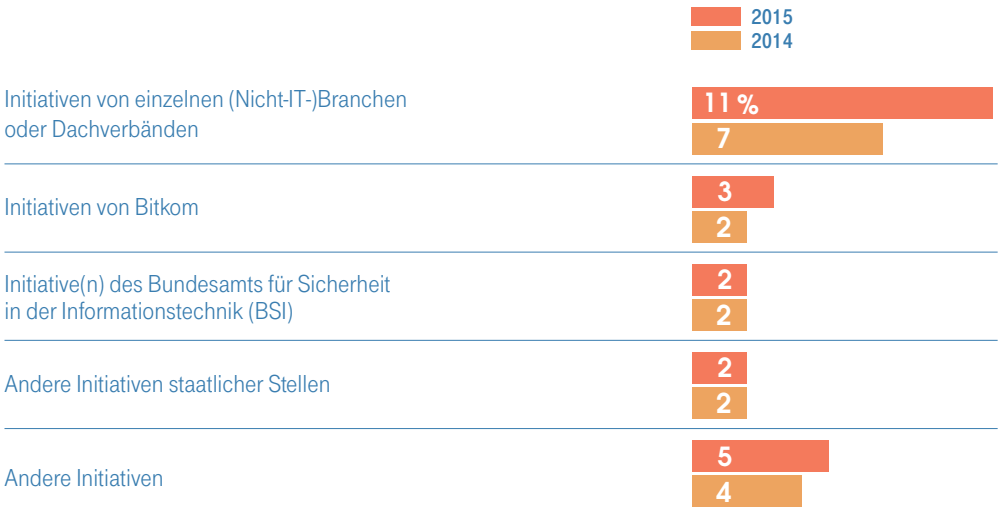
Auf 100 fehlende Prozent: Unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7231 (September 2015)

Schaubild 46

KONKRETE INITIATIVEN IM BEREICH IT-SICHERHEIT SIND KAUM BEKANNT

Frage: „Welche Initiativen in diesem Bereich sind Ihnen bekannt oder sind Ihnen da keine Initiativen bekannt?“ (offene Ermittlung, ohne Antwortvorgaben)



Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen 6289, 7231

Die wenigsten Führungskräfte können auf die offene Frage (ohne Antwortvorgaben), welche Initiativen zur IT-Sicherheit sie kennen, konkrete Initiativen benennen. Am ehesten noch sind Initiativen von einzelnen Branchen oder Dachverbänden außerhalb der IT-Branche bekannt. 11 Prozent der Führungskräfte nannten Initiativen aus diesem Bereich. Die Initiativen des IT-Branchenverbands Bitkom kennen 3 Prozent. Initiativen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und Aktivitäten anderer staatlicher Stellen werden jeweils von 2 Prozent aller Führungskräfte in mittleren und großen Unternehmen spontan genannt **(Schaubild 46)**.

Bei der gestützten Abfrage war aber erneut eine Zunahme der Bekanntheit des Cyber Security Summits zu verzeichnen. Vor zwei Jahren gaben 27 der Entscheider an, bereits vom Cyber Security Summit gehört zu haben, im Vorjahr waren es 44 Prozent, in diesem Jahr sind es 51 Prozent.

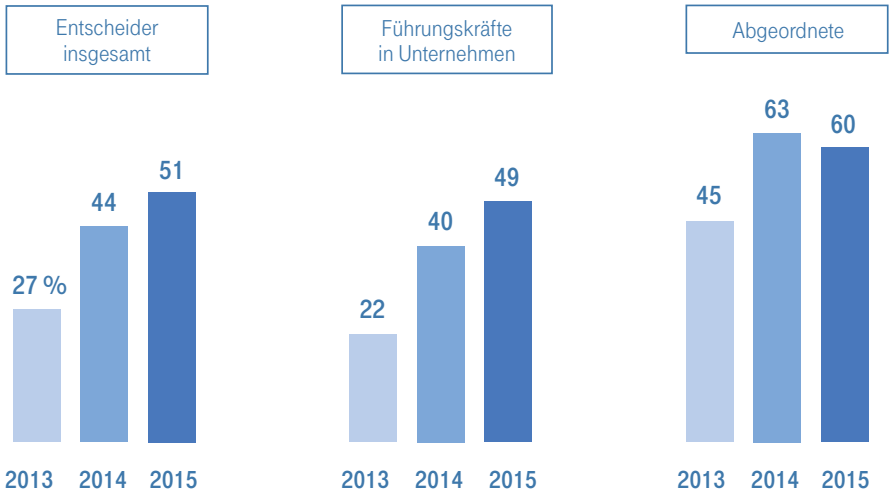
Besonders hoch ist die gestützte Bekanntheit unter Abgeordneten, von denen 60 Prozent angeben, von der Veranstaltung bereits gehört zu haben. Von den Unternehmensentscheidern haben 49 Prozent den Cyber Security Summit registriert **(Schaubild 47)**.

Schaubild 47

GESTÜTZTE BEKANNTHEIT CYBER SECURITY SUMMIT

Frage: „Seit 2012 findet jährlich der sogenannte Cyber Security Summit zum Thema IT-Sicherheit mit Teilnehmern aus Wirtschaft, Wissenschaft und Sicherheitsbehörden statt. Haben Sie von dieser Veranstaltung gehört oder haben Sie davon noch nicht gehört?“

Es haben schon vom Cyber Security Summit gehört –



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7231

STUDIENDESIGN IM ÜBERBLICK

STICHPROBE

Insgesamt 645 Topentscheider aus Politik und Wirtschaft, davon:

a) 113 Abgeordnete, davon
35 Bundestagsabgeordnete,
68 Landtagsabgeordnete und
10 deutsche Abgeordnete im EU-Parlament

b) 532 Führungskräfte aus mittleren und großen Unternehmen, davon

285 Führungskräfte aus mittleren Unternehmen,
247 Führungskräfte aus Großunternehmen,

337 Inhaber, Geschäftsführer oder Vorstände und
195 andere Führungskräfte (z. B. Bereichsleiter)

Als Großunternehmen gelten gemäß der Definition der EU-Kommission Unternehmen mit mindestens 250 Beschäftigten und/oder mehr als 50 Mio. Euro Jahresumsatz.

Mittlere Unternehmen sind gemäß Definition der EU-Kommission Unternehmen, die zwischen 50 und 249 Mitarbeiter haben und/oder einen Jahresumsatz von 10 bis höchstens 50 Mio. Euro erzielen.

Da das Schwerpunktthema „Industrie 4.0“ vor allem für das verarbeitende Gewerbe von Bedeutung ist, wurden Unternehmen aus diesem Wirtschaftssektor mit 293 Interviews überproportional berücksichtigt, sodass für die Analyse eine ausreichende Fallzahl vorliegt. Gleichzeitig wurde durch eine faktorielle Gewichtung sichergestellt, dass die Unternehmen des verarbeitenden Gewerbes in die Gesamtergebnisse nur mit ihrem tatsächlichen Anteil an allen Unternehmen eingehen.

METHODE

Telefonische Interviews (CATI)

BEFRAGUNGSZEITRAUM

19. August bis 2. Oktober 2015